Chapter 6

Emerging Critical Information Technology and Great Power Competition

By Richard Andres

Over the past few decades, the foundation of Great Power competition has changed. Where control of industrial resources was once the key to geopolitical power, today control of information resources is most important. China is currently investing heavily in three critical new information technologies—5G wireless, quantum computing, and artificial intelligence—that, as part of its information strategy, will vastly increase its control of the global information flow. The United States has a short window to contest China's state-led ascent in these technologies, as well as in the underlying conditions that are allowing China to outpace the United States in this wider field. If the United States does not prevent China from dominating global flows of information, China will attain a clear advantage in its rise to replace the United States as the world's leading Great Power.

Over the past few decades, and as observed in the chapter 4 discussion of the fourth industrial revolution, the foundation of Great Power wealth and competitive advantage has fundamentally changed from one dominated by industrial era technology to one in which information technology (IT) has become the primary source of geopolitical power. U.S. businesses were quick to recognize and act on this change. Today, the top three U.S. IT companies are worth 70 times as much as the top three U.S. car manufacturers. Apple Incorporated alone could buy all five major U.S. defense contractors with its cash on hand. Like U.S. private businesses, China's government has seen and acted on this new IT reality. It has poured billions of dollars into key information technologies and bankrolled its so-called private company Huawei's schemes to dominate global information infrastructure. China has focused vast military and commercial resources on stealing its adversaries' intellectual property, infesting their critical infrastructure with malware, and conducting social media–based influence campaigns at home and abroad. Unfortunately, unlike U.S. commercial interests and the Chinese government, U.S. Government defense policy has been slow to respond to the changing foundations of global power. Today, U.S. defense resources generally go toward industrial era capabilities, and America's strategy remains fixed on winning industrial era battles.

This chapter focuses on the critical role of IT in current geopolitics. It argues that the foundation of geopolitical power has shifted from industrial output to information control. This change has been affecting the global balance of power in favor of China for over a decade but is about to enter a dramatic new phase as China pours state-managed resources into new technologies—most critically, 5G wireless communication, quantum computing, and artificial intelligence (AI)—with the goal of increasing its control over the global flow of information. Meanwhile, although recognizing the problem on paper, U.S. defense policy remains wedded to the quixotic Cold War–era notion that U.S. entrepreneurialism and technology will eventually overcome China's aggressive information policy—something that cannot happen so long as China continues to steal technology as fast as U.S. entrepreneurs and laboratories develop it.

It is imperative that U.S. policymakers recognize and act on the new reality. Information, not physical resources, is now the foundation of geopolitical power. Just as IT has reversed the relative value of physical- and information-based businesses in the past decade, in the next decade, IT will invert the effectiveness of physical- and information-based Great Power policies and politics. The United States has only a short window to come to grips with and act on the new foundation of global power. To do this, America must prioritize countering China's current ability to steal intellectual property and otherwise control the flow of information within the United States and other developed nations while reprioritizing resources into key technologies and capabilities that will allow it to contest China's ability to increase its future power and act in cyberspace.

This chapter is presented in six sections. The first describes the relationship between technology and geopolitical power. The second describes the difference between the way industrial and information era technologies affect global power. The third describes the way autocratic countries are currently using information technology against the United States and its allies. The fourth discusses the race for the three information technologies that will determine which country leads in the emerging geopolitical contest over control of the global flow of information. The fifth describes the problem with current U.S. defense policy, focusing on the futility of racing to develop technology when China can quickly steal it. The chapter concludes with a call to prioritize information over physical conflict as the key to success in Great Power competition.

Technology and Geopolitical Power

Throughout history, states have pursued their political interests using various instruments of national power. The types of issues that states compete over vary. In the second half of the 20th century, the two main actors—the United States and the Soviet Union—vied over which superpower would control which regions of the globe and whether weaker states would be governed by communist or capitalist economic systems. Today's main players are the United States and China, and the main issues in contention center on whether the U.S.-led liberal global order will persist or be supplanted by one based on China's autocratic system and preferences. While the United States still dominates in industrial age military power, China has acted aggressively using information-based power. As a result, China's system is beginning to hold sway over important issues in a number of countries in Asia and, increasingly, in Europe. On some key issues, such as its right to steal intellectual property without penalty or to force foreign business such as the National Basketball Association to conform to Chinese Communist Party *dictat*, its system could be said to prevail even inside the United States.[1]

In the current system, as in previous eras, geopolitical power is mainly determined by the amount of economic and military capabilities major players can project abroad, and these abilities in turn are shaped by the era's dominant technology. Between the 15th and 19th centuries, both economic and military power were principally shaped by ocean-borne trade and sea power. During this period, the nations best able to control the flow of commerce on the world's seas tended to make the world's rules. During the 20th century, the major powers best able to harness industry tended to dominate global politics; the countries able to bring the most men and materiel to bear tended to make the rules. In the current era, information technology is the key to both economic and military power. In this era, the countries best able to control the flow of information across the world's networks tend to make the system's rules.[2]

Industrial vs. Information and Global Power

To understand how states have been using information technology to shape geopolitics and how they are likely to utilize emerging IT over the next decade, it helps to consider how the dynamics and incentives connected with IT differ from those associated with traditional industrial power.

In the past century, a state's power was closely linked with its industrial capacity. To increase their power, major players worked to bolster their manufacturing base at home and often attempted to seize other states' resources through military action. Both world wars were caused by nations acting on the belief that they could increase their power by seizing territory, and throughout the Cold War, the United States and Western Europe based much of their defense policies on the fear that the Soviet Union would invade Western Europe in order to seize its industrial resources.

