COUNCIL on FOREIGN RELATIONS

March 13, 2020

China's Alternative Cyber Governance Regime

Prepared statement by

Adam Segal

Ira A. Lipman Chair in Emerging Technologies and National Security and Director, Digital and Cyberspace Policy Program
Council on Foreign Relations

Before the
U.S. China Economic Security Review Commission
March 13, 2020

Hearing on A 'China Model?' Beijing's Promotion of Alternative Global Norms and Standards

China's cyber governance regime is designed to achieve four goals. First, Beijing desires to maintain tight control over the flow of information to ensure domestic stability, regime legitimacy, and the continued rule of the Chinese Communist Party. Second, China wants to reduce security vulnerabilities in critical networks and defend the country against a range of cyber operations, including espionage as well as disruptive and destructive attacks. Third, Chinese leaders want to ensure technological autonomy, diminish reliance on foreign suppliers, and help Chinese companies dominate markets in emerging technologies. Finally, Beijing looks to expand its influence over cyberspace and limit the room for maneuver for the United States and its partners. Under President Xi Jinping, China has set itself the goal of become a "cyber superpower" and governance has shifted from being primarily focused inward to more actively projecting outward. In short, Chinese leaders decided that controlling the domestic internet was necessary but not sufficient. They would also have to shape the global internet.

To accomplish these goals, China has developed a matrix of interlocking cybersecurity strategies, laws, measures, regulations, and standards at home. Abroad, it has used diplomatic efforts to enshrine and expand the concept of cyber sovereignty in international organizations and forum. As described by President Xi at the 2015 World Internet Conference in Wuzhen, cyber sovereignty means "respecting each country's right to choose its own internet development path, its own internet management model, and its own public policies on the internet."[1] This position has been held out in contrast to the vision held by the United States and its partners that cyberspace should remain an open, global platform.

These multilateral efforts are bolstered by the Belt and Road Initiative and other tools of commercial diplomacy as well as the global activities of Chinese technology firms. Beijing also coordinates with the companies in efforts to define technology standards in pursuit of economic and political interests. The result of Chinese efforts will be a less open and less free internet. Beijing will strengthen the capacities of other states looking to block the flow of information and tighten their control over their populations. In addition, intelligence and cyber offensive gains will flow to China with the widespread adoption of Chinese technologies and standards. The domination of global information and communication technology markets by American technologies and standards certainly strengthened U.S. intelligence and cyber offensive capabilities. As former NSA director Michael Hayden once put it when justifying some of the agencies' intelligence gathering activities, "This is a home game for us. Are we not going to take advantage that so much of it [data] goes through Redmond, Washington? Why would we not turn the most powerful telecommunications and computing management structure on the planet to our use?"[2] Chinese intelligence and military agencies will certainly look to exploit familiarity with Chinese technology and standards in search of home field advantage.

Domestic Cybersecurity Governance

China's domestic cyber governance system consists of overlapping and interlinked strategies, laws, measures, regulations, and standards focused on critical infrastructure, data storage, security reviews, and the protection of personal data. [3] Launched in 2006, updated in 2018, and administered by the Ministry of Public Security (MPS), the Multi-Level Protection System ranks networks by sensitivity on a scale of one to five, with stricter security reviews as third-party certification and source-code delivery for networks ranked at higher levels. While the original version only covered government systems, the update of the MLPS covers all networks, private sector and foreign firms included.

The Cyber Security Law, which officially went into effect in June 2017, also includes a focus on what it terms critical information infrastructure (CII), but the definition of CII was initially unclear. Early documents identified sectors like "public communication and information services, power, traffic, water resources, finance, public service, and e-government," but following draft regulations added media, healthcare, and cloud computing and big data providers.

The Cybersecurity Law also requires the storage of "personal information" and "important data" inside of China, creating review procedures for transferring certain information out of China if it can "impact national security, damage public interest or is not fully secured." As with CII, the contours of what constitutes "important data" are uncertain and being set by follow up regulations. In addition, the Cybersecurity Law established a regime to review "critical network equipment and specialized cybersecurity products." Certification was required for 15 types of products, including routers and servers, to access domestic the market. Foreign companies such as Cisco, IBM, Juniper, Dell, and Siemens AG provided feedback to the Ministry of Industry and Information Technology (MIIT), which drafted this set of rules.[4]

While the Cybersecurity Law is the most authoritative law protecting personal information, Beijing is also in the process of building out a framework for user consent and the collection, storage, processing, and use of personal data.[5] The "Personal Information Security Specification" came into effect in May 2018, and includes requirements that data must be de-identified before sharing, imposes limits on "secondary uses" of data beyond the original purpose, and requires third-party vendors handling data to undergo security assessments.[6] Under its guidelines the Ministry of Industry and Information Technology has called out and fined hundreds of companies for apps and websites that excessively collected private data.

