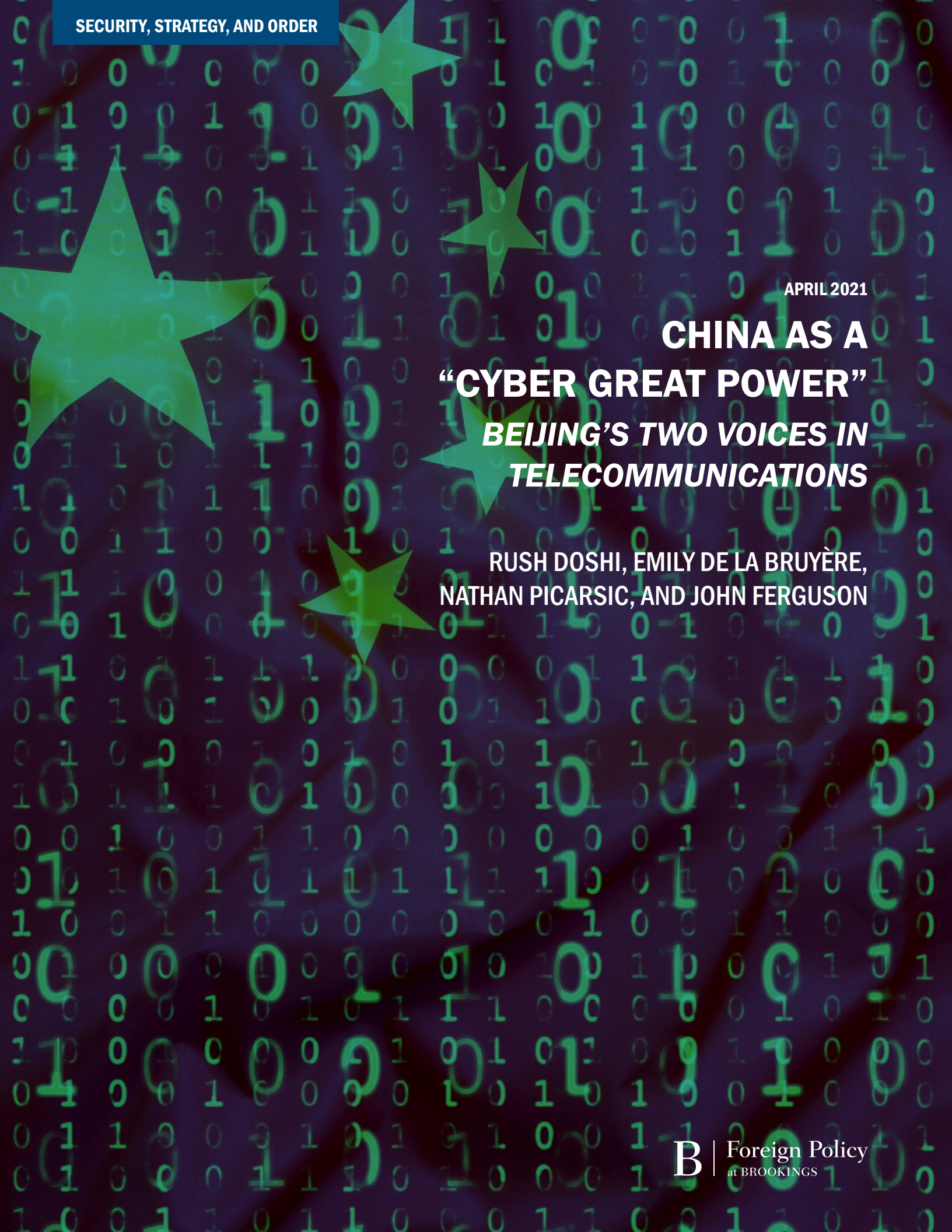

APRIL 2021

CHINA AS A "CYBER GREAT POWER"

BEIJING'S TWO VOICES IN TELECOMMUNICATIONS

RUSH DOSHI, EMILY DE LA BRUYÈRE, NATHAN PICARSIC, AND JOHN FERGUSON

B | Foreign Policy at BROOKINGS

CHINA AS A "CYBER GREAT POWER"

BEIJING'S TWO VOICES IN TELECOMMUNICATIONS

RUSH DOSHI, EMILY DE LA BRUYÈRE,
NATHAN PICARSIC, AND JOHN FERGUSON

EXECUTIVE SUMMARY

External Chinese government and commercial messaging on information technology (IT) speaks in one voice. Domestically, one hears a different, second voice. The former stresses free markets, openness, collaboration, and interdependence, themes that suggest Huawei and other Chinese companies ought to be treated like other global private sector actors and welcomed into foreign networks. Meanwhile, domestic Chinese government, commercial, and academic discourse emphasizes the *limits* of free markets and the dangers of reliance on foreign technologies — and, accordingly, the need for industrial policy and government control to protect technologies, companies, and networks. Domestic Chinese discourse also indicates that commercial communication networks, including telecommunications systems, might be used to project power and influence offensively; that international technical standards offer a means with which to cement such power and influence; and — above all — that IT architectures are a domain of zero-sum competition.

That external Chinese government and corporate messaging might be disingenuous is by no means a novel conclusion. However, the core differences between that messaging and Chinese internal discussion on IT remain largely undocumented — despite China's increasing development of and influence over international IT infrastructures, technologies, and norms. This report seeks to fill that gap, documenting the tension between external and internal Chinese discussions on telecommunications, as well as IT more broadly. The report also parses internal discourse for insight into Beijing's intent, ambitions, and strategy. This report should raise questions about China's government and commercial messaging, as well as what that messaging may obscure.

This report is motivated by China's growing influence in telecommunications and the growing controversy accompanying that influence. However, China's telecommunications resources, ambitions, and strategic framing are intertwined with those around IT more broadly. For that reason, this report reviews Chinese government, commercial, and academic discussion of both IT generally and telecommunications specifically. This report also contextualizes its analysis in terms of Beijing's program to become a

"cyber great power," also translated as "network great power," the blueprint for China' ambitions to leapfrog legacy industrial leaders and define the architecture of the digital revolution.

A new technological landscape is taking shape. China works to define that landscape. More than ever, it is imperative that China's ambitions be documented.

INTRODUCTION

In 2020, the Chinese telecommunications firm Huawei contacted a prominent Western periodical with a request: Would they publish a series of 10 articles in support of Huawei as the company grappled with Western pressure?[1] Huawei proposed a range of themes for those articles, including the company's purported respect for intellectual property; the benefits its government subsidies provided for the world; its role as a responsible actor with faith in market competition; and its status as an employee-owned company, independent from Chinese government influence. Huawei offered up its scientists and staff for interviews. It also suggested consultations with select non-Huawei voices. Huawei requested final review of the materials before publication.

> **External Chinese government and commercial messaging on information technology (IT) speaks in one voice. Its domestic counterpart reveals a radically different second voice.**

Efforts to shape public reporting are not uncommon among large companies, in China as elsewhere. Yet Huawei's is particular. It stands out for its confluence with a larger Chinese government bid to influence global discourse on telecommunications and information networks. And this messaging — on the part of company and government — contrasts starkly with domestic Chinese government, academic, and commercial discourse.

External Chinese government and commercial messaging on information technology (IT) speaks in one voice. Its domestic counterpart reveals a radically different second voice. Like Huawei's proposed articles, the former stresses free markets, openness, collaboration, and interdependence; themes that suggest Huawei and other Chinese companies ought to be treated like other global private sector actors and included in foreign networks. Meanwhile, domestic Chinese discourse emphasizes the *limits* of free markets, and, accordingly, the need for industrial policy and government control to protect technologies, companies, and networks; the danger of reliance on foreign technology; the competitive value of setting international standards; and, underlying it all, the inevitability of zero-sum competition in IT.

That external Chinese government and corporate messaging might be disingenuous is by no means a novel conclusion. However, the core differences between that messaging and internal discussion on IT remain largely undocumented — despite China's increasing development of and influence over international IT infrastructures, technologies, and norms. This report seeks to fill that gap, documenting the tension between external and internal Chinese discussions on telecommunications, as well as IT more broadly. The report also parses internal discourse for insight into Beijing's intent, ambitions, and strategy. This report should raise questions about China's government and commercial messaging, as well as what that messaging may obscure.

This report is motivated in particular by China's growing influence in telecommunications and by the growing controversy accompanying that influence. However, China's telecommunications resources, ambitions, and strategic framing are intertwined with those around IT more broadly. For that reason, this report reviews Chinese government, commercial, and academic discussion of both IT generally and telecommunications specifically. This report also contextualizes its analysis in terms of Beijing's program to become a "cyber great power,"[2] the blueprint for China's ambitions to leapfrog legacy industrial leaders and define the architecture of the digital revolution. The report advances several primary findings:

1. **While China repeatedly discusses its "cyber great power" ambitions internally, those are rarely acknowledged in outward-facing messaging.** The phrase "cyber great power" is a key concept guiding Chinese strategy in telecommunications as well as IT more broadly. It appears in the title of almost every major speech by President Xi Jinping on China's telecommunications and network strategy aimed at a domestic audience since 2014. But the phrase is rarely found in messaging aimed at external foreign audiences, appearing only once in six years of remarks by Foreign Ministry spokespersons. This suggests that Beijing intentionally dilutes discussions of its ambitions in order not to alarm foreign audiences.

