A HOOVER INSTITUTION ESSAY

China, Encryption Policy, and International Influence

ADAM SEGAL

Series Paper No. 1610

Hanging over the stand-off between the FBI and Apple over access to an encrypted iPhone used by one of the San Bernardino attackers was the question: What would China do?[1] If Apple created unique software that allowed Washington access to the phone, would that open the door for Beijing to make similar demands on the company and all other foreign technology firms operating in China? As Senator Ron Wyden of Oregon argued, "This move by the FBI could snowball around the world. Why in the world would our government want to give repressive regimes in Russia and China a blueprint for forcing American companies to create a backdoor?"[2]

There was, at least at the rhetorical level, interaction between Chinese and US policymakers on the question of encryption. An early draft of China's counterterrorism law, for example, included provisions requiring the installation of backdoors and the reporting of encryption keys. President Barack Obama criticized these provisions in a March 2015 interview with Reuters, claiming they "would essentially force all foreign companies, including US companies, to turn over to the Chinese government mechanisms where they could snoop and keep track of all the users of those services." He added, "We've made very clear to them [the Chinese government] that this is something they're going to have to change if they expect to do business with the United States."[3]

A few days later, in the face of criticism from the US government and foreign technology companies, Fu Ying, spokeswoman for the National People's Congress, defended the provisions as in accordance with "international common practices." Fu argued that Western countries such as the United States and the United Kingdom often request that technology firms disclose encryption methods.[4] A commentary published in *Xinhua,* China's state news agency, at the same time stated, "Many countries including the United States have written into law technology firms' duty to cooperate in terror-related surveillance or probe."[5] The final law, passed in December 2015, was much more ambiguous about what type of demands the government would make on technology companies, but it was clear that Chinese leaders were more than happy to exploit the debate over encryption in the United States and Europe as rhetorical cover.

Despite this interplay, it is difficult to disentangle the influence of US encryption policy on the development of Chinese regulations and laws. Independent of what happens in Washington, Beijing has a long history of using encryption policy to foster national and domestic security as well as to promote economic growth and indigenous innovation. Moreover, the Snowden revelations have reenergized Chinese efforts to use cyber security regulations as a catalyst for industrial policy; the desire for access to data, encrypted or not, is likely to intensify under President Xi Jinping's leadership. The Chinese Communist Party appears increasingly worried about domestic stability, regime legitimacy, and the spread of information within China. In short, the very public debate between Apple and the FBI dovetailed with many of the Chinese government's long-term concerns and interests.

In the past, US economic and political pressure has shifted Chinese policy, but within parameters defined by security and techno-nationalist concerns. Under President Xi Jinping, these concerns have heightened and the parameters have significantly narrowed. The demands made on foreign and domestic technology companies can be expected to increase over the next several years.

Encryption as Industrial Policy

The Chinese government began regulating encryption in 1999 with the release of State Council Directive No. 273, Regulations on the Administration of Commercial Encryption. These regulations banned foreign encryption products, deemed all commercial encryption standards a state secret, and required that commercial encryption products only be produced and sold by units designated by the relevant government authorities: the State Encryption Management Bureau and the Office of State Commercial Cryptography Administration. The rules also required that the strength of encryption systems not surpass a level set by the state regulator.[6]

At the time of their introduction, the regulations were criticized as overly broad, but subsequent clarifications by Chinese officials in March 2000 revealed that regulators did not see the rules as covering products that use encryption as a secondary function (e.g., laptops, mobile phones, web browsers, and computer software).[7] In other words, the ban on foreign encryption was only on products whose "core function" was encryption, not commercial information and communication technology (ICT) products that applied encryption. Beijing also announced that it would not carry out key escrow of foreign encryption products and equipment containing encryption technology.[8]

The State Encryption Management Bureau has been working on revisions to the regulations since 1999. US and EU trade negotiators have long feared that encryption

regulations would eventually be expanded to other products. In early 2012, for example, Beijing mandated that a 4G Long Term Evolution (LTE) encryption algorithm developed by a Chinese government-owned research lab, known as the ZUC standard, be used in telecommunication infrastructure.[9] Implementation of the mandate would have also presented foreign manufacturers with compulsory testing of 4G LTE products and source code and intellectual property disclosure requirements. The United States Trade Representative has argued that ZUC contravenes not only Beijing's promise to be technology-neutral in procurement by network operators but also its commitment to allow foreign encryption standards in the broad commercial market and its pledge that "Chinese only" requirements will only be imposed on products whose core function is encryption.[10] After pushback from the United States and others, China announced that it would not mandate any one particular standard.[11]