The bureaucratic lines of authority over cybersecurity and data protection are multiple and conflicting. The Cyberspace Administration of China, MIIT, and MPS as well as China Electronic Standards Institute, China Academy of Information and Communications Technology, and National Information Security Standardization Committee (TC260) all have some say over standards, regulations, and implementation. CSIS estimates TC260 has issued close to 300 standards related to cybersecurity since 2015.[7] Its membership was expanded from 48 members to 81 members, mainly Chinese officials and representatives of Chinese technology companies, though foreign companies have occasionally been allowed to participate in working groups. The committee's seven working groups are focusing on encryption, big data, and other cybersecurity issues.

The immediate impact of these overlapping jurisdictions and authorities is to create uncertainty for Chinese and foreign firms, as well as to impose cost through security audits and IP and source code submissions. An additional outcome of the standards framework is to bring companies under greater supervision and control. In the longer term, Beijing hopes that data privacy laws will increase trust in Chinese firms, helping them compete globally.

Domestic regulations shape global governance through two mechanisms. First, China does provide training to officials from the developing world in internet management and cybersecurity, and some countries have consciously tried to mirror Chinese regulations in their own laws.[8] In 2015, for example, Tanzania passed cybersecurity laws that resembled China's.[9] Second, there is a more indirect effect, as China can position itself, along with Europe, as having a robust governance model for data and security.

The Diplomacy of Cyber Sovereignty

China has promoted "cybersovereignty" as an organizing principle of internet governance, in direct opposition to U.S. support for a global, open, and secure internet. China envisions a world of national internets, with government control justified by the sovereign rights. Beijing also wants to weaken the bottom-up, private-sector-led model of internet governance, known as the multistakeholder approach championed by the United States and its allies. 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."[10]

While China endorsed the norms of responsible state behavior included in the 2013 and 2015 reports from the UN Group of Government Experts (GGE) on the Developments in the Field of Information and Telecommunications in the Context of International Security, it has resisted U.S. efforts to apply international law, especially the laws of armed conflict and the right of self defense, to cyberspace.[11] In 2017, the participating countries in the GGE failed to issue a follow-on report in part because China and Russia opposed language endorsing the right of self-defense.

In the wake of the failure to reach consensus, Russia proposed an Open-Ended Working Group (OEWG) to study the existing norms contained in the previous UN GGE reports, identify new norms, and study the possibility of "establishing regular institutional dialogue ... under the auspices of the United Nations." At the September 2019 meeting of the OEWG, the division between those supporting state sovereignty in cyberspace and those emphasizing an open, free, and secure internet was clear. In their opening statement, for example, the Chinese representative noted that it was "widely endorsed by the international community that the principle of sovereignty applies in cyberspace" and argued that the group "should enrich and elaborate on the specification of the principle, thus laying solid foundation for order in cyberspace."[12]

Beijing can also be expected to work in concert with Moscow in promoting a new UN cybercrime treaty. Russia has long wanted to replace the Council of Europe's Budapest Convention, which is the one international agreement subject to human rights safeguards that criminalizes computer crimes such as fraud and child pornography and prohibits illegal access and interception, data and system interference, and intellectual property theft. Although 64 countries have now signed the treaty, including Argentina, Australia, Japan, Turkey, and the United States, Moscow has consistently argued that the convention is only a regional agreement that violates principles of state sovereignty and non-interference. In December 2019, member states approved a Russian-backed resolution that established a committee of experts to consider a new treaty. In the run up to the vote, U.S. officials warned that the proposal was an opportunity for Russia, China, and others to create UN approved standards for controlling the flow of information, but large democracies such as Nigeria and India have found Russia and China's arguments on the need to fight cyber crime and terrorism convincing.[13]