2. **Even as the Chinese government encourages foreign audiences to purchase Huawei products, its leaders warn domestic audiences of the dangers that stem from reliance on foreign technology.** Years before the trade war and the Trump administration's restrictions on Huawei, Xi argued that "the control of core technology by others is our biggest hidden danger" and that allowing foreigners to control core technology "is like building a house on someone else's foundation."[3] He declared that "China must have its own technology, and it must have strong technology."[4]

3. **The Chinese government encourages foreign audiences skeptical of Huawei to adhere to market principles. At the same time, the government cautions domestic audiences that IT network development requires industrial policy and cannot be entrusted to market forces.** Xi has declared, explicitly, that "market exchange cannot bring us core technologies, and money cannot buy core technologies."[5]

4. **Beijing calls foreign security concerns over Huawei "lame excuse[s]" and pure "politics."[6] At the same time, China expresses similar concerns domestically over the incorporation of foreign technology into its networks.** Security is paramount for Xi, who has repeatedly declared that "without cyber security, there will be no national security."[7] Accordingly, he argues for adoption only of foreign technology that is "controllable" — while leaders at the Ministry of Industry and Information Technology (MIIT) stress that foreign technology networks tend not to be "controllable."[8] China must therefore build its own networks that are both "independent and controllable."[9]

5. **Commercial and academic Chinese sources suggest that the international community's security concerns over Chinese telecommunications might not be misplaced, and that Beijing might see telecommunications and other commercial networks as means to project offensive power globally.** Xi presents IT as a key part of China's military-civil fusion strategy: In 2018, he said that "military-civil fusion in cybersecurity and informatization is the key field and frontier field for military-civil fusion."[10] Downstream, Qin An, director of the China Institute of Cyberspace

Strategy, argued in 2016 that "due to the highly monopolistic nature of information technology systems, it is unlikely that there will be two different systems for military and civilian use … it is particularly necessary [for China] to integrate military and civilian resources through a military-civil fusion system."[11]

6. **When discussing standard-setting with foreign audiences, the Chinese government stresses win-win collaboration.** Yet domestic discussion emphasizes the competitive value of standards for establishing technological dominance and, correspondingly, the need to build "discourse power" in global IT development. Xi argues that in cyber security and telecommunications, the "game of great powers is not only a game of technology but also a game of ideas and discourse power," a reference to internet governance and standards.[12] Other sources build on Xi's language, noting that China works to set standards in 5G — and IT more broadly — in order to overtake the West, that doing so provides economic and military advantages. In short, those "who set the standards gain the world."[13]

This report begins with an overview of the strategic framing into which Beijing's telecommunications ambitions fit — the "cyber great power" concept, first presented by Xi in 2014, that entails sweeping ambitions to capture the Fourth Industrial Revolution. Informed by that framing, the next sections explore specific elements of Beijing's discourse on telecommunications and IT as well as the contrast between external and internal messaging therein. The first of them focuses on a relatively defensive element: The danger of dependence on foreign "core technologies," and the need for industrial policy, rather than reliance on market forces, to redress that danger. The next section turns to Chinese discussion of network and cyber security: On the one hand, Beijing's dismissal of foreign security concerns over Chinese systems and technologies; on the other Beijing's preoccupation with cyber and network security and the role that domestic inputs play in it; more pointed yet, suggestions that Beijing does in fact see international, commercial information networks as means through which to project offensive power. The final section explores China's standard-setting ambitions and corresponding bid for structural power.

A note on methodology

In assessing externally-facing discourse, the report relies primarily on official diplomatic statements and remarks by China's Foreign Ministry spokespersons. These are intended to reach foreign audiences.

For internally-facing discourse, the report turns to a wider range of sources including speeches and articles by Xi and other senior figures in the Chinese government directed at domestic audiences, as well as to dozens of authoritative journals affiliated with elements of the party-state ranging from the MIIT to the People's Liberation Army (PLA).

Sources that cannot be attributed to Xi himself must be considered less authoritative, and therefore to offer less explanatory value, than those with his imprimatur. Even within China's centralized government system, high-level officials are likely to reflect a diversity of views; even within China's relatively controlled high-level academic community (e.g., the Chinese Academy of Sciences), experts likely differ in elements of their analysis from government leadership. Despite these limitations, this report's authors consider such unofficial or less official sources critical for understanding Chinese competitive framings and ambitions. Xi himself is unlikely to speak in great detail about a specific technology or technological application. Officials at MIIT or the Ministry of Science and Technology might. High-level government officials, whose statements are subject to regular scrutiny,

are also unlikely to discuss sensitive topics (e.g., military applications of 5G), that more insulated academic and commercial sources do. And government statements tend to reflect policy as it has already formed; academic and commercial discussions can provide insight into the evolution of, and emerging trends in, relevant thought.

This report seeks to square the circle by vetting the authoritativeness of all sources used, providing context along the way. Authoritativeness of sources was assessed based on author, publisher, and the degree to which arguments echoed others strains of Chinese strategic discourse. This methodology does not assume that any single source has perfect explanatory value. Rather, the goal is to present a relatively comprehensive, candid collection of sources that together reflect China's strategic-level internal discourse on telecommunications and IT.

AMBITION: CHINA AS A "CYBER GREAT POWER"

"Building China into a 'cyber great power' is a long-term, complex, and systematic strategic project involving all aspects of the economy and society."

—Chen Zhaoxiong, deputy minister of the Ministry of Industry and Information Technology, 2017[14]

Xi introduced the concept of a "cyber great power" (网络强国), also translated as "network great power,"[15] in February 2014, at the launch of the Chinese Communist Party's highest-level body on internet issues: the Central Leading Small Group for Cybersecurity and Informatization.[16] Then, Xi framed becoming a "cyber great power" as the cornerstone of China's internet policy, a critical step toward achieving the party's centenary goals — key milestones the party hopes to reach by the centennials of its founding (2021) and its victory in the Chinese Civil War (2049).[17] The cyber great power concept has since become widespread in Chinese official discourse. It has emerged as a key framing for Chinese strategy in telecommunications and IT more broadly; the phrase "cyber great power" appears in the title of almost every major Xi speech on China's telecommunications and network strategy directed at domestic audiences since 2014.

However, the phrase rarely figures in messaging aimed at external foreign audiences. It appears only once in six years in remarks by Foreign Ministry spokespersons.[18] The sparse references to "cyber great power" in external messaging suggest that Beijing is intentionally minimizing the extent of its ambitions when communicating with foreign audiences. Such caution would not be unwarranted: Based on Xi's speeches and related officials' statements, this section finds that the cyber great power concept suggests precisely the sort of sweeping, competitive ambitions likely to raise foreign alarms.[19]

Xi is explicit that his is a global program: A cyber great power wields global influence. At the World Internet Conference in 2015, he declared that "China will vigorously implement a strategy to make China a cyber great power" including through construction of a "community of common destiny in cyberspace," global internet infrastructure, and appropriate internet governance norms.[20] Similarly, a 2017 article in the top party journal, Qiushi, by officials at the Cyberspace Administration of China (CAC)[21] describes deepening China's influence over global internet governance as a key goal in developing cyber great power status.[22]

This global cyber great power vision rests on a competitive orientation. Xi frames the information revolution as an opportunity to make up for China's relative disadvantage

in previous industrial revolutions. He suggests the cyber great power concept as the roadmap for doing so. In a wide-ranging 2016 speech, Xi explained the imperative of becoming a cyber great power in the context of China's humiliation in the Opium Wars and the country's failure to industrialize in the 20th century.[23] He noted that China had missed the Industrial Revolution, but would seize the information revolution. In this competition over cyberspace, according to Xi, "the winners will rejoice and the losers will collapse."[24]

Chinese officials have echoed that framing. For example, deputy minister of the MIIT Chen Zhaoxiong argued in a 2019 piece published in the Journal of Military-Civil Fusion in Cyberspace that the present is a moment of historic importance poised to shape the balance of power in global politics and economics — and, accordingly, a moment in which China has the opportunity to capture new power. "The current and future period is one of major strategic opportunity for China to move from a major manufacturing country and a major cyber country to a manufacturing great power and a cyber great power,"[25] he wrote. He offers larger strategic context: "Throughout the history of world civilization, every technological revolution and industrial change has brought incalculable effects and influences on human society, triggering a profound adjustment of the world economic and political structure." In those times of change, whoever can "grasp the historical trend" and "make the first move" can achieve "leapfrog development," seizing competitive advantages.[26]

In a 2017 piece in People's Daily, Chen also emphasized that the cyberspace contest is one of great power competition; that the cyber great power project hinges on Chinese victory in that competition. He explained that "cyberspace has become a new arena for major countries" and many "major countries in the world regard the internet as the strategic direction of future competition." As a result, they are "promoting and applying new generations of network information technology" and "competing for leadership in cyberspace."[27] China would not be an exception: In light of "increasingly fierce international competition, [China] must seize the new opportunities in this new era with a sense of urgency" and "accelerate the construction of new advantages in international competition" as well as cooperation in the digital age. China would have to "seize the commanding heights of technological competition related to the long term and to the overall situation."[28]

This logic — that the information revolution offers a competitive opportunity for China to leapfrog and, in doing so, ascend to the top of the global order — is borne out specifically in discussions of telecommunications. "5G has increasingly become a strategic commanding height to win the country's long-term competitive advantage," wrote Duan Weilun,[29] deputy director of the Office of the Leading Group for Comprehensively Deepening Reform at Datang Telecom Group, in a 2020 article.[30]

A 2020 article in Party & Government Forum, a journal run by the Party School of the Chinese Communist Party (CCP), is more direct: "Before the internet era, European and American countries had played a leading role in forming the new world economic order, political order, and legal order" but "in the era of the internet, especially in the new era of informatization pioneered by 5G, it is entirely possible for China to go ahead and make greater contributions." Nor does that piece leave doubt as to what China's contributions will entail: "In the internet era, whoever has the discourse power [话语权] and rule-making power [规则制定权] has the power to lead the future order [主导权]." From this perspective, 5G offers a "historic opportunity" for leadership in more than just

technology and a chance to "enhance China's international competitiveness" — despite having missed out on past, similar revolutionary shifts.[31]

INDIGENIZATION: DEPENDENCE AS CHINA'S "HIDDEN DANGER"

"The control of core technology by others is our biggest hidden danger."

—Xi Jinping, 2016[32]

If the ambition to become a cyber great power is muted in external messaging about China's digital plans, its constituent parts tend to be outright misrepresented. Beijing's emphasis on domestic core technologies, and the inadequacy of market mechanisms to protect them, offers an obvious and salient case.

In outward-facing messaging, Chinese government and commercial sources often argue that free markets, rather than politics, should determine the telecommunications landscape. For example, Foreign Ministry spokespersons frequently highlight to foreign audiences the importance of market principles in technology decisions. Several spokespersons have advocated that a "fair, just, open, and non-discriminatory business environment" is incompatible with restrictions on or concerns over Huawei.[33] Foreign Ministry spokesperson Hua Chunying noted in July 2020 that such restrictions "blatantly violated market economy principles and free trade rules" and the United Kingdom's decision to pursue them showed that the British "are against the international community."[34] In another press conference, she argued that "what the U.S. has done shows clearly that the market economy and fair competition principle it claims to champion is nothing but a fig leaf" and that U.S. behavior "violates rules of international trade."[35]

However, Xi's domestic-facing statements, as well as those of other figures in the Chinese government and commercial landscape, strike a different tone. They emphasize the importance, if not the primacy, of reducing dependence on foreign sources of core technology (核心技术) and the corresponding limits of free markets. Accordingly, they underscore the need to implement industrial policy. Such industrial policy is to focus on manufacturing and supply chains as well as on research and development. It is also to entail close collaboration between the government and private sector, in its domestic and international operations.