Encryption regulations have also been deployed as part of a larger effort to use standards policy to bolster the competitiveness of Chinese technology firms. The Chinese standards process is top-down, driven by state organizations, in contrast to the voluntary, private sector-led effort that is the norm in the United States, Europe, and Japan.[12] In December 2003, the government announced that the WLAN Authentication and Privacy Infrastructure encryption technique, or WAPI, would be the mandatory standard for any wireless product sold in China.[13] Beijing banned 802.11 WiFi over "national security concerns," but the policy was also designed to reduce payments to foreign patent holders and support domestic producers. The policy would have forced Intel and other foreign companies to cooperate with one of eleven Chinese vendors licensed to develop WAPI products, although it did not allow the foreign partner to see details of the wireless specification. After a letter from the Bush administration implicitly threatened to pursue the case at the World Trade Organization (WTO), the Chinese government agreed to revise the standard after soliciting comments from domestic and foreign firms.[14] (Perhaps to avoid the controversy, the first Apple phones in China supported neither WAPI nor WiFi, and did not sell well. China abandoned its WAPI-only policy after opposition from the International Organization for Standardization, and Apple eventually introduced a 3GS iPhone model that supported both WiFi and WAPI. Stewart Baker and the FBI have suggested that since WAPI is based on encryption algorithms that are not transparent and were developed in cooperation with Chinese security agencies, Apple has essentially installed a backdoor in products on the mainland.[15])

In 2007, the State Encryption Administration released the Regulations on Classified Protection of Information Security, also known as the Multi-Level Protection Scheme

(MLPS). The regulations required that information security systems sold within China—including encryption—use certain indigenous technologies if they had a high risk of impacting national security or domestic stability should they be compromised.[16] The regulations, which were jointly released with the Ministry of Public Security, State Secrecy Bureau, and State Council Information Office, classified information systems into five grades. The first grade was for products that had little potential impact on national interests, the fifth for those with an "especially grave" impact on national interests.[17]

Systems classified as grade three or above—a broad designation that includes state affairs, finance, banking, tax, customs, audit, industry, communications, commerce, health, education, and social services, as well as activities "related to national economy and people's livelihood"—are required to rely primarily on technology that has "indigenous intellectual property rights."[18] Dieter Ernst and Sheri Martin have described the enforcement of encryption standards in the MLPS as "another area in which government involvement trumps industry." The agency in charge of enforcing the standard can carry out unannounced inspections of systems, can access key management and other cryptologic protocols, and can require, through the Office of State Commercial Cryptography Administration, that a significant portion of source code be handed over.[19]

Foreign businesses and governments have claimed that the MLPS is being used to protect large portions of the Chinese economy from international competition.[20] The Information Technology Industry Council, for example, estimated that 60 to 70 percent, or $35.2 billion to $41 billion, of China's $58.6 billion total commercial and public sector IT spending, was covered by MLPS in 2010.[21] At a 2012 meeting of the US-China Joint Commission on Commerce and Trade, Beijing indicated that it would begin revising the MLPS, but by 2015 had made no move toward changes.[22]

The newly created Cyberspace Administration of China has declared its intention to make China a "cyber power."[23] In pursuit of this goal, China has introduced a series of measures designed to make technology "secure and controllable" and to reduce dependence on foreign information technology products and services. A draft measure issued by the China Banking Regulatory Commission, for example, called for 75 percent of ICT products used in China's banking system to be "secure and controllable" by 2019. As originally drafted, the regulation would have required banks to file source code for all software with the Chinese government and submit encryption products to Chinese regulators for testing and certification.[24] These measures raised serious concerns in the United States and the

global ICT industry as they appeared to be an expansion of the 1999 measure on encryption of commercial IT products. The foreign business community protested, and in April 2015 China announced that it would suspend implementation of the banking regulations.[25]

While specifically focused on national security concerns, the counterterrorism law is also related to Beijing's push for technology that is "secure and controllable." The November 2014 draft law would have required "telecommunications service providers" and "Internet service providers" to file their encryption solutions with the Chinese government and embed a "technical interface" in the construction of their networks. They were also expected to keep relevant equipment and user data within the territory of China.[26]

Under the final version of the law, the requirement to file encryption solutions with the Chinese government and embed a technical interface in relevant networks was replaced by a vaguer and more general requirement in Article 18 to "provide technical support and assistance, such as technical interface and decryption, to support the activities of the public security and state security authorities in preventing and investigating terrorist activities."[27] The data localization requirement was completely removed.