To counter the industrial era incentive for invasion during the Cold War, nations built alliances to bolster their military capability; they expanded their conventional military power and developed large, often hair-trigger nuclear forces. By the end of the war, the Earth was encircled in competing military alliances and ringed in bases, bombers, and aircraft carriers. The United States and the Soviet Union, with the largest industrial capacities, dominated geopolitics, generally set the rules within their respective spheres of influence, and used their economic and military power to shape world politics.

Yet, even during the Cold War, there were signs that industrial power was beginning to lose its place to information power as the dominant technology in geopolitics. In a well-known story, the Soviets were among the first to recognize this change. At the height of the Cold War, Soviet analysts noted that, while the Soviet Union could produce far more steel and mobilize a far larger army than the United States (the two traditional indicators of industrial-military capability), the West's information economy allowed it to more than overcome its industrial disadvantages with superior information-based military technology.[3] Even worse, from the Soviet perspective, was the West's ability to use what the Soviets saw as psychological-information operations to foment insurrection within the Eastern bloc. The first fear was proved accurate by the success of U.S. information age weapons in the 1990 Gulf War, the second by the fall of Soviet communism to internal insurrection.

While the Soviet Union did not survive long into the information age, the People's Republic of China did. Writing in the early 2000s, holding up the fall of the Soviet Union as evidence, Chinese geopolitical strategists, such as Major General Xu Hezhen, spoke of the threat posed by the United States to the Chinese Communist Party.[4] As a counter to this, China proposed a national strategy based on information rather than industrial era methods. According to this argument, the most effective route to geopolitical power in the current century involved information. This led China to an overall strategy that sought control over the flow of knowledge, secrets, and beliefs rather than simply raw materials and industrial output.[5] This included, for instance, its Three Warfares doctrine and an industrial policy aimed at controlling key industries that produced, among other things, software, undersea cables, microchips, and telecommunications rather than an approach aimed at merely controlling territory.[6]

With the advantage of hindsight, a U.S. strategist might characterize the idea as attempting to encircle the world in a virtual network rather than trying to compete directly with America's physical network of bases, bombers, and ships. The new information age methods do not make conventional and nuclear war obsolete any more than nuclear forces made industrial era technology irrelevant or railroad and other industrial era technology made navies irrelevant. Rather, information technology has been layered on top of and throughout the older system. This overall philosophy has infused much of China's geopolitical strategy for the past two decades.[7]

Geopolitical Targets of Autocratic Countries

The Chinese strategy is effective. To benefit economically from emerging IT, the United States and other developed nations have connected essentially everything in their territories to computer networks. This includes businesses, critical infrastructure, and social media networks. Once connected, all these institutions are potentially vulnerable to exploitation or destruction by anyone connected to the global telecommunications grid.[8] Meanwhile, as an autocratic state, China's government has been able to control information domestically by fencing off many of its own information vulnerabilities from outside penetration.[9]

After two decades of experimentation by states attempting to use information as an instrument of geopolitics, three main types of targets have emerged. The first is economic. In traditional industrial era economies, wealth is generated and stored in physical assets, and this pattern continues in many less developed countries, including China and Russia. In the developed world, over the past few decades, firms have increasingly generated and stored wealth in nonphysical assets. By one estimate, as early as 2010, about 80 percent of U.S. corporate value was stored in intellectual property and trade secrets vulnerable to cyber theft.[10] That percentage is almost certainly considerably higher today. Beyond this, in the United States, large amounts of wealth—much of which can be stolen—are stored in the knowledge and research held within state-funded universities.

In the industrial age, if an ambitious Great Power hoped to plunder the most valuable resources of the United States or Europe, it would have had to physically defeat North Atlantic Treaty Organization armed forces. Today, to steal the West's assets, it is necessary only to penetrate the computer networks where companies and nonprofit organizations store their wealth. According to the independent U.S. Intellectual Property Commission, China uses these methods to steal hundreds of billions of dollars of intellectual property from U.S. and European firms every year.[11] The overall effect is to stunt the economies of plundered nations while vastly accelerating China's economic growth. Over the past two decades, this approach has contributed to China's rapid economic growth. Information theft is not the only cause of China's economic miracle, but it is a necessary one. If it stops, China's swift economic progress would slow considerably, but if it continues over the next decade, all things equal, it will likely lead to China's economy eclipsing that of the United States. No state-sponsored physical piracy campaign in history has had anything like the geopolitical impact of China's virtual piracy campaign. Given the costs of occupying conquered nations, it is unlikely that China could have gained as much wealth from even a Soviet-style conquest of the small countries on its borders.

The second main target for information operations involves civilian and military critical infrastructure. As early as 2010, when Stuxnet malware was found in Iranian nuclear centrifuges at the country's Natanz facility, firms around the world began to realize they were vulnerable to software-based attacks on their hardware. Moreover, on inspection, thousands of critical infrastructure-providing companies discovered that their computers were infected with malware, and many more learned that unknown entities had developed methods of accessing their equipment. In 2015, the commander of U.S. Cyber Command informed the Senate that China and other countries had the means in place to take down U.S. critical infrastructure.[12] On one end of the spectrum, such malware could be used to cause individual civilian or military systems to temporarily stop functioning; on the other, it could be used to create continent-wide, months-long infrastructure failures that could cause millions of deaths.[13] As China works to increase its ability to attack civilian infrastructure, it also has integrated information operations into all aspects of its military capability and posture.[14]

Methods that use information technology to take down an adversary's critical infrastructure and military systems are generally not as dependable as methods that use conventional or nuclear