Xi has repeatedly stressed domestic strength and relative independence in core technology as key factors in cyber great power construction. He emphasizes as much while China exports technology that creates international reliance on it. In his very first major address outlining the concept of becoming a "cyber great power" in 2014, Xi underlined the need to reduce reliance on foreign technology as well as "to strengthen indigenous innovation (自主创新) of core technologies and infrastructure construction."[36] He argued that "to build China into a cyber great power, China must have its own technology, and it must have strong technology."[37] Importantly, that speech — and, with it, China's discussion of unraveling mutual technological dependence — preceded the election of Donald Trump, the trade war, and U.S. rhetoric that would come to be summarized by a focus on "decoupling."

Xi elaborated on his core technology focus in a major 2016 internet policy speech, also before the U.S. election. In that speech, Xi offered a broad definition of "core technology": "In my opinion, it can be grasped from three aspects. One is basic technology and general technology; the second is asymmetric technology, or 'assassin's mace' technology; the

third is cutting-edge technology and disruptive technology."[38] In a notable addendum, Xi stated that the key is that "in these fields, we are on the same starting line as foreign countries. If we can deploy ahead of time and focus on research, it is very possible to realize the transformation from running behind others to running ahead of others and leading."[39] In other words, core technology elements are identified not only for their foundational nature, but also for China's present competitive status in them, and the potential it grants China ultimately to lead.

Despite that favorable overall prognosis, Xi pointed elsewhere in the speech to China's lingering technological deficiencies. "When compared with the world's advanced level and when compared with our strategic goal of building ourselves into a cyber great power, we still have a gap in many aspects," he said, adding: "The biggest gap lies in core technology."[40] He stressed the accompanying dangers. "The core technology of the internet is our biggest 'major artery,'" Xi declared, employing a phrase (命门) which refers to the vital area of the body responsible for respiration, digestion, reproduction.[41] "The control of core technology by others is our biggest hidden danger."[42]

It would therefore be essential for China to strengthen its core technology. "If we want to grasp the initiative in China's internet development and ensure internet security and national security, we must break through the core technology problem and strive to achieve 'overtaking on the curve'[43] in certain fields."[44] Xi justified this claim in language that applies as much to foreign dependence on China as it does to China's dependence on others:

> No matter how large an internet company is, no matter how high its market value is, if it is heavily dependent on foreign countries for its core components, and if the "major artery" of the supply chain is in the hands of others, it is like building a house on someone else's foundation. No matter how big and beautiful it is, it may not stand up to wind and rain, and it may be so vulnerable that it collapses at the first blow.[45]

To this end, Xi called for a robust industrial policy. China would have to "invest more human, material, and financial resources in core technology research and development" as well as to "gather our best forces and make strategic arrangements" for moving ahead. China would have to "formulate an outline for the development strategy for core technology and equipment in the information field" and "formulate a roadmap, timetable, a list of tasks, as well as near-term, mid-term, and long-term goals." And China would have to "closely focus on climbing up to the strategic commanding heights."[46]

Xi proposed that China do so according to a sort of middle ground between the absolutes of outright protectionism[47] and free market integration.[48] "Core technology is the country's important weapon, and the most critical and core technology must be based on indigenous innovation and self-reliance," he declared. The free market would not be sufficient. "Market exchange cannot bring us core technologies, and money cannot buy core technologies. We must rely on own research and development." Yet at the same time, in a globalized environment such research and development could not be expected to take place "behind closed doors." Xi explained that "only when we fight against masters can we know the gap" in ability.[49] China "would not reject any new technology." Rather, it would strategically determine "which ones can be introduced [from abroad], digested, absorbed, and then re-innovated" versus "which ones must be indigenously innovated on their own."[50]

Xi further clarified that China's industrial policy would guide and support supply chains and the manufacturing base, as well as research and development. He explained that

without a solid manufacturing base for core technologies, capacity would be "a waste of work;" that "in the global information field, the ability to integrate innovation chains, production chains, and value chains has increasingly become the key to success or failure;" and that doing so requires that "the final result of technology research and development in core technology should not only be technical reports, scientific research papers, and laboratory samples but should [also] be market products, technical strength, and industrial strength."[51] In other words, scientific research would only yield sufficient returns when supported by supply chains and manufacturing strength.

Both in its domestic and its international application, this industrial policy would require close collaboration between Chinese government and corporate players. Xi explained in his 2016 speech that while "the fate of [technology] enterprises is closely related to the development of the country," private companies also need the state. "Without state support, without the support of [China's] masses, without serving the country and the people, it is difficult for enterprises to become stronger and bigger."[52] State support would extend to companies' foreign operations: As Xi argued in 2016, "we must encourage and support China's internet companies to go global … and actively participate in the construction of the 'Belt and Road' so as to achieve the principle of 'wherever our national interests are, [our] informatization [technology] will also cover those areas.'"[53] Xi has yet to address the question of whether these global ambitions create for the rest of the world the dangerous dependencies on foreign — in this case Chinese — technology that Beijing is so intent on redressing at home.

A 2019 article by Chen Zhaoxiong is particularly pointed on the deficiencies of market forces when it comes to developing core technology, and therefore on the need for industrial policy. "Money and the market," writes Chen, neither "brought the core technology of an operating system" nor allowed that technology to be "digested, absorbed and re-innovated." China therefore had no choice but to support "indigenous innovation" to "build a safe and controllable information technology system."[54]

Other Chinese sources apply this framing directly to 5G. For example, a 2017 article in the MIIT-affiliated journal Communications World encourages the government to "coordinate operators and related departments to efficiently deploy a national experimental plan to prepare for 5G commercial use," a plan that China ultimately began implementing in 2020.[55] Similarly, authors from Shanxi University argued in a 2020 International Economics and Trade journal article that building out a 5G industry requires "top-level design" from the country's national administrative departments and that the government must "provide financial support too." They attribute this to the "long-term development and exploration, costing huge amounts of money" required of high-tech industries like 5G. In other words, "the state conducts top-level design at the strategic level and uses industry support funds rationally."[56]

CYBER AND NETWORK SECURITY: "BOTH OFFENSIVE AND DEFENSIVE"

"Without cyber security, there will be no national security."

—Xi Jinping, 2014[57]

Chinese external messaging on cyber and network security also downplays the risks that foreign technologies, like Huawei's, might present in information systems. However, domestic Chinese government discourse prioritizes security — and presents

"independent and controllable"[58] IT systems as a means to achieve it. One beat further, Chinese academic and commercial discussions of offensive applications of information networks suggest that security concerns over Chinese systems are well justified. Beijing might see commercial telecommunications and other IT networks as vehicles through which to project military power, as well as to shape the global system and narrative in its interests.

Beijing might see commercial telecommunications and other IT networks as vehicles through which to project military power, as well as to shape the global system and narrative in its interests.

Foreign Ministry spokesperson Hua Chunying has described cyber and network security concerns as examples of countries "politicizing commercial and technological issues at all costs." She claimed in 2020 that restrictions on Huawei "are not about national security, but political manipulation."[59] More explicit yet, Hua has also said that "'promoting national security' is such a lame excuse cited by the U.S. side," and that foreign concerns are driven by politicized, "non-existent risks"[60] based on having "overstretched the concept of national security."[61]

Independent, controllable technologies for cyber and network security

If the United States has overstretched the concept of national security, Beijing's domestic-facing discourse suggests that it is guilty of the same. Such discourse stresses the critical importance of security in information networks, calling for adoption of independent, controllable technologies. In the same 2014 speech in which Xi introduced the concept of a "cyber great power" and launched a small leading group tasked with implementing that objective, he declared, "without cyber [or network] security,[62] there will be no national security."[63] He also introduced a phrase that has become a mainstay of China's discourse on telecommunications. "Cybersecurity and informatization are two wings of one body, and two wheels of one engine," he said. "They must be planned, deployed, advanced, and implemented in a unified manner."[64] In other words, security stands at the core of China's digital ambitions. This integral role of security in "cyber great power" construction is a near-constant in Xi's major speeches on the subject.[65]

Discussion downstream from Xi's remarks applies this emphasis on security specifically to telecommunications. Researchers at the Investigation Technology Center of the Political and Legal Committee of the Central Military Commission (军委政法委侦查技术中心) stress security in 5G:

> As today's advanced communication technology, 5G's wide application will bring new changes to the production and life of the entire society. The security issues of related technologies and applications are related to social public security and military interests and should be included in the key considerations from the perspective of overall national security.[66]

Domestic Chinese discourse points to "controllable" (可控) technologies and systems as a means of achieving security. In 2016, Xi explained that China should consider whether technologies are "secure and controllable" before introducing them.[67] Also in 2016, he said that China must "build a secure and controllable information technology system."[68]

Other sources more sharply emphasize the imperative of domestic technologies. In a 2019 article in the journal Military-Civil Fusion in Cyberspace, Chen Zhaoxiong argued

that China had to "build a secure and controllable information technology system," and do so through "indigenous innovation."[69] In a 2015 article, a researcher at the Shanghai Academy of Social Sciences explained the security risks of reliance on foreign technologies in IT: "We started late in information technology, relying on Western technologies for core technologies like chips, operating systems." This created a vulnerability: "Western countries, led by the United States, take advantage of the technological industry to develop and customize various cyber-attack weapons to achieve cyber surveillance, cyber-attacks, and cyber deterrence." He concludes: "If the core technology is not independent and controllable, the network we build will be an 'unprotected network.'"[70]

Militarized information technology networks

At a next level, analysis of academic and commercial sources indicates that foreign security concerns over Chinese technologies and systems might not be misplaced — that Beijing might see commercial and civilian IT networks as tools through which to project offensive power.[71] That power projection can take many forms. At the most traditional level, Chinese discourse is rife with discussion of information networks, including telecommunications, as military-civil fusion systems, as well as of 5G's military applications.