The foreign community was relieved to have the filing of encryption solutions and the mandate for backdoors removed, but the wording of Article 18 seems to leave local public security and state security authorities with "broad discretionary authority to require companies to provide access to their equipment and decryption support in particular cases."[28] It may still require firms to hand over encryption keys to Chinese authorities. Failure to comply with Article 18 can attract penalties, if the circumstances are serious, that include fines of more than 500,000 renminbi (about $73,000) for the company and fines of up to 500,000 RMB and criminal detention of up to fifteen days for the relevant responsible person (Article 84).

Encryption and Domestic Stability

Despite consolidating power more quickly than his predecessors and mounting a widespread and vigorous anticorruption campaign, Xi is clearly worried about threats to regime legitimacy and domestic stability. China has tightened censorship of the Internet and media, passed a new law regulating foreign nongovernmental organizations, launched ideological campaigns in universities and think tanks, and arrested rights lawyers, feminists, foreign NGO workers, bloggers, and environmental activists. Chinese leaders and academics are also likely to see the Erdogan government's

ability to retain control over social media as a central reason for the failure of the attempted coup in Turkey in July 2016.

As part of the crackdown on civil society and the Internet, China has blocked access to most encrypted messaging applications. During July 2014, KakaoTalk and Line, two South Korean messaging apps, were disrupted by Domain Name System (DNS) tampering and HTTP request filtering for users based in China.[29] A month later, Beijing told Seoul it had blocked access to the apps, claiming terrorist organizations were using them to incite attacks and spread bomb-making instructions.[30] During the same month, China tightened restrictions on domestic messaging apps and social media. Users of messaging services were required to verify their real name identities before registering new accounts. Public accounts were also banned from publishing or sharing "political news" without approval.[31]

Several Chinese human rights lawyers were detained in July 2015, and media reports suggested they were using encrypted messaging app Telegram. Around the same time the service suffered a DDoS (distributed denial of service) attack that knocked it offline for users in the Asia Pacific region.[32] In November 2015, the government shut down the mobile services of residents of Xinjiang, China's restive Muslim region, who were using circumvention software.[33] Users who were using virtual private networks (VPNs) or accessing WhatsApp and Telegram were told to report to local police stations to have their mobile phone service restored.

China has not responded to WhatsApp's announcement in April 2016 that it would implement end-to-end encryption (and as of this writing it is still not blocked in China). While many of Hong Kong's Umbrella Movement leaders used WhatsApp group chats to organize protests, political messages did not spread to the mainland as they did on Instagram, which was blocked during the protests.[34] This may explain why WhatsApp was not blocked as well as the fact that the app has a relatively small number of users on the mainland, with 23 million monthly active users compared to WeChat and QQ with 700 million and 860 million monthly active users, respectively.[35] These domestic services are encrypted in transit, but they do not offer end-to-end encryption, and it is unknown if messages are stored in plaintext.

Shaping Chinese Policy

How much influence do policy developments or outside companies and governments have on Beijing, given the strong domestic motivations for Chinese encryption policy? In the past decade, security and technology concerns limited

foreign influence on domestic debates, but did not completely insulate Chinese policymakers. Direct foreign pressure moderated Chinese policy in a number of instances, including the counterterrorism law and the WAPI case. In August 2016, representatives of forty-six international businesses wrote to Premier Li Keqiang urging China to revise draft cyber security laws. The signatories argued that security reviews for ICT products would weaken security and might constitute technical barriers to trade under the WTO.[36] In an effort to ease foreign concerns, Intel, Cisco, Microsoft, IBM, and other companies were asked to join an advisory committee under the Cyberspace Administration of China shaping the changes to the law.[37] What these cases had in common was a unified front among American technology companies, a willingness to raise the issue at the highest level of the US government, and multilateral pressure as Japan and the European Union also threatened to take a case to the WTO.[38]

Chinese policy also moves when the interests of foreign companies and governments overlap with those of Chinese consumers. In June 2009, for example, the Ministry of Industry and Information Technology announced that all new computers sold in China would be required to have the "Green Dam-Youth Escort" Internet filtering software preinstalled.[39] The official purpose of the software was to help parents protect children from pornography and "smut" on the web. But University of Michigan researchers found that it had broader censorship functions—it had a list of sensitive words that could be continually updated to block surfing—and could make PCs vulnerable to hacking. It also allegedly stole code from two US software companies.[40]

As usual, the US government and the EU as well as personal-computer makers objected to the regulation.[41] But online protests within China made this case different from previous tussles over industrial policy. Blogs and forums criticized the software, petition letters were submitted online, and users circulated sarcastic cartoons and videos. Inexpensive "anti-Green Dam" software was also available for purchase on the Chinese market. After a month, Beijing announced that it was delaying (indefinitely) the implementation of the regulation.[42]