Beijing also uses cyber sovereignty to reinforce its regional position and to bolster its leadership role in regional and developing country groupings. In 2015 the Shanghai Cooperation Organization submitted a Draft International Code of Conduct for Information Security to the United Nations General Assembly, which was an update of a code submitted by China, Russia, Tajikistan, and Uzbekistan in 2011.[14] The code call on states to agree that they will not "use information and communications technologies, including networks, to carry out hostile activities or acts of aggression, pose threats to international peace and security." The code also reaffirmed "that policy authority for Internet-related public issues is the sovereign right of States, which have rights and responsibilities for international Internet-related public policy issues." Similarly, the 2017 BRICS (Brazil, Russia, India, China, and South Africa) Leaders Declaration stressed "the paramount importance of the principles of international law enshrined in the Charter of the United Nations, particularly the state sovereignty, the political independence, territorial integrity and sovereign equality of states, non-interference in internal affairs of other states and respect for human rights and fundamental freedoms."[15]

BRI and Commercial Diplomacy

These multilateral efforts are bolstered by the Belt and Road Initiative (BRI) and other tools of commercial diplomacy as well as the global activities of Chinese technology firms. Chinese companies have played a large role in building the "digital silk road" in BRI countries, investing in cross-border optical cables and other communications trunk line networks, transcontinental submarine optical cable projects, and spatial (satellite) communication.[16] The large-scale investment in hardware is being followed up with increasing investment in e-commerce, cloud services, fintech, and big data.

This investment is being driven by bottom-up and top-down forces. Chinese companies are searching for new markets and customers while the government is providing support in pursuit of economic, strategic, and political goals. Beijing has provided credit lines to the companies as well as credit to BRI partners. China's Export-Import Bank financed 85% of the China-Pakistan Fiber-Optic Project, for example, and loaned to Nigeria the full cost of a Huawei-built 5G network.[17] The Mercator Institute estimates that China has made $7 billion in loans and investment in cables and telecoms networks, and over $10 billion on e-commerce and mobile payments systems, and more on research and data centers.[18]

Two sets of technologies—5G and surveillance—are at the center of competition over the future of cyberspace. Huawei equipment is now behind two-thirds of the commercially launched 5G networks outside China, although these networks may combine products from several suppliers.[19] ZTE and Huawei, leaders in 5G, are significant contributors to BRI. ZTE, for example, operates in over fifty of the sixty-four countries on the route of the Belt and Road Initiative. The two companies have training centers

in 9 African countries, for example, and Huawei is building Zambia's communications infrastructure from the ground up.[20]

Chinese companies are on the front lines of setting up smart cities that combine facial recognition and video surveillance with big data and advanced analytic capabilities, competing with suppliers from France, Germany, Israel, UK, and US. In addition, Chinese firms, led by Huawei, are the world's leading suppliers of AI surveillance technology used for public security.[21] Hikvision, for example, partnered with Zimbabwe's Nations Hardware and Electrical to implement broader CCTV coverage in the country, and Cloudwalk Technology Co. is providing facial recognition cameras and developing a national facial database.[22]

While Chinese companies often export these technologies to liberal democracies, their sales to developing countries put surveillance technologies in the hands of governments lacking their own capabilities, strengthening control over information and populaces. [23] Along with the hardware, Chinese firms also pass on training and techniques. According to reporting by the *Wall Street Journal* and *Associated Press*, Chinese technicians from Huawei worked with government security forces in Uganda and Serbia to install advanced facial recognition cameras for surveillance purposes. Embedded Huawei technicians also helped Ugandan and Zambian security forces intercept encrypted communications and use cell data to track opponents.[24]

As noted above, Chinese commercial diplomacy will lead to increased use of surveillance and internet filtering technologies by repressive regimes that lack their own technological capabilities. The on-the-ground presence of Chinese firms gives them influence over decisions on how tightly controlled the internet is in partner countries. There is also the possibility of the diversion of data back to China from countries along the BRI to enhance economic competitiveness and intelligence gathering. Many, for example, have pointed to the African Union's headquarters, built by the Chinese, reportedly sending confidential data back to China.[25]

Technology Standards

Beijing is expending significant effort to shape global standards in emerging technologies, especially 5G, AI, and the Internet of Things, believing they convey market and political influence. For example, as Jeffrey Ding, Samm Sacks, and Paul Triolo note, the New Generation Artificial Intelligence Development Plan has a large focus on standards-setting not only for technological interoperability but also for safety procedures and ethical norms of deploying AI-enabled systems.[26]

In recent years, as noted earlier, Beijing has issued hundreds of domestic standards, generally excluding foreign companies from participating in the process. Standards development is directed by the Standardization Administration of China, and research is often conducted in institutes linked to ministries. This state-led process contrasts with the European model of private actors coordinating under the auspices of national non-governmental organizations, and the American model, where there are more than 600 standards organizations, most of them industry associations.