Military-civil fusion refers to the integration of military and civilian resources, actors, and positioning in pursuit of a unified goal.[72] Xi elevated military-civil fusion to national-level strategy in 2015.[73] He has frequently underlined the key place of IT within that strategy: At the National Cybersecurity and Informatization Work Conference in 2018, Xi said: "Military-civil fusion in cybersecurity and informatization is the key field and frontier field for military-civil fusion, and it is also the most dynamic field and the field with the most potential for advancement in military-civil fusion."[74]

Downstream Chinese discussions are even more explicit about the relationship between information networks and military-civil fusion, suggesting that commercial networks can serve military purposes. For example, Qin An argued in 2016 that "due to the highly monopolistic nature of information technology systems, it is unlikely that there will be two different systems for military and civilian use" and the two systems will in actuality be one system. Moreover, given China's "current technological foundation … it is an arduous task for China to build a system" that can rival the world's advanced standard. Therefore, "it is particularly necessary [for China] to integrate military and civilian resources through a military-civil fusion system."[75]

In this same vein, Duan Weilun called in 2020 for China to "strengthen the basic common technologies of the 5G network system for both military and civilian use, support the in-depth development of military-civil fusion of 5G and its technological evolution, and promote the large-scale application of 5G autonomous and controllable technologies in military equipment."[76]

An article in the journal National Defense by researchers from the Academy of Military Science took the fusion idea one step further. The authors propose that "the military application of 5G technology should follow the evolutionary laws of informatization," which include the "global penetration" of 5G technology and "comprehensive linkage" between military and civilian capabilities. Accordingly, they argue that China's construction of 5G should build "a close connection between peacetime and wartime."[77]

These framings suggest that Chinese approaches to 5G and other information networks, as well as to the technologies and applications built on top of them, might incorporate

military utility from the point of design. Additional sources offer insight into specific military implications.

Information capabilities lie at the heart of China's military modernization program.[78] As Zheng Anqi of the China Academy of Information and Communications Technology put it in 2020, "if modern military forces have strong information power, they have strong military power."[79] According to Zheng, the military must "grasp the theme of the era in the military field of information as the country implements the network power strategy, absorb and learn from brand-new information technologies and concepts, and leverage the development 5G technology to use the Internet of Things, big data, and cloud computing."[80] Zheng concludes: "The foundation of an information force is the network. Without the support of ubiquitous, broadband, and mobile networks, a powerful information army is just empty talk."[81] Similarly, researchers at the Academy of Military Sciences explained, also in 2020, that China "will give full play to the capabilities of future communication technologies — including large connections, low latency, high bandwidth, and wide coverage — to provide more powerful scientific and technological support for our military's intelligent combat system."[82]

A 2019 article in China's National Defense journal by military officers and permanent faculty at the Academy of Military Sciences offers a powerful summary of 5G's military applications. They write that "5G technology has strong military application value. It is of great strategic significance to seize the opportunity of military applications of 5G technology."[83] In sweeping terms — touching on both China's military-civil fusion strategy and informatization of the military — they argue that "the fifth-generation mobile communication technology (5G technology) is a new engine for the upgrading of the network-information military-civil fusion industry, and a new support for a strong military through information."[84] And the authors indicate that the military value of 5G is to be used for offensive ends, noting that China must "carefully study and comprehensively demonstrate and formulate our army's 5G technology development strategy for defeating the enemy."[85]

Those authors detail a series of use cases for 5G. First, battlefield interconnection and command and control: They note that China's military seeks "the comprehensive integration of networked systems." In practical terms, this goal is to "integrate joint operations [across] three-dimensional information networks of land, sea, air, and space," with "every combat unit and even weapons platform, sensor, and other combat equipment … connected safely, quickly, and seamlessly." These goals are longstanding, but the authors stress that 5G provides the necessary capabilities to operationalize this vision of an interconnected battlefield: "5G technology provides technical conditions for the interconnection of various weapons systems, information systems, and command and control systems." [86]

Second, advanced military tools: The National Defense journal authors outline a wealth of possibilities — ranging from "projected virtual holographic images," military Internet of Things, and military robots — that 5G might make feasible.[87]

Third and more broadly, battlefield communications: "Various mobile terminals can directly use 5G communication networks for encrypted data communication, providing the military with 'wide coverage, high speed, and strongly compatible'" integrated communication on the battlefield. These mobile terminals can be integrated with more traditional military networks and equipment — including "military communication satellites, early warning aircraft, and other resources" — such that "communication achieves almost unimpeded effects, which can significantly reduce the cost of military operations."[88]

A 2019 article in the journal Business Observation by the general manager of China Telecom's cloud computing branch also argues that "from a military perspective … 5G's qualitative leap in transmission rate and stability allow it easily to meet the needs of future battlefield communication tasks."[89] 5G networks could even be used to support a globally deployed PLA:

> Once the 5G communication system is deployed globally, it will have the same or even stronger service capabilities as military communication systems. In addition to accessing military tactical communication networks, various military mobile terminals can also directly use 5G communication networks for encrypted data communication, providing the military with integrated air-ground backup communication capabilities, which can greatly enhance the battlefield's informatization support capabilities.[90]

Experts at the Academy of Military Sciences added logistics as another military application in a 2020 article: "5G technology is bringing about changes in models, efficiency improvements, and economic benefits in the field of civilian logistics. It can be foreseen that it will play a key supporting role in the construction of our military's intelligent logistics."[91]

Sun Bolin of the Expert Advisory Working Committee of Chinese Society of Automation summarizes the value of these military applications in a 2020 piece, describing a scenario for 5G-enabled war that emphasizes the threat of a militarized telecommunications network:

> When the war has just begun, 5G technology could completely paralyze the opponent's command and control system and logistics support system. With the battle not yet started, the outcome has already been known. 5G communication technology will provide the military with an integrated air-ground information communication network with wide-area coverage, high-speed transmission, and strong compatibility, thereby greatly improving the battlefield's information support capability.[92]

Information networks and a new type of security threat

The nature of 5G-enabled power projection extends well beyond traditional security domain. Chinese discussion of cyber and network security derives from a broad framing of what precisely security entails and the vulnerabilities that IT creates. Economic, social, and informational domains figure alongside the military domain in this conception of network and cyber security. In those fields, information networks can be used to influence, coercively or for destructive ends, as well as to conduct direct attack — as, for example, through the proliferation of propaganda or by shaping capital markets.

Chen Baoguo of the State Council's International Institute of Technology explained in a 2010 article that the increased exposure to outside players brought about by advances in IT risked circumscribing a state's sovereignty:

> The new generation of information technology revolution has … increased mutual penetration and interdependence among countries … It has become difficult for countries to enjoy their sovereignty in internal affairs, diplomacy and military in the traditional and absolute way. Therefore, in the era of informatization and economic integration, the decision of any country can hardly be its own decision. In the era of the

> new generation of information technology revolution, the absolute sovereignty and independence a country traditionally enjoyed is increasingly eroded and weakened, internally and externally, by the new generation of information technology.[93]

In support of his point, Chen outlines the dependence of national and social systems on information networks and, accordingly, the vulnerability those networks create:

> A new generation of information technology revolution has made national security issues no longer limited to traditional military and economic security. The entire society is becoming more and more dependent on the internet. The development of a new generation of information technology revolution has become the backbone of the 21st century society and the internet has become the nerve center of a country. The financial, commercial, transportation, communications, education, and health care systems that operate through the internet have become the basis for national economic and social development.[94]

In short, information networks expand the domain of contestation and connection, thereby expanding vulnerability. A network attack can threaten the "financial, commercial, transportation, communications, education, and health care systems that operate through it."[95]

Information networks expand the domain of contestation and connection, thereby expanding vulnerability.

Other sources move beyond framing the areas of vulnerability created by networks to explore the types of threat posed within them. Notably, they point not simply to direct confrontation, but also to influence — to the risk that information systems might be used to shape national affairs in a manner that impinges on national security and autonomy. Liu Honglin of the Shanghai Municipal Party School of the Chinese Communist Party warned in 2011 of the "cultural penetration, ideological infiltration, and political infiltration" that IT could permit:

> In the information age, there are multiple cultures and many ideas. Western countries use the advantages of information technology to carry out cultural penetration, ideological infiltration, and political infiltration, in order to achieve political objectives. This will undoubtedly affect the Party's ideology and ideological foundation. Moreover, the information network has broken the top-down, one-way communication of traditional media. If opened to an even greater interactive information environment, how does our Party uphold and develop Marxism, resist the influence of thoughts, and strengthen the appeal of the Party's ideology?[96]

Similarly, a National Social Science Fund Project published in 2020 describes the danger of ideological subversion and "cultural erosion" that emerges from 5G and other new, cross-border technological systems: "In the new era, with the innovation and application of new technologies represented by AI and 5G … national cultural security is faced with multiple challenges such as insufficient innovation in cultural theory, weakness of mainstream ideology dissemination, and weak capacity to resolve the erosive impact of Western culture." In response, the report argued, "our country should, from the height of the national security macro strategic plan … build a national cultural security guarantee system of 'internal and external linkage' (内外联动), 'both offensive and defensive' (攻守兼备)."[97] That idea of fusing offense and defense might indicate that Beijing intends

not only to protect against outside influence exerted through information networks, but also to use them to project its own.

In 2020, Foreign Ministry spokesperson Zhao Lijian suggested that for other countries to use Huawei equipment would prevent U.S. espionage: "The reason why the United States suppresses Huawei may be because it is worried that if other countries use Huawei, the United States will no longer be able to go through the 'back door' and engage in eavesdropping."[98] That line acknowledges the security leverage that can be claimed through foreign information networks. It also begs the question of how that security picture evolves when such leverage is claimed by a player that sees commercial networks as battlefields for military and ideological confrontation.

A 2017 article by Long Zaiye, a researcher at the Cyberspace Military-Civil Fusion Strategy Forum, offers a compelling portrait of China's fused offense and defense in network and cyber security:

> On its journey from a major cyber power to a cyber great power, China has for a long time been engaged in arduous struggles with various opposition forces. We need to … coordinate network security issues and recognize that the internet has brought enemies and the battlefield closer. With the current background of the times, we have won the overall battle against contradictions and conflicts, eliminated obstacles … and effectively responded to the public security issues of the information society with the network inspection model. The specific implementation focuses on three aspects: First, the global target survey. Dragnet-style reconnaissance screening and cluster analysis are carried out on networked targets on a global scale, and temporary safety areas and key inspection areas are designated. The second is detailed investigation of hostile targets. For national targets that have listed [China] as a major strategic opponent or have experienced hostilities, we will conduct key inspections and conduct random inspections to identify them. The third is the verification of combat objectives. Maintain regular inspections of countries, companies, or personal goals that may pose a danger to [China], and reserve the ability to fight for destruction at any time.[99]

STANDARD-SETTING: CHINA'S SEARCH FOR "DISCOURSE POWER"

"At present, the cybersecurity game of the great powers is not only a game of technology, but also a game of ideas and discourse power."