The ability of foreign companies and governments to get Beijing not to do something it wants has, however, dramatically changed over the last decade. The great recession of 2008 and slow growth in Europe and the United States have weakened the West's economic and political leverage within China. The new policies appear to come from the top—from the Central Leading Group for Cyberspace Affairs, which is chaired by President Xi—while previous policies were pushed by specific ministries. In addition, banks and other sectors often chose not to comply with past regulations, arguing

that swapping out foreign products for domestic competitors was too expensive and would affect the reliability of their systems. Companies have been told with the most recent regulations they cannot opt out. Chinese products may lag slightly behind, but there are now close approximations to Western technologies in the domestic market—Huawei for Cisco; Inspur for IBM; Xiaomi for Apple; and Kylin for Microsoft.

Moreover, there is no guarantee that there will be no defections from foreign technology companies over the encryption issue in China. While American companies have maintained a united front in face of pressure from the US government, the importance of the Chinese market to current revenues and future growth may lead firms to fork their technologies, creating different products for different markets. There has been little fallout for LinkedIn over its decision to create a separate Chinese version that censors posts within China. If Facebook's efforts to convince Chinese regulators to allow it into the market succeed, it seems inevitable that Facebook will have to censor within China. Then again, the reputational cost of refusing to cooperate with the US government on encryption, thus possibly threatening national security while providing backdoors for the Chinese Communist Party, may greatly outweigh the public relations damage that comes from censorship, which has long been seen as part of the cost of doing business with Beijing.[43]

There are fewer obvious cases of modeling, or Chinese decision-makers using US policy as cover or precedent for new regulations. The argument might be made in the case of Huawei and the increased regulation of Cisco, Microsoft, and other foreign firms within China. Despite claims from Huawei that it has no ties to the Chinese government, US policymakers and analysts have long suspected that the telecommunications equipment manufacturer cooperates with the People's Liberation Army (PLA).[44] As a result, US government officials opposed a bid from Huawei and Bain Capital to buy 3Com, an American computer equipment maker, in 2008. A year later, US objections derailed Huawei's efforts to buy patents and hire employees from a computer services company, 3Leaf. In 2010, then Commerce Secretary Gary Locke called the head of Sprint Nextel to express "deep concerns" that Huawei might win a contract to upgrade the mobile phone carrier's network. In November 2011, the House Select Intelligence Committee started an investigation of the threat posed to US cyber security by Huawei and ZTE, another Chinese telecommunications company headquartered in Shenzhen.[45]

Concerns about Huawei ran so high that the National Security Agency reportedly created backdoors into the company's equipment. A project code-named SHOTGIANT

attempted to find connections between the company and the PLA, according to documents released by Snowden and published by the *New York Times* and *Spiegel*. "If we can determine the company's plans and intentions," an analyst wrote, "we hope that this will lead us back to the plans and intentions of the PRC [People's Republic of China]."[46]

The Chinese press often cites Huawei's experience in the US market as justification for investigations of Cisco and others; technology watcher Bill Bishop has described the pressuring of foreign firms as being "Huawei'd."[47] For some Chinese policymakers, apprehension about the alleged security threat posed by Huawei in itself proves that foreign companies are a danger. The logic is that if Washington is hesitant to have foreign suppliers in its computer and telecommunications networks, and the United States is more advanced than China in its cyber security, then there must really be something to worry about.

Chinese Firms

Chinese encryption policy is shaped by domestic politics, security concerns, techno-nationalist strategies, foreign businesses and governments, and a new, emerging variable: the "going out" of Chinese technology firms. Theoretically, as these firms have a greater presence in global markets, they will face the same pressures as US firms to reassure their customers that they have some degree of independence from intelligence and law enforcement agencies. Xiaomi, for example, announced that it was migrating the data of international users out of centers in Beijing to centers in California and Singapore.[48] Huawei reportedly backed Apple's position on encryption.[49] Globalizing Chinese firms also have a shared interest in transparent standards (technological and legal) that allow companies to take advantage of scale, not respond to multiple competing national requirements that splinter the market.

Yet, as with many economic and political spheres, there is a limit to the convergence of interests between Chinese and US technology firms. After at least two decades of standing outside of and disrupting the state-owned economy, Chinese technology firms are growing increasingly reliant on government support for future growth. They may be growing more dependent on the state and less willing to challenge it. Moreover, Beijing has appeared willing to sacrifice economic interests for political goals. In April 2015, researchers at the Citizen Lab at the University of Toronto and International Computer Science Institute at the University of California, Berkeley, identified a tool they called the Great Cannon that hijacked traffic and directed it at GreatFire.org, a site that runs mirrors of other sites blocked in China, and GitHub, a software coding site that was

also hosting content Beijing found objectionable. In particular, the cannon orchestrated these attacks by injecting malicious scripts into connections to Baidu, the Chinese search giant. As the researchers concluded, use of Baidu in the attacks is evidence "that the Chinese authorities are willing to pursue domestic stability and security aims at the expense of other goals, including fostering economic growth in the tech sector."[50] In addition, exploiting Baidu undermines Beijing's stated goal of helping Internet companies increase their presence in international markets.