Chinese technology companies have become more active and effective participants in international standards-setting forums. At the 3rd Generation Partnership Program, an international coalition of seven standards organizations working on 5G, representatives from Chinese companies and institutions reportedly have 10 of 57 chair and vice-chair positions.[27] Of the 200 participants in an International Telecommunications Union (ITU) study group on protocols for fixed and mobile networks, between 40

and 50 delegates were from Huawei.[28] ZTE, Huawei, Hikvision, and Dahua have submitted all of the surveillance standards—20 since 2016—to the ITU.[29]

China has also worked to expand its influence over international standard boards such as the ITU, the International Organization of Standardization (ISO), and the International Electrotechnical Commission (IEC). China, after France and Germany, has the third highest participation in IEC technical committees and holds 10 secretariats. At the ISO it has 79, and, though China holds no formal chairmanships of study groups at the ITU, representatives of Huawei, ZTE, China Telecom, China Mobile, Alibaba, and CAICT hold vice chairmanships.[30]

Beijing has made standards part of bilateral agreements and the BRI. Memorandums of understanding on standardization have been signed with Mexico, Vietnam, Myanmar, and Indonesia, and Chinese standards are likely to be adopted in many developing economies both because they are cheaper than Western alternatives and the draw of the Chinese market. Since 2015, China has also integrated standards work with the development of the BRI. The Action Plan for Standards Connectivity for the Joint Construction of the Belt and Road calls for uniform technical standards to be used across BRI. At a 2017 Belt and Road Forum, for example, China signed agreements on mutual standard recognition with 12 countries, including Russia, Cambodia, Malaysia, Switzerland, and Greece. By 2019, there were 85 agreements with 49 countries and regions.[31]

The ability to define international standards is a tool of both market and political influence. While European, Japanese, and U.S. companies have traditionally dominated global standards, Beijing is making a concerted push on the standards of emerging technologies such as 5G and AI. This is likely to increase the intelligence and cyber offensive capabilities of Chinese intelligence agencies and the People's Liberation Army. Chinese officials are certain to know of NSA's efforts to weaken the random number generator in the encryption standard Dual_EC_DRBG and alleged payments to RSA Security to include it in its BSAFE software library.[32] There is no reason to believe Chinese intelligence agencies will not try to do the same thing to Chinese standards.

Policy Recommendations

In order to push back against China's influence of global cyber governance, Washington must renew and reinvigorate its own cyber diplomacy. The State Department should move forward as quickly as possible with plans to create a Bureau of Cyberspace Security and Emerging Technologies headed by a Senate-confirmed assistant secretary of State, who would report to the Secretary of State or Deputy Secretary of State.

U.S. efforts should be focused on combatting Chinese efforts to promote cyber sovereignty through the United Nations and other international organizations. This would require a rethinking of the U.S. internet freedom agenda and a re-engagement with international organizations. In the wake of the interference in the 2016 election, the United States and its allies have increasingly called for online content moderation and other controls on disinformation. While Washington might stress that these processes occur transparently and through the rule of law, they do not look dissimilar to Chinese and Russian calls for cyber sovereignty to third countries who face similar pressures.

In the competition over 5G, the United States should offer countries alternatives to Huawei that can compete on price and efficiency. Through the U.S. International Development Finance Corporation, Washington should provide loans or loan guarantees for telecommunications equipment in developing economies. Washington also should work with allied governments to improve their cybersecurity,

developing shared standards for inspecting and deploying 5G equipment, similar to the joint statement issued by thirty countries in Prague, Czech Republic, in May 2019.[33] And it should invest in research in order to master both 5G technologies and the ones that will come after that. The federal government should fund several 5G R&D centers at universities in areas where the United States might lead, including security and merging communications, storage, and computation in 5G. Those centers should also begin research into 6G technologies that are likely to roll out fifteen years from now.[34]

The U.S. standards process is industry-led, and Washington should not re-create Beijing's top-down, national-plan approach. There are, however, technologies and international forums where American companies could use additional government support. The National Institute of Standards and Technology should do a comprehensive study and suggest standards dialogues for emerging technologies where the federal government can play a more active supporting role.