—Xi Jinping, 2016[100]

Information technologies offer a subtler, more systemic form of power projection as well: standard-setting. Chinese internally-directed discourse suggests competitive ambitions to set international technical standards for the sake of increasing global power.

That framing is entirely absent from foreign-facing discussion. Beijing's outward messaging presents standard-setting as a mutually beneficial domain and calls for cooperation and joint rule development within it. For example, in discussing the Global Data Security Initiative in 2020, Foreign Ministry spokesperson Zhao Lijian claimed that China sought to "provide a blueprint for formulating global standards," leaning on inclusive concepts of "mutual respect and shared governance," efforts to "build mutual trust and deepen cooperation," support for "multilateralism," and new ways to "work together with others." Zhao declared that "extensive consultation and joint contribution

for shared benefits is the right way forward" if China is to build "a community with a shared future in cyberspace."[101] Similarly, a 2016 article in People's Daily argues that "China and the United States need network cooperation rather than confrontation … win-win cooperation and jointly to explore network codes of conduct."[102]

China's internally-facing discourse tells a different story. Standard-setting emerges as the means to lead, or even dominate, future technology — and, in doing so, to lead, or dominate, the emerging world order. Standards are consistently framed as zero-sum, competitive, and instruments of national power. Decidedly different from the Foreign Ministry's public line, a 2015 article in the Zhejiang Daily by then-deputy director of the Policy Research Office of the Zhejiang Provincial Party Committee provides a succinct example of the competitive, strategic value China assigns standards:

> Under the conditions of economic globalization and modern market economy … Standards are the commanding heights, discourse power, and the power to control. Therefore, "the one who obtains the standards gains the world" ("得标准者得天下"), and "the first-rate enterprises sell standards. Second-rate companies sell-brands, and third-rate companies sell products" ("一流企业卖标准、二流企业卖品牌、三流企业卖产品").[103]

The highest levels of the party — including Xi — have echoed this emphasis on standards. They have also outlined a government role in leading the technical standard-setting effort. In 2016, Xi declared that China would "actively implement a standardization strategy,"[104] an effort to strengthen and export Chinese technical standards.[105] "We must accelerate the promotion of China's international discourse power and rule-making power in cyberspace and make unremitting efforts towards the goal of building a cyber great power," he said then.[106] In March 2018, Beijing launched the China Standards 2035 project, led by the Chinese Academy of Engineering.[107] After a two-year research phase, that project evolved into the National Standardization Development Strategy Research in January 2020.[108] The "Main Points of Standardization Work in 2020" issued by China's National Standardization Committee in March 2020 outlined intentions to "strengthen the interaction between the standardization strategy and major national strategies."[109]

Nor does domestic Chinese discourse suggest that the standard-setting process is to be a collaborative one. A director at the Chinese Academy of Sciences noted in 2016 that the various "principles" put forward by Xi for governing cyberspace "will also be recognized by all countries in the world and will become the basic norms for internet governance in all countries."[110]

China's standardization ambitions extend across fields. They apply to high-speed rail as well as to telecommunications. Yet Beijing appears to place particular emphasis in emerging domains — areas where global standards are still being set, and therefore where China has the opportunity to leapfrog incumbents.[111] For example, the Main Points for National Standardization Work in 2020 outline efforts in emerging industries (e.g., intelligent manufacturing, new energy and energy efficient transportation systems, advanced materials); emergent priorities (e.g., COVID-19 prevention and control technology); biotechnology (e.g., bio-based materials and advanced medical equipment); service infrastructure (e.g., e-commerce, finance, social credit, and logistics); and information technology (e.g., the Internet of Things, cloud computing, big data, 5G, smart cities, geographic information).[112]

As that taxonomy suggests, 5G and information technology more broadly play a central role in China's standard-setting agenda. The Chinese government supports and organizes the promotion of telecommunications standards. Xi declared in 2016 that China will "promote the reform of the global internet governance system," both via existing institutions like the United Nations and through new, Chinese-led mechanisms like the Belt and Road Initiative and subordinate banners like the Digital Silk Road.[113] Zhao Dachun, a representative to the National People's Congress and deputy general manager of China Mobile, made the state's central role in organizing and promoting telecommunications standards clear in 2018. "In terms of 5G standard determination, spectrum allocation, license issuance, technical verification, and industrial promotion," he declared, "the government and relevant departments will carry out top-level design and provide relevant policy support to accelerate the development of the 5G industry."[114]

In another reflection of the state's role in standard-setting and emphasis on 5G, Tong Guohua, chairman and secretary of the Party Committee of China Information and Communication Technology Group, promised in 2018 that "for the future industry development direction, we follow the instructions of General Secretary Xi and the strategic deployment of the State-owned Assets Supervision and Administration Commission of the State Council to form six industrial layouts, namely focusing on 5G standards," among others.[115]

In a 2020 article, Duan Weilun described the success of this approach:

> After years of efforts of following [others] in 2G, catching up in 3G, synchronizing [with others] on 4G, China has entered the first camp of 5G development in the world and taken the lead in technological innovation. Chinese enterprises have fully participated in the formulation of international 5G standards, strengthened 5G international cooperation, and worked with international enterprises to promote the formation of a global unified 5G standard.[116]

Duan supports the claim with empirics: "As of April 2019, the number of SEP (Standards-Essential Patents) applications for 5G communications systems by Chinese companies ranked first in the world, accounting for 34%."[117] Key actors filing those applications were Huawei, ZTE, and the Institute of Telecommunications Science and Technology.[118] Duan then proceeds to present lines of effort through which China might further its standard success, calling on Chinese companies to engage the International Standardization Organization, International Electrotechnical Commission, and International Telecommunications Union, to "actively participate in the formulation of 5G and other new-generation information technology network security international standards … and further enhance China's international voice and influence in the formulation of international network space security standards."[119]

Chinese discourse clearly describes global, competitive ambitions underlying this state-led effort to shape telecommunications standards. A 2019 article by authors at the Academy of Military Sciences[120] in China's National Defense journal offers a clear summary of the stakes:

> The core technology of 5G is almost completely new. Whoever masters the model, architecture, and standards of 5G technology first has the right to speak in the future mobile network and the first-mover advantage of the industry chain. They can occupy a strategic leading position in future economic trade and military competition.[121]

Those lines suggest that only one player will be able to claim this "strategic leading position." The point is made more explicitly elsewhere. Shenzhen Commercial Daily called 5G "winner-take all" (赢家通吃) in 2019.[122] Miao Wei, head of the Ministry of Industry and Information Technology, himself has endorsed this argument. In a 2020 speech, Miao Wei said that "there were three global standards in the 3G era, two global standards in the 4G era, and one unified global standard in the 5G era."[123]

Why are these winner-take-all 5G standards so strategically important? In part, argues Tong Guohua, because if China can set these standards it can better control its technology and networks, thus supporting national autonomy. "Mastering the standards by yourself, and building networks on your own," he wrote in 2018, "will bring great guarantees to information and even national security."[124]

But 5G standards — and those of information technology more broadly — offer more strategic, more potentially offensive, and more foundational rewards as well. Chinese discourse suggests that information technology standards will define the architecture of the emerging information technology world. Setting those standards therefore offers the chance to write the rules of the future world and, in doing so, to leapfrog, or supplant, the Western order. A 2020 piece in the Chinese Cadres Tribune puts this plainly:

> In the internet era, whoever has discourse power and rule-making power has the power to lead the future order … Before the internet era, European and American countries played a leading role in forming the new world economic, political, and legal order … However, in the era of the internet, and especially in the new era of informatization pioneered by 5G, it is entirely possible for China to leap ahead and make greater contributions. The historic opportunity brought by the internet will surely become an important boost to enhance China's international competitiveness.[125]

That description of an "era of informatization pioneered by 5G" is critical. It helps to explain the outsize importance that China appears to assign 5G in its larger effort to define the information era's architecture. 5G is described a sort of standard of standards — a system that will empower a cascading set of technologies, capabilities, and standards, and therefore that will define the larger information technology ecosystem. Zhao Dachun explained this in clinical terms in a 2018 interview:

> The research and development of 5G is an important measure to implement the network power and develop the digital economy. It can drive the development of the Internet of Things, the industrial Internet of Things, etc., enabling the digital transformation of the whole industry and providing strong support for building a smart society.[126]

The same year, Tong Guohua[127] offered slightly different language:

> The great significance of 5G for the development of the country [China] is that it will subvert the application of various industries, and then trigger the birth of new standards and ecosystems in various industries. It can be said that competing for the leading position of 5G technology is a top priority for the country's economic growth and competitiveness.[128]

Chen Baoguo added another layer to the picture in a prescient 2010 article, noting that the ecosystem of standards and networks that 5G is to empower will span not only the virtual information world but also the physical one:

> The Internet of Things technology makes it possible to control the real world through the network … In the past, the idea has been to separate the physical infrastructure from the information technology infrastructure: Airports, highways, buildings, on the one hand, and on the other hand, data centers, personal computers, broadband, etc. In the era of the Internet of Things, reinforced concrete, cables, chips, and broadband will be integrated into a unified infrastructure. In this sense, the network and reality have become an integral whole.[129]

By extension, the world that can be defined by setting 5G standards spans the real and the virtual, granting power not only over the movement of information, but also over physical space.

All of these points — the state's role in setting 5G standards, their winner-take-all nature; their role in propelling the larger ecosystems that will define the information era, and the control that those ecosystems offer over the virtual and physical worlds — combine in Chinese discourse to frame 5G standards as a competitive domain and a strategically determinative one. "China continues to dominate the global standard of mobile communications," reads a 2017 interview with Tong Guohua, who continues: "Overtaking in the 5G era provides a rare historical opportunity."[130]

China also has the chance to break U.S. and Western holds over international standards, and therefore to undermine U.S. and Western influence. Control over global standards — and, especially, information technology standards — is consistently described as the core of U.S. and Western global power. According to Yang Zhen, then-chairman of the Council of Jiangsu Institute of Communications in 2010:

> The standards and core technologies of the internet are set by the United States. The internet is just a virtual world, and the Internet of Things is a huge system that connects all things in the world … If the key technologies and main standards of the Internet of Things are in the hands of Western developed countries, and [China] has no independent intellectual property rights, then China will have no chance of achieving its peaceful rise and national rejuvenation.[131]

CONCLUSION

A new digital architecture is taking form. This architecture will shape communications and resource flows, security and prosperity, global norms, and information. It will inform the international balance of power and the ways in which power can be deployed within that balance.