Conclusion

Three uncertainties may reshape Beijing's encryption policy. Little is known about Chinese users' attitudes toward encryption and whether they see it as important to cyber security or personal privacy. In July 2016, Chinese mobile phone manufacturer Gionee introduced a privacy-focused device that included an encryption chip.[51] These claims may have been directed at users' concerns about growing cybercrime, since Chinese citizens have little expectation of privacy from government surveillance. Still, increased consumer demand for security could place greater pressure on Chinese firms to provide increased levels of encryption.

Second, as has happened in the United States, France, and Germany, a successful terrorist attack within China could result in greater demands for access to encryption and quickly raise the political pressure on technology companies. In the wake of an attack, the Chinese are also likely to make calls for international regulation of encryption a larger part of their cyber diplomacy.

Third, there is a great deal of uncertainty about the nature of innovation in the Chinese economy. While Beijing's recent technology policy has had a strong mercantilist slant, there is still a domestic debate over whether a more open, inclusive approach is more appropriate to achieving the goal of becoming a science and technology power. A number of prominent technologists have argued that cutting off China from foreign competition will hamper innovation, not foster it. Huawei CEO Eric Xu told Reuters, for example, "If we're not open, if we don't bring in the world's best technology, we'll never have true information security."[52]

These are, however, not the dominant voices now. The drive for "secure and controllable" technologies and the heightened sensitivity to perceived threats to domestic stability have combined to further narrow the space in which technology companies and foreign governments might move Beijing. When China has changed its technology policies in the past, it has done so when faced with broad international pressure and unified industry opposition. These reversals, however,

have usually been temporary; one policy is replaced with another designed to achieve a similar set of outcomes. Given Beijing's historical techno-nationalist and security concerns, foreign influence on China's encryption policy has been and will continue to be limited.

NOTES

1 Adam Segal, "China Is Watching the FBI-Apple Battle Very Closely," *Defense One,* March 4, 2016, www.defenseone.com/ideas/2016/03/china-fbi-apple-encryption/126450/.

2 David Pierson, "Why Apple's Fight with the FBI Could Have Reverberations in China," *Los Angeles Times,* February 19, 2016, www.latimes.com/business/technology/la-fi-tn-apple-global-privacy-20160219-story.html.

3 "Exclusive: Full Text of Reuters Interview with Obama," Reuters, March 2, 2015, www.reuters.com/article/us-usa-obama-transcript-idUSKBN0LY2J820150302.

4 Gerry Shih and Paul Carsten, "China Says Tech Firms Have Nothing to Fear from Anti-Terror Law," Reuters, March 4, 2015, www.reuters.com/article/us-china-parliament-cybersecurity-idUSKBN0M00IU20150304.

5 "China's Anti-terrorism Legislation No Excuse for U.S. Agitation," *Xinhua,* December 27, 2015.

6 State Council of the People's Republic of China, "Regulations on the Administration of Commercial Encryption," Order 273, October 7, 1999, www.oscca.gov.cn/News/200512/News_1053.htm.

7 Christopher T. Cloutier and Jane Y. Cohen, "Casting a Wide Net: China's Encryption Restrictions," *WorldECR,* November 2011, www.kslaw.com/imageserver/KSPublic/library/publication/2011articles/11-11WorldECRCloutierCohen.pdf.

8 Bert-Jaap Koops, "People's Republic of China," *Crypto Law Survey,* February 2013, www.cryptolaw.org/cls2.htm.

9 Stephen J. Ezell and Robert D. Atkinson, "The Middle Kingdom Galapagos Island Syndrome: The Cul-De-Sac of Chinese Technology Standards," Information Technology & Innovation Foundation, December 2014, www2.itif.org/2014-galapagos-chinese-ict.pdf.

10 Office of the United States Trade Representative, "2014 Section 1377 Review on Compliance with Telecommunications Trade Agreements," 2014, https://ustr.gov/sites/default/files/2013-14%20-1377Report-final.pdf.

11 Ibid.

12 Ezell and Atkinson, "The Middle Kingdom Galapagos Island Syndrome."

13 US Trade Representative, "2014 Section 1377 Review."

14 "Letter from Bush Administration to Beijing Protesting Wi-Fi Encryption Standards," *Bloomberg,* March 15, 2004, www.bloomberg.com/news/articles/2004-03-14/online-extra-letter-from-bush-administration-officials-to-beijing-protesting-wi-fi-encryption-standards.