In addition, the Department of Commerce should work with major trading partners to promote the secure and free flow of data and the development of common technology standards. Washington and its partners should look for common principles on privacy that would allow for the secure, privacy-protected flow of data in the near term, with a longer-term goal of developing new multilateral agreements.

---

[1] Remarks by H.E. Xi Jinping President of the People's Republic of China at the Opening Ceremony of the Second World Internet Conference, December 16, 2015, http://www.fmprc.gov.cn/mfa_eng/wjdt_665385/zyjh_665391/t1327570.shtml.
[2] Michael Hirsch, "How America's Top Tech Companies Created the Surveillance State," *National Journal*, July 25, 2013, http://www.nationaljournal.com/magazine/how-america-s-top-tech-companies-created-the-surveillance-state-20130725.
[3] Paul Triolo, Samm Sacks, Graham Webster, and Rogier Creemers, "China's Cybersecurity Law One Year On," *DigiChina*, New America, November 30, 2017 https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinas-cybersecurity-law-one-year/
[4] Yuko Kubota, "American Tech Shudders as China Cyber Rules Are Expected to Get Tougher," *Wall Street Journal*, July 29, 2019, https://www.wsj.com/articles/chinas-cybersecurity-regulations-rattle-u-s-businesses-11564409177
[5] Mingli Shi, Samm Sacks, Qiheng Chen, and Graham Webster, "Translation: China's Personal Information Security Specification," *DigiChina*, New America, February 8, 2019, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinas-personal-information-security-specification/
[6] Samm Sacks, "China's Emerging Data Privacy System and GDPR," *CSIS Commentary*, March 9, 2020, https://www.csis.org/analysis/chinas-emerging-data-privacy-system-and-gdpr
[7] Samm Sacks and Manyi Li, "How Chinese Cybersecurity Standards Impact Doing Business In China," *CSIS Briefs*, August 2, 2018, https://www.csis.org/analysis/how-chinese-cybersecurity-standards-impact-doing-business-china
[8] He Huifeng, In a remote corner of China, "Beijing is trying to export its model by training foreign officials the Chinese way," *South China Morning Post*, July 14, 2018, https://www.scmp.com/news/china/economy/article/2155203/remote-corner-china-beijing-trying-export-its-model-training
[9] Jessica Chen Weiss, "Understanding and Rolling Back Digital Authoritarianism," *War on the Rocks*, February 17, 2020, https://warontherocks.com/2020/02/understanding-and-rolling-back-digital-authoritarianism/
[10] Adam Segal, "When China Rules the Web," *Foreign Affairs*, September/October 2018, https://www.foreignaffairs.com/articles/china/2018-08-13/when-china-rules-web
[11] Adam Segal, "Chinese Cyber Diplomacy in a New Era of Uncertainty," *Aegis Paper Series*, Hoover Institution, June 2, 2017, https://www.hoover.org/sites/default/files/research/docs/segal_chinese_cyber_diplomacy.pdf
[12] https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/09/china-submissions-oewg-en.pdf
[13] Ellen Nakashima, "The U.S. is urging a no vote on a Russian-led U.N. resolution calling for a global cybercrime treaty," *Washington Post*, November 16, 2019, https://www.washingtonpost.com/national-security/the-us-is-urging-a-no-vote-on-a-russian-led-un-resolution-calling-for-a-global-cybercrime-treaty/2019/11/16/b4895e76-075e-11ea-818c-fcc65139e8c2_story.html
[14] General Assembly, "International Code of Conduct for Information Security", UN document A/66/359, 14 September 2011; letter from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan addressed to the Secretary-General, "International Code of Conduct for Information Security", A/69/723, 22 January 2015.