A new digital architecture is taking form… Beijing is positioning itself to play a core role in — even to guide — the development of this architecture.

Beijing is positioning itself to play a core role in — even to guide — the development of this architecture. The Chinese government does so while outwardly messaging a set of assumptions and goals in contradiction to those communicated internally. That China speaks with two voices is no novel conclusion. However, the core differences between those voices in IT remain largely undocumented, despite China's increasing influence over international IT infrastructures, technologies, and norms.

ENDNOTES

1 The research team for this paper received copies of emails between the publication's advisory service and writers it had hoped to contract to write content on behalf of Huawei.

2 The term "cyber" (网络) in "cyber great power" can also be translated as "network." This report relies on the "cyber great power" translation, but recognizes that there is room for disagreement. In fact, at least one of the authors prefers the "network great power" translation, owing to the pillars of effort most commonly associated with pursuit of the concept's ambition. (See: Emily de La Bruyère, "The Network Great Power Strategy: A Blueprint for China's Digital Ambitions," The National Bureau of Asian Research, forthcoming in 2021.)

3 习近平 [Xi Jinping], "习近平在网信工作座谈会上的讲话全文发表" [The Full Text of Xi Jinping's Speech at the Forum on Cybersecurity and Informatization Work], (speech, Beijing, April 25, 2016), http://www.xinhuanet.com//politics/2016-04/25/c_1118731175.htm.

4 习近平 [Xi Jinping], "习近平:把我国从网络大国建设成为网络强国-高层动态- 新华网" [Xi Jinping: Build China from a Major Cyber Country to a Cyber Great Power], Xinhua, February 27, 2014, http://www.xinhuanet.com//politics/2014- 02/27/c_119538788.htm.

5 习近平 [Xi Jinping], "习近平在网信工作座谈会上的讲话全文发表" [The Full Text of Xi Jinping's Speech at the Forum on Cybersecurity and Informatization Work].

6 Hua Chunying, "Foreign Ministry Spokesperson Hua Chunying's Regular Press Conference on July 15, 2020," (speech, Beijing, July 15, 2020), https://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/t1797967.shtml; Hua Chunying,"Foreign Ministry Spokesperson Hua Chunying's Regular Press Conference on December 11, 2020," (speech, Beijing, December 11, 2020), https://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/2511_665403/t1839583.shtml.

7 "中央网络安全和信息化领导小组第一次会议召开" [The First Meeting of the Central Network Security and Informatization Leading Group Was Held], 中央政府门户网站 [Central Government Portal], February 27, 2014, http://www.gov.cn/ldhd/2014-02/27/content_2625036.htm.

8 "习近平称努力让关键核心技术自主可控 促产业迈向全球价值链中高端" [Xi Jinping Said That Efforts to Make Key Core Technologies Independent and Controllable to Promote the Industry to the High-End Global Value Chain], Reuters, May 28, 2018, https://cn.reuters.com/article/china-xi-jinping-tech-value-chain-0528-idCNKCS1IT0XT; 陈肇雄 [Chen Zhaoxiong], "推进工业和信息化高质量发展" [Promote the High-Quality Development of Industry and Informatization], 网信军民融合 [*Military-Civil Fusion on Cyberspace*], July 9, 2019, CNKI: F424;F49.

9 "习近平称努力让关键核心技术自主可控 促产业迈向全球价值链中高端" [Xi Jinping Said That Efforts to Make Key Core Technologies Independent and Controllable to Promote the Industry to the High-End Global Value Chain], Reuters.

10 习近平 [Xi Jinping], "习近平：自主创新推进网络强国建设" [Xi Jinping: Independent Innovation Promotes the Building of a Network Power], 新华 [Xinhua], April 21, 2018, http://www.xinhuanet.com/politics/2018-04/21/c_1122719810.htm.

11 秦安 [Qin An], "网络强国的意识认识共识" [Awareness, Understanding, and Consensus of a Network Power], 中国信息技术安全评估中心 [*China Information Security*] 9 (2016), CNKI: TP393.08.

12 习近平 [Xi Jinping], "习近平在网信工作座谈会上的讲话全文发表" [The Full Text of Xi Jinping's Speech at the Forum on Cybersecurity and Informatization Work].

13 郭占恒 [Guo Zhanheng], "习近平标准化思想与浙江实践" [Xi Jinping's Standardization Thought and Zhejiang Practice], 浙江日报 [*Zhejiang Daily*], September 25, 2015, CNKI: F203;F092.7. Both quoted phrases are common in Chinese corporate and policy discussions of standards.

14 陈肇雄 [Chen Zhaoxiong], "加快推进新时代网络强国建设" [Accelerate the Construction of a Network Power in the New Era], *People's Daily*, November 17, 2017, http://opinion.people.com.cn/n1/2017/1117/c1003-29651140.html.

15 See endnote 2.

16 The Central Leading Small Group for Cybersecurity and Informatization is referred to as 中央网络安全和信息化领导小组, and then transformed in a March 2018 upgrade into a commission: 中央网络安全和信息化委员会.

17 "中央网络安全和信息化领导小组第一次会议召开" [The First Meeting of the Central Network Security and Informatization Leading Group Was Held], 中央政府门户网站 [Central Government Portal]."

18 The service Oriprobe was used to search the phrase 网络强国. Xi Jinping and Politburo Standing Committee member Wang Huning have used the phrase on at least two occasions at the World Internet Conference, but with far less detail than in speeches addressing domestic audiences, and not recently.

19 For a list of relevant Xi speeches and quotes, see: 习近平 [Xi Jinping], "习近平谈加快建设网络强国-中共中央网络安全和信息化委员会办公室" [Xi Jinping Talks about Accelerating the Construction of a Cyber Power-Office of the CPC Central Committee Cyber Security and Information Technology], September 9, 2019, http://www.cac.gov.cn/2019-09/11/c_1569738113999057.htm; see also Paul Triolo, Lorand Laskai, Graham Webster, and Katharin Tai, "Xi Jinping Puts 'Indigenous Innovation' and 'Core Technologies' at the Center of Development Priorities," New America, May 1, 2018, http://newamerica.org/cybersecurity-initiative/digichina/blog/xi-jinping-puts-indigenous-innovation-and-core-technologies-center-development-priorities/.

20 习近平 [Xi Jinping], "习近平在第二届世界互联网大会开幕式上的讲话" [Speech by Xi Jinping at the Opening Ceremony of the Second World Internet Conference], (speech, Wuzhen, December 16, 2015), http://www.xinhuanet.com//politics/2015-12/16/c_1117481089.htm.

21 CAC is China's internet regulator. The article draws on analysis of Xi Jinping's statements.

22 "深入贯彻习近平总书记网络强国战略思想 扎实推进网络安全和信息化工作" [In-Depth Implementation of General Secretary Xi Jinping's Strategic Thinking on Strengthening the Country through the Internet, and Solid Progress in Network Security and Information], 求是 [Qiushi], September 15, 2017, http://www.qstheory.cn/dukan/qs/2017-09/15/c_1121647633.htm.

23 习近平 [Xi Jinping], "习近平在网信工作座谈会上的讲话全文发表" [The Full Text of Xi Jinping's Speech at the Forum on Cybersecurity and Informatization Work].

24 Ibid; the same year, Deputy Director of China's Cyberspace Administration Zhuang Rongwen echoed that line: "We missed our opportunities during the industrial revolution … we should never lag behind in the new round of competition." See: Mandy Zuo, "China Aims to Become Internet Superpower by 2050," *South China Morning Post*, July 28, 2016, https://www.scmp.com/news/china/policies-politics/article/1995936/china-aims-become-internet-cyberpower-2020.

25 陈肇雄 [Chen Zhaoxiong], "推进工业和信息化高质量发展" [Promote the High-Quality Development of Industry and Informatization].

26 Ibid.

27 Ibid.

28 陈肇雄 [Chen Zhaoxiong], "加快推进新时代网络强国建设" [Accelerate the Construction of a Network Power in the New Era], 人民网- 人民日报 [*People's Daily*], November 17, 2017, http://theory.people.com.cn/n1/2017/1117/c40531-29651453.html.

29 Duan wrote with a co-author, Han Xiaolu, also affiliated with Datang Group.

30 段伟伦 [Duan Weilun] and 韩晓露 [Han Xiaolu], "全球数字经济战略博弈下的5G供应链安全研究" [Research on 5G Supply Chain Security under the Strategic Game of Global Digital Economy], 信息安全研究 [*Information Security Research*] 6, no. 1 (2020): 46-51, http://www.sicris.cn/CN/abstract/abstract715.shtml.

31 许正中 [Xu Zhengzhong], "网络空间治理的任务与挑战" [The Tasks and Challenges of Network Space Governance], 中国党政干部论坛 [*Party & Government Forum*], no. 1 (2020): 36-37, CNKI: D669. The author is a member of the Standing Committee of the Hubei Provincial Party Committee and director of the Provincial Party Committee Propaganda Department.

32 习近平 [Xi Jinping], "习近平在网信工作座谈会上的讲话全文发表" [The Full Text of Xi Jinping's Speech at the Forum on Cybersecurity and Informatization Work].

33 Zhao Lijian, "Foreign Ministry Spokesperson Zhao Lijian's regular press conference on November 19, 2020," (speech, Beijing, November 19, 2020), https://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/t1833798.shtml.

34 Hua Chunying, "Foreign Ministry Spokesperson Hua Chunying's Regular Press Conference on July 15, 2020."

35 Zhao Lijian, "Foreign Ministry Spokesperson Zhao Lijian's Regular Press Conference on August 18, 2020," (speech, Beijing, August 18, 2020), https://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/t1807193.shtml.

36 习近平 [Xi Jinping], "习近平:把我国从网络大国建设成为网络强国-高层动态-新华网" [Xi Jinping: Build China from a Major Cyber Country to a Cyber Great Power].

37 Ibid.

38 习近平 [Xi Jinping], "习近平在网信工作座谈会上的讲话全文发表" [The Full Text of Xi Jinping's Speech at the Forum on Cybersecurity and Informatization Work].

39 Ibid.

40 Ibid.

41 This term translates more literally as "life gate" or "gate of vitality," but since it is used metaphorically here in Chinese, we have opted for an English metaphor to render it more comprehensible to English-speaking readers.