15 Stewart A. Baker, "Deposing Tim Cook," *Lawfare,* February 27, 2016, www.lawfareblog.com/deposing-tim-cook.

16 "Regulations on Classified Protection of Information Security," Chinese Classified Protection of Information Security Online, July 27, 2007, http://www.djbh.net/webdev/web/HomeWebAction.do?p=getZcbz&id=2c9090942a0d4f31012a1c15302b003b&classification=ZCBZ_GLGF.

17 Nathaniel Ahrens, "National Security and China's Information Security Standards," Center for Strategic & International Studies, November 2012, 4, https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/121108_Ahrens_NationalSecurityChina_web.pdf.

18 Office of State Commercial Cryptography Administration, "Guide to Information Security Classified Protection of Commercial Encryption Testing Mechanism Review Services," September 2015, www.oscca.gov.cn/WebSite/smb/Upload/File/201509/20150918164831439375.pdf.

19 Dieter Ernst and Sheri Martin, "The Common Criteria for Information Technology Security Evaluation—Implications for China's Policy on Information Security Standards," East-West Center Working Papers, No. 108, January 2010, www.files.ethz.ch/isn/134351/econwp108.pdf.

20 Robert McMillan, "China Policy Could Force Foreign Security Firms Out," *Network World,* August 26, 2010, www.networkworld.com/article/2217282/security/china-policy-could-force-foreign-security-firms-out.html.

21 "2014 Written Comments to the U.S. Government Interagency Trade Policy Staff Committee In Response to Federal Register Notice Regarding China's Compliance with Its Accession Commitments to the World Trade Organization (WTO)," Information Technology Industry Council, Semiconductor Industry Association, Software & Information Industry Association, and Telecommunications Industry Association, September 19, 2014, www.tiaonline.org/sites/default/files/pages/2014%20USITO%20China%20WTO%20Compliance%20Filing.pdf.

22 Office of the United States Trade Representative, "23rd U.S.-China Joint Commission on Commerce and Trade," December 19, 2012, https://ustr.gov/about-us/policy-offices/press-office/fact-sheets/2012/december/23rd-JCCT.

23 "Xi Jinping Leads Internet Security Group," *Xinhua,* February 27, 2014, http://news.xinhuanet.com/english/china/2014-02/27/c_133148273.htm.

24 Chinese Banking Regulatory Commission, "Guiding Opinions on Applying Secure and Controllable Information Technologies to Strengthen the Cybersecurity and Informatization Construction of the Banking Industry," September 3, 2014, www.cbrc.gov.cn/govView_EE29BABB27EB4E51A4343517691438F9.html.

25 Paul Mozur, "New Rules in China Upset Western Tech Companies," *New York Times,* January 28, 2015, www.nytimes.com/2015/01/29/technology/in-china-new-cybersecurity-rules-perturb-western-tech-companies.html; Paul Mozur and Jane Perlez, "China Halts New Policy on Tech for Banks," *New York Times,* April 16, 2015, www.nytimes.com/2015/04/17/business/international/china-suspends-rules-on-tech-companies-serving-banks.html; Adam Segal, "What to Do about China's New Cybersecurity Regulations?" *Net Politics* (blog), Council on Foreign Relations, February 2, 2015, http://blogs.cfr.org/cyber/2015/02/02/what-to-do-about-chinas-new-cybersecurity-regulations/.

26 "Counter-Terrorism Law (Initial Draft)," *China Law Translate,* November 8, 2014, http://chinalawtranslate.com/ctldraft/?lang=en.

27 National People's Congress, "Counter-Terrorism Law of the People's Republic of China" (author's translation), December 27, 2015, http://news.xinhuanet.com/politics/2015-12/27/c_128571798.htm.

28 Paul D. McKenzie, Gordon A. Milner, and Wei Zhang, "China's Anti-Terrorism Law Raises Data Security Concerns," *Lexology,* January 20, 2016, www.lexology.com/library/detail.aspx?g=705429e6-d560-4ef9-a415-d34650f3629c.

29 "Asia Chats: LINE and KakaoTalk Disruptions in China," *The Citizen Lab,* July 2014, https://citizenlab.org/2014/07/line-kakaotalk-disruptions-china/.

30 Se Young Lee, "China Tells South Korea It Blocked KakaoTalk, Line to Fight Terrorism," Reuters, August 7, 2014, www.reuters.com/article/us-southkorea-china-apps-idUSKBN0G709E20140807.