[15] Full text of BRICS Leaders Xiamen Declaration, *Xinhua*, September 4, 2017, http://www.xinhuanet.com//english/2017-09/04/c_136583396_2.htm
[16] "Vision and Actions on Jointly Building Silk Road Economic Belt and 21st-Century Maritime Silk Road," Consulate-General of the PRC in Vancouver, April 4, 2015, http://vancouver.china-consulate.org/eng/topic/obor/.
[17] Andrew Kitson and Kenny Liew, "China Doubles Down on Its Digital Silk Road," CSIS, Reconnecting Asia Program, November 14, 2019 https://reconnectingasia.csis.org/analysis/ entries/china-doubles-down-its-digital-silk-road; and Don Weinland, "China State Banks Pull Back from Risky Overseas Projects," *Financial Times*, April 4, 2019, https://www.ft.com/content/273c324c-55ec-11e9-a3db-1fe89bedc16e
[18] Merics "Networking the Belt and Road- The Future is Digital," *Mercator Institute for China Studies,* https://www.merics.org/en/bri-tracker/networking-the-belt-and-road
[19] https://techcrunch.com/2019/06/25/huawei-wins-5g-contracts/
[20] "China's mighty Telecom footprint in Africa," *New Security Learning*, February, 11, 2011, http://www.newsecuritylearning.com/index.php/archive/75-chinas-mighty-telecom-footprint-in-africa; "Going global" in the growth markets – Chinese investments in telecommunications in Africa, Centre for Chinese Studies at Stellenbosch University, April 2012, http://www.ccs.org.za/wp-content/uploads/2012/04/Telecom_Policy-Briefing_final.pdf.
[21] Steven Feldstein, "When it Comes to Digital Authoritarianism, China is a Challenge — But Not the Only Challenge," *War on the Rocks*, February 20, 2020, https://warontherocks.com/2020/02/when-it-comes-to-digital-authoritarianism-china-is-a-challenge-but-not-the-only-challenge/
[22] Valentin Weber, *The Worldwide Web of Chinese and Russian Information Controls*, Open Technology Fund, September 17, 2019, https://public.opentech.fund/documents/English_Weber_WWW_of_Information_Controls_Final.pdf
[23] Steven Feldstein, *The Global Expansion of AI Surveillance*, Carnegie Endowment for International Peace, September 17, 2019, https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847
[24] Joe Parkinson, Nicholas Bariyo and Josh Chin, "Huawei Technicians Helped African Governments Spy on Political Opponents," *Wall Street Journal*, August 15, 2019, https://www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017
[25] Joan Tilouine and Ghalia Kadiri, "A Addis-Abeba, le siège de l'Union africaine espionné par Pékin, Le Monde, January 26, 2018, https://www.lemonde.fr/afrique/article/2018/01/26/a-addis-abeba-le-siege-de-l-union-africaine-espionne-par-les-chinois_5247521_3212.html
[26] "Chinese Interests Take a Big Seat at the AI Governance Table, *DigiChina*, New America, June 28, 2018, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinese-interests-take-big-seat-ai-governance-table/
[27] Newley Purnell and Stu Woo, "China's Huawei Is Determined to Lead the Way on 5G Despite U.S. Concerns," *Wall Street Journal*, March 30, 2018, https://www.wsj.com/articles/washington-woes-aside-huawei-is-determined-to-lead-the-way-on-5g-1522402201
[28] Maria Farrell, "Now Any Government Can Buy China's Tools for Censoring the Internet," *Medium*, December 5, 2019, https://onezero.medium.com/now-any-government-can-buy-chinas-tools-for-censoring-the-internet-18ed862b9138
[29] Anna Gross and Madhumita Murgia, "China shows its dominance in surveillance technology," *Financial Times*, December 29, 2019
[30] John Seaman, :China and the New Geopolitics of Technical Standardization," *Notes de l'Ifri*, January 2020, https://www.ifri.org/en/publications/notes-de-lifri/china-and-new-geopolitics-technical-standardization
[31] ibid
[32] Joseph Menn, "Exclusive: Secret Contract Tied NSA and Security Industry Pioneer," *Reuters*, December 20, 2013 http://www.reuters.com/article/2013/12/20/us-usa-security-rsa-idUSBRE9BJ1C220131220.
[33] Lenka Ponilkeska, "Countries Seek United 5G Security Approach Amid Huawei Concerns," *Bloomberg*, May 3, 2019, http://bloomberg.com/news/articles/2019-05-03/ countries-seek-united-5g-security-approach-amid-huawei-concerns.
[34] James Manyika, William McRaven, and Adam Segal, *Innovation and National Security: Keeping Our Edge*, Council on Foreign Relations Task Force, September 2019, https://www.cfr.org/report/keeping-our-edge/