42 习近平 [Xi Jinping], "习近平在网信工作座谈会上的讲话全文发表" [The Full Text of Xi Jinping's Speech at the Forum on Cybersecurity and Informatization Work].

43 A phrase that refers to passing a competitor on the outside along a turn.

44 习近平 [Xi Jinping], "习近平在网信工作座谈会上的讲话全文发表" [The Full Text of Xi Jinping's Speech at the Forum on Cybersecurity and Informatization Work].

45 Ibid.

46 习近平 [Xi Jinping], "习近平在第二届世界互联网大会开幕式上的讲话" [Speech by Xi Jinping at the Opening Ceremony of the Second World Internet Conference].

47 Xi said: "One view is that we must close the door, start afresh, completely get rid of dependence on foreign technology, and rely on indigenous innovation to seek development, otherwise we will always follow others and never catch up."

48 Xi said: to "open up and innovate and develop our own technology on the shoulders of [foreign] giants."

49 习近平 [Xi Jinping], "习近平在网信工作座谈会上的讲话全文发表" [The Full Text of Xi Jinping's Speech at the Forum on Cybersecurity and Informatization Work].

50 Ibid.

51 Ibid.

52 Ibid.

53 Ibid.

54 陈肇雄 [Chen Zhaoxiong], "推进工业和信息化高质量发展" [Promote the High-Quality Development of Industry and Informatization].

55 墨翡 [Mo Fei], "英国高调发布5G战略 意欲成为全球领导者" [The UK Launches a High-Profile 5G Strategy, Intends to Become a Global Leader], 通信世界 [*Communications World*], no. 21 (2017), CNKI: F627.

56 乔龙 [Qiao Long], 任天舒 [Ren Tianshu], and 刘优 [Liu You], "中国高新技术产业应对贸易摩擦的影响研究—以5G产业为例" [Research on the Impact of China's High-Tech Industries in Response to Trade Frictions—Taking 5G Industry as an Example], 国际经贸 [*International Economics and Trade*] 5 (2020), CNKI: F276.44;F752.02.

57 "中央网络安全和信息化领导小组第一次会议召开" [The First Meeting of the Central Network Security and Informatization Leading Group Was Held], 中央政府门户网站 [Central Government Portal].

58 "习近平称努力让关键核心技术自主可控 促产业迈向全球价值链中高端" [Xi Jinping Said That Efforts to Make Key Core Technologies Independent and Controllable to Promote the Industry to the High-End Global Value Chain], Reuters.

59 Hua Chunying, "Foreign Ministry Spokesperson Hua Chunying's Regular Press Conference on July 15, 2020."

60 Hua Chunying, "Foreign Ministry Spokesperson Hua Chunying's Regular Press Conference on December 11, 2020."

61 Hua Chunying, "Foreign Ministry Spokesperson Hua Chunying's Regular Press Conference on October 9, 2020," (speech, Beijing, October 9, 2020), https://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/t1822871.shtml.

62 The Chinese term for "cyber" (网络) in "cyber security" can also be translated as "network." For the purposes of this report, quoted uses of the term will be translated the "cyber security" rather than "network security." In general discussion, the report will use the phrase "cyber and network security."

63 "中央网络安全和信息化领导小组第一次会议召开" [The First Meeting of the Central Network Security and Informatization Leading Group Was Held], 中央政府门户网站 [Central Government Portal]. He also named the leading group launched at that event the "Central Leading Small Group for Cybersecurity and Informatization," defining it in terms of security.

64 Ibid.

65 Take, for example, Xi's 2018 reiteration that "without network security, there will be no national security." See: 习近平 [Xi Jinping], "习近平：自主创新推进网络强国建设" [Xi Jinping: Independent Innovation Promotes the Building of a Network Power].

66 刘棟 [Liu Li], 孟宪民 [Meng Xianmin], and 李阳 [Li Yang], "5G安全及网络监管问题探析" [Analysis of 5G Security and Network Supervision Issues], 国防科技 [*National Defense Technology*] 41, no. 3 (2020): 76-79, CNKI: TN929.5;TN915.08.

67 习近平 [Xi Jinping], "习近平在网信工作座谈会上的讲话全文发表" [The Full Text of Xi Jinping's Speech at the Forum on Cybersecurity and Informatization Work].

68 习近平 [Xi Jinping], "习近平:加快推进网络信息技术自主创新 朝着建设网络强国目标不懈努力" [Xi Jinping: Accelerate the Independent Innovation of Network Information Technology and Make Unremitting Efforts towards the Goal of Building a Network Power], (speech, Beijing, October 10, 2016), http://cpc.people.com.cn/n1/2016/1010/c64094-28763907.html.

69 陈肇雄 [Chen Zhaoxiong], "推进工业和信息化高质量发展" [Promote the High-Quality Development of Industry and Informatization].

70 轩传树 [Xuan Chuanshu], "正确认识网络强国建设所面对的成就_问题和影响" [Correctly Understand the Achievements of the Network Power Building: Problems and Impact], 中国信息安全 [*China Information Security*] 2 (February 2015), CNKI: TP393.08;E86.

71 This strain of more offensively-oriented, aggressive language is unlikely to appear in Xi Jinping's public rhetoric, or that of other government entities that direct their remarks to external audiences and are subject to international scrutiny. This section therefore relies primarily on less official sources. Of course, these come with caveats concerning authoritativeness: These should not be considered official mandates or strategies issued by the Chinese government, but rather reflections of prevalent thinking in Chinese analytical circles.

72 For in-depth discussion of China's military-civil fusion strategy, see: Emily de La Bruyère and Nathan Picarsic, "Military-Civil Fusion: China's Approach to R&D, Implications for Peacetime Competition, and Crafting a US Strategy," USN/NPS Acquisition Research Symposium, May 2019, https://nps.edu/web/gsdm/acquisition-research-program.

73 "《2015年中国军民融合发展报告》呈现五大亮点" [Five Highlights of the '2015 Military-Civil Fusion Development Report'], 中国日报 [*China Daily*], September 24, 2015, https://cn.chinadaily.com.cn/2015-09/24/content_21968926.htm.

74 习近平 [Xi Jinping], "习近平：自主创新推进网络强国建设" [Xi Jinping: Independent Innovation Promotes the Building of a Network Power].

75 秦安 [Qin An], "网络强国的意识认识共识" [Awareness, Understanding, and Consensus of a Network Power]."

76 段伟伦 [Duan Weilun] and 韩晓露 [Han Xiaolu], "全球数字经济战略博弈下的5G供应链安全研究" [Research on 5G Supply Chain Security under the Strategic Game of Global Digital Economy], CNKI: F623;TN929.5.

77 郭超 [Guo Chao], 于川信 [Yu Chuanxin], and 王景芳 [Wang Jingfang], "对第五代移动通信技术军事应用的几点认识" [Some Understandings on the Military Application of the Fifth-Generation Mobile Communication Technology], 国防 [*National Defense*], no. 1 (2019): 27-29, CNKI: E962;TN929.5.

78 See, for example, Xi's speech at the 22nd study session of the Chinese Communist Party Politburo in July 2020, in which he calls for the acceleration of "informatization and intelligentization" to strengthen China's military: "习近平在中央政治局第二十二次集体学习时强调　统一思想坚定信心鼓足干劲抓紧工作　奋力推进国防和军队现代化建设" [During the 22nd Collective Study Session of the Political Bureau of the Central Committee, Xi Jinping Emphasized the Unification of Thinking, Firm Confidence and Enthusiasm, and Work Hard to Promote the Modernization of National Defense and the Military], 新华 [Xinhua], July 31, 2020, http://www.xinhuanet.com/politics/leaders/2020-07/31/c_1126310486.htm.

79 郑安琪 [Zheng Anqi], "立足现实基础推动我国网络强国建设" [Promote My Country's Network Power Construction Based on Reality], 通信管理与技术 [*Communication Management and Technology*] 3 (2020), CNKI: F49.

80 Ibid.

81 Ibid.

82 李峰 [Li Feng], 马方方 [Ma Fangfang], 刘海 [Li Hai], and 李凯 [Li Kai], "浅析5G技术在现代军事物流中的应用" [Analysis on the Application of 5G Technology in Modern Military Logistics], 物流技术 [*Logistics Technology*] 39, no. 4 (2020.): 133-37, CNKI: TN929.5;E075.

83 郭超 [Guo Chao], 于川信 [Yu Chuanxin], and 王景芳 [Wang Jingfang], "对第五代移动通信技术军事应用的几点认识" [Some Understandings on the Military Application of the Fifth-Generation Mobile Communication Technology].

84 Ibid.

85 Ibid.

86 Ibid.

87 Ibid.

88 Ibid.

89 王峰 [Wang Feng], "军民融合热度渐升A股酝酿主题行情" [The Enthusiasm for Military-Civil Fusion Is Rising, A-Shares Are Brewing Themed Market], 商业观察 [*Business Observation*] 8 (2019): 42-47, CNKI:F426.48;E25;F832.51.

90 Ibid.

91 李峰 [Li Feng], 马方方 [Ma Fangfang], 刘海 [Li Hai], and 李凯 [Li Kai], "浅析5G技术在现代军事物流中的应用" [Analysis on the Application of 5G Technology in Modern Military Logistics].

92 孙柏林 [Sun Bolin], "5G赋能现代军事" [5G Empowers Modern Military], 计算机仿真 [*Computer Simulation*] 37, no. 1 (2020): 1-6, CNKI: TN929.5;E11.

93 陈宝国 [Chen Baoguo], "新一轮信息技术革命浪潮对我国的影响" [The Affect of A New Round of Information Technology Revolution to Our Country], 科学决策 [*Scientific Decision Making*] 11 (2010): 1-25, CNKI: F49.

94 Ibid.

95 Ibid.

96 刘红凛 [Liu Honglin], "信息化发展对党的建设的多重影响" [The Multiple Influences of Information Development on Party Building], 中共中央党校学报 [*Journal of the Party School of the Central Committee of the C.P.C.*] (December 2011), CNKI: TP399-C2.

97 易华勇 [Yi Huayong] and 邓伯军 [Deng Bojun], "新时代中国国家文化安全策论" [China's National Cultural Security Policy in the New Era], 江海学刊 [*Jianghai Academic Journal*] (2020), CNKI: TP18;TN929.5;G120.

98 Zhao Lijian, "Foreign Ministry Spokesperson Zhao Lijian's Regular Press Conference on October 19, 2020," (speech, Beijing, October 19, 2020), https://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/t1825131.shtml.