31 Ma Danning, "Real Names Now Required for WeChat and Other IMS," *China Daily,* August 7, 2014, www.chinadaily.com.cn/china/2014-08/07/content_18268073.htm; Ned Levin, Eva Dou, and Min-Jeong Lee, "China Tightens Restrictions on Messaging Apps," *Wall Street Journal,* August 7, 2014, www.wsj.com /articles/china-issues-new-restrictions-on-messaging-apps-1407405666; Paul Bischoff, "A Brief History of China's Campaign to Enforce Real-Name Registration Online," *Tech in Asia,* February 5, 2015, https://www .techinasia.com/history-chinas-campaign-enforce-realname-registration-online.

32 Josh Horwitz, "A Cyber Attack Struck Messaging App Telegram Just as China Was Cracking Down on Human Rights Lawyers," *Quartz,* July 13, 2015, http://qz.com/451575/a-cyber-attack-struck-messaging-app -telegram-just-as-china-was-cracking-down-on-human-rights-lawyers/.

33 Paul Mozur, "China Cuts Mobile Service of Xinjiang Residents Evading Internet Filters," *New York Times,* November 23, 2015, www.nytimes.com/2015/11/24/business/international/china-cuts-mobile-service-of -xinjiang-residents-evading-internet-filters.html.

34 Te-Ping Chen, Fiona Law, and Newley Purnell, "Apps Speed Up, and Often Muddle, Hong Kong Protesters' Messages," *Wall Street Journal,* October 9, 2014, www.wsj.com/articles/whatsapp-key-to -quickly-rallying-protesters-in-hong-kong-but-groups-struggle-to-stay-on-message-1412878808; "Instagram Appears Blocked in China," BBC, September 29, 2014, www.bbc.com/news/technology -29409533; Paul Bischoff, "Instagram Accessible Again in China, but Service Is Patchy," *Tech in Asia,* January 25, 2015, www.techinasia.com/instagram-accessible-china-service-patchy.

35 Steven Millward, "WeChat Still Unstoppable, Grows to 697m Active Users," *Tech in Asia,* March 17, 2016, www.techinasia.com/wechat-697-million-monthly-active-users; "WeChat Breaks 700 Million Monthly Active Users," April 20, 2016, www.businessinsider.com/wechat-breaks-700-million-monthly-active-users-2016-4; Richard Macauley, "Facebook Already Has a Social Network in China—but Nobody Uses It," *Quartz,* January 14, 2015, http://qz.com/321788/facebook-already-has-a-social-network-in-china-but-nobody-uses-it/.

36 Michael Martina, "Business Groups Petition China's Premier on Cyber Rules," Reuters, August 11, 2016, www.reuters.com/article/us-cyber-china-business-idUSKCN10M1DN.

37 Eva Dou and Rachel King, "China Sets New Tone in Drafting Cybersecurity Rules," *Wall Street Journal,* August 26, 2016, www.wsj.com/articles/china-moves-to-ease-foreign-concerns-on-cybersecurity-controls -1472132575.

38 Jason Subler, "Major Powers Team Up to Tell China of Concerns over New Laws," Reuters, March 1, 2016, www.reuters.com/article/us-china-lawmaking-idUSKCN0W225P.

39 "Notification on Pre-Installed Green Web-browsing Filter Software," Ministry of Industry and Information Technology, June 10, 2009, www.china.com.cn/policy/txt/2009-06/10/content_17918230.htm; "What Is All the Debate about Filtering Software?" *Xinhua,* June 12, 2009, news.xinhuanet.com/politics /2009-06/12/content_11532769.htm.

40 Richard Koman, "US Developer: China's Green Dam Steals Our Code," *ZDNet,* June 13, 2009, www.zdnet .com/article/us-developer-chinas-green-dam-steals-our-code/; "US Company Sues China for Green Dam 'Code Theft,' " BBC, January 6, 2010, http://news.bbc.co.uk/2/hi/technology/8442771.stm.

41 Thomas Claburn, "U.S. State Dept. Condemns China's Green Dam Filter as Boycott Brews," *Information Week,* June 22, 2009, www.darkreading.com/risk-management/us-state-dept-condemns-chinas-green -dam-filter-as-boycott-brews/d/d-id/1080706.

42 Steve Mollman, "China Extends Deadline on Filtering Software," CNN, July 1, 2009, http://edition.cnn .com/2009/TECH/06/30/china.green.dam/.

43 Lincoln Davidson, "Journey to the East: Why Facebook Won't Make it in China," *Net Politics* (blog), Council on Foreign Relations, April 5, 2016, http://blogs.cfr.org/cyber/2016/04/05/journey-to-the-east-why -facebook-wont-make-it-in-china/.

44 Evan S. Medeiros, Roger Cliff, Keith Crane, and James C. Mulvenon, *A New Direction for China's Defense Industry,* chap. 5, " 'The Digital Triangle': A New Defense-Industrial Paradigm?" (Santa Monica, CA: RAND Corporation, 2005), www.rand.org/content/dam/rand/pubs/monographs/2005/RAND_MG334.pdf.

45 Adam Segal, *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age* (New York: Public Affairs, 2016), 138–41.

46 David E. Sanger and Nicole Perlroth, "N.S.A. Breached Chinese Servers Seen as Security Threat," *New York Times,* March 22, 2014, www.nytimes.com/2014/03/23/world/asia/nsa-breached-chinese-servers-seen-as-spy-peril.html; "Targeting Huawei: NSA Spied on Chinese Government and Networking Firm," *Spiegel,* March 22, 2014, www.spiegel.de/international/world/nsa-spied-on-chinese-government-and-networking-firm-huawei-a-960199.html.

47 Bill Bishop, "In China, a Push for Cleaner Air," DealBook, *New York Times,* June 17, 2013, http://dealbook.nytimes.com/2013/06/17/in-china-a-push-for-cleaner-air.

48 Gillian Wong, "Xiaomi Is Moving International Users' Data out of China," *Wall Street Journal,* October 23, 2014, http://blogs.wsj.com/digits/2014/10/23/xiaomi-moves-international-users-data-out-of-china/.

49 Caroline Hyde, "China's Huawei Backs Apple Stance in Phone Unlocking Dispute," *Bloomberg,* February 21, 2016, www.bloomberg.com/news/articles/2016-02-22/china-s-huawei-backs-apple-stance-in-phone-unlocking-dispute.

50 "China's Great Cannon," *The Citizen Lab,* April 10, 2015, https://citizenlab.org/2015/04/chinas-great-cannon/.

51 Diogo Costa, "Meet Gionee M6, the Smartphone with an Encryption Chip," *Engadget,* July 12, 2016, https://www.engadget.com/2016/07/12/meet-gionee-m6-the-smartphone-with-an-encryption-chip/; Conner Forrest, "Can an Encrypted Chip Make the Gionee M6 the Most Secure Android Phone Ever?" *TechRepublic,* July 12, 2016, www.techrepublic.com/article/can-an-encrypted-chip-make-the-gionee-m6-the-most-secure-android-phone-ever/.

52 Gerry Shih, "Huawei CEO Says Chinese Cybersecurity Rules Could Backfire," Reuters, April 22, 2015, www.reuters.com/article/us-huawei-services-idUSKBN0ND07320150422.

Adam Segal, “China, Encryption Policy, and International Influence,” Hoover Working Group on National Security, Technology, and Law, Aegis Series Paper No. 1610 (November 28th, 2016), available at https://lawfareblog.om/china-encryption-policy-and-international-influence.

About the Author

ADAM SEGAL

Adam Segal is the Ira A. Lipman Chair in Emerging Technologies and National Security, and Director, Digital and Cyberspace Policy. An expert on cyber security and Chinese domestic and foreign policy, his most recent book is *The Hacked World Order* (PublicAffairs, 2016).

Author Photo

http://www.cfr.org/content/bios/SegalPhotoBig_1.png
credit: David White

Jean Perkins Foundation Working Group on National Security, Technology, and Law

The Working Group on National Security, Technology, and Law brings together national and international specialists with broad interdisciplinary expertise to analyze how technology affects national security and national security law and how governments can use that technology to defend themselves, consistent with constitutional values and the rule of law.

The group focuses on a broad range of interests, from surveillance to counterterrorism to the dramatic impact that rapid technological change—digitalization, computerization, miniaturization, and automaticity—are having on national security and national security law. Topics include cyber security, the rise of drones and autonomous weapons systems, and the need for—and dangers of—state surveillance. The working group's output, which includes the Aegis Paper Series, is also published on the *Lawfare* blog channel, "Aegis: Security Policy in Depth," in partnership with the Hoover Institution.

Jack Goldsmith and Benjamin Wittes are the cochairs of the National Security, Technology, and Law Working Group.

For more information about this Hoover Institution Working Group, visit us online at http://www.hoover.org/research-teams/national-security-technology-law-working-group.

Hoover Institution, Stanford University
434 Galvez Mall
Stanford, CA 94305-6003
650-723-1754

Hoover Institution in Washington
The Johnson Center
1399 New York Avenue NW, Suite 500
Washington, DC 20005
202-760-3200

HOOVER INSTITUTION