99 龙在野 [Long Zaiye], "网络强国和信息治国的网信军民融合路径探悉" [Exploration of the Path of Cyber-Information Military-Civil Fusion for a Network Power and Information Governance], 网信军民融合 [*Military-Civil Fusion in Cyberspace*] (October 2017), CNKI: E25.

100 习近平 [Xi Jinping], "习近平在网信工作座谈会上的讲话全文发表" [The Full Text of Xi Jinping's Speech at the Forum on Cybersecurity and Informatization Work].

101 Zhao Lijian, "Foreign Ministry Spokesperson Zhao Lijian's Regular Press Conference on September 8, 2020," (speech, Beijing, September 8, 2020), https://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/t1813183.shtml.

102 "'网络空间战略论坛'三载路:网络强国理论高地行" ['Cyberspace Strategy Forum' Three-Year Road: Cyber Great Power Theory Highland Tour].

103 郭占恒 [Guo Zhanheng], "习近平标准化思想与浙江实践" [Xi Jinping's Standardization Thought and Zhejiang Practice], 浙江日报 [*Zhejiang Daily*], September 25, 2015, CNKI: F203;F092.7. Both quoted phrases are common in Chinese corporate and policy discussions of standards.

104 "'标准化'作用何在？习近平为你一一讲来" [What Is the Role of 'Standardization'? Xi Jinping Tells You], 中国日报 [*China Daily*], September 13, 2016, https://china.chinadaily.com.cn/2016-09/13/content_26783549.htm. That was no new focus for Xi: As early as 2006, when secretary of the Zhejiang Provincial Party Committee, Xi proposed to "actively implement the strategy of intellectual property rights and standardization," calling "standardization" a "strategic height" for economic and social development. See: 郭占恒 [Guo Zhanheng], "习近平标准化思想与浙江实践" [Xi Jinping's Standardization Thought and Zhejiang Practice].

105 For additional discussion of China's standards ambitions, see Emily de La Bruyère and Nathan Picarsic, "China Standards 2035: Beijing's Platform Geopolitics and Standardization Work in 2020," Horizon Advisory, April 2020, https://www.horizonadvisory.org/china-standards-2035-introduction; Emily de La Bruyère, "Platform Geopolitics: The New Metrics for Building Geopolitical Power in a New World," *The National Interest*, April 12, 2020, https://nationalinterest.org/feature/new-metrics-building-geopolitical-power-new-world-143147.

106 习近平 [Xi Jinping], "中共中央政治局就实施网络强国战略进行第三十六次集体学习" [The Political Bureau of the CPC Central Committee Conducts the 36th Collective Study on the Implementation of the Strategy of Network Power], 新华 [Xinhua], October 9, 2016, http://www.gov.cn/xinwen/2016-10/09/content_5116444.htm.

107 金英果 [Jin Yingguo], "'中国标准2035'项目" [China Standards 2035 Project], 中国标准话 [*China Standardization*] 1 (2019): 38-43, CNKI: F203.

108 "'中国标准2035'项目结题会暨'国家标准化发展战略研究'项目启动会在京召开" ['China Standard 2035' Project Closing Meeting and 'National Standardization Development Strategy Research' Project Kick-off Meeting Held in Beijing], 铁道技术监督 [*Railway Technical Supervision*] 2 (2020): 16, CNKI: F203.

109 "2020年全国标准化工作要点" [Main Points of National Standardization Work in 2020], 国家标准化管理委员会 [National Standardization Administration].

110 孙强 [Sun Qiang], "乌镇讲话彰显习近平网络强国战略的思想内核" [Wuzhen Speech Highlights The Ideological Core of Xi Jinping's Network Power Strategy], 人民日报 [*People's Daily*], January 2016, CNKI: TP393.4.

111 This calculus is not unlike Xi Jinping's point, cited earlier in this report, that core technologies are fields where China is "on the same starting line as foreign countries. I few can deploy ahead of time and focus on research, it is very possible to realize the transformation from running behind others to running ahead of others and leading." See: 习近平 [Xi Jinping], "习近平在网信工作座谈会上的讲话全文发表" [The Full Text of Xi Jinping's Speech at the Forum on Cybersecurity and Informatization Work].

112 "2020年全国标准化工作要点" [Main Points of National Standardization Work in 2020], 国家标准化管理委员会 [National Standardization Administration].

113 习近平 [Xi Jinping], "习近平:加快推进网络信息技术自主创新 朝着建设网络强国目标不懈努力" [Xi Jinping: Accelerate the Independent Innovation of Network Information Technology and Make Unremitting Efforts towards the Goal of Building a Network Power].

114 高超 [Gao Chao], "加快5G进程助力网络强国建设" [Speeding up the 5G Process to Help Build a Network Power], 通信产业报 [*Communication Industry News*], March 12, 2018, http://www.qikan.com/article/txcy20180928.html.

115 童国华 [Tong Guohua], "立足自主 重点布局 探索网络空间内生安全" [Based on Autonomy, Focus on Layout, Explore Endogenous Security in Cyberspace], 保密科学技术 [*Confidential Science and Technology*] 11 (2018): 33, CNKI: TP393.08.

116 段伟伦 [Duan Weilun] and 韩晓露 [Han Xiaolu], "全球数字经济战略博弈下的5G供应链安全研究" [Research on 5G Supply Chain Security under the Strategic Game of Global Digital Economy]. Duan writes with a co-author, Han Xiaolu, also affiliated with Datang Group.

117 Ibid.

118 Ibid.

119 Ibid.

120 The article is by a lieutenant colonel at the Graduate School of the Academy of Military Sciences, a professor at the Academy of Military Sciences, and a colonel in the 93605 unit. See: 郭超 [Guo Chao], 于川信 [Yu Chuanxin], and 王景芳 [Wang Jingfang], "对第五代移动通信技术军事应用的几点认识" [Some Understandings on the Military Application of the Fifth-Generation Mobile Communication Technology].

121 Ibid.

122 胡蓉 [Hu Rong], "发展5G，深圳使命在肩" [Development of 5G, Shenzhen's Mission Is on Its Shoulders], 深圳商报 [*Shenzhen Commercial Daily*], April 29, 2019, http://www.sznews.com/news/content/mb/2019-04/29/content_21705204.htm.

123 苏德悦 [Su Deyue], "苗圩在国务院新闻发布会上表示稳步推进5G网络建设 深化5G应用发展" [Miao Wei Said at the State Council Press Conference to Steadily Promote the Construction of 5G Networks and Deepen the Development of 5G Applications

Artificial Intelligence Technology Information], 人民邮电报 [*People's Post and Telegraph*], January 21, 2020, http://www.cnii.com.cn/sy/tt/202001/t20200121_150863.html.

124 童国华 [Tong Guohua], "立足自主 重点布局 探索网络空间内生安全" [Based on Autonomy, Focus on Layout, Explore Endogenous Security in Cyberspace].

125 许正中 [Xu Zhengzhong], "网络空间治理的任务与挑战" [The Tasks and Challenges of Network Space Governance].

126 高超 [Gao Chao], "加快5G进程助力网络强国建设" [Speeding up the 5G Process to Help Build a Network Power].

127 Tong, also cited above, is chairman and secretary of the Party Committee of China Information and Communication Technology Group.

128 童国华 [Tong Guohua], "立足自主 重点布局 探索网络空间内生安全" [Based on Autonomy, Focus on Layout, Explore Endogenous Security in Cyberspace].

129 陈宝国 [Chen Baoguo], "新一轮信息技术革命浪潮对我国的影响" [The Affect of A New Round of Information Technology Revolution to Our Country].

130 童国华 [Tong Guo], "大唐电信集团董事长兼总裁童国华：不忘初心 牢记使命，做引领5G发展的国家队" [Tong Guohua, Chairman and President of Datang Telecom Group: Do Not Forget Your Original Aspiration, Keep Your Mission in Mind, and Be the National Team Leading the Development of 5G], 中国电子报 [*China Electronic News*], November 21, 2017, http://www.cena.com.cn/infocom/20171121/90412.html.

131 杨震 [Yang Zhen], "物联网:引领新一轮信息技术革命" [Internet of Things: Leading a New Round of Information Technology Revolution], 江苏通信 [*Jiangsu Communications*] 3 (2010): 12113, CNKI: F49;F426.6.

ABOUT THE AUTHORS

Rush Doshi was the director of the Brookings China Strategy Initiative and a fellow in Brookings Foreign Policy. He was also a fellow at Yale Law School's Paul Tsai China Center and part of the inaugural class of Wilson China fellows. His research focused on Chinese grand strategy as well as Indo-Pacific security issues. Doshi is the author of *The Long Game: China's Grand Strategy to Displace American Order*, forthcoming from Oxford University Press. He is currently serving in the Biden administration.

Emily de La Bruyère is a co-founder of Horizon Advisory, a geopolitical consultancy, as well as a senior fellow at the Foundation for Defense of Democracies (FDD). Her work focuses on China's standardization ambitions, military-civil fusionstrategy, and platform geopolitics, as well as their implications for globalsecurity and the economic order. She holds a Bachelor of Arts summa cum laude from Princeton University and an Master of Arts summa cum laude from Sciences Po, Paris, where she was the Michel David-Weill fellow.

Nathan Picarsic is a co-founder of Horizon Advisory, a geopolitical consultancy, and a senior fellow at the Foundation for Defense of Democracies (FDD). His research focuses on the development of competitive strategies responsive to the Chinese Communist Party's asymmetric orientation for global economic and security competitions. He holds a Bachelor of Arts from Harvard College and has completed executive education programs through Harvard Business School and the Defense Acquisition University.

John Ferguson is a former Brookings intern with the Center for East Asia Policy Studies and the China Strategy Initiative. He will graduate from Harvard in May 2022 completing both a Bachelor of Arts in Government and a Master of Arts in Regional Studies-East Asia, concurrently in four years. He was previously a research intern for the Director of the Carnegie-Tsinghua Center for Global Policy and leads the Harvard Undergraduate Foreign Policy Initiative.

ACKNOWLEDGEMENTS

The authors wish to thank former interns Isabella Lu, Gaoqi Zhang, and Zijin Zhou for their research assistance on this project, Anna Newby and Ted Reinert for editing this paper, and Chris Krupinski for providing layout. Brookings is grateful to the U.S. Department of State and the Institute for War and Peace Reporting for funding this research.

BROOKINGS

The Brookings Institution
1775 Massachusetts Ave., NW
Washington, D.C. 20036
brookings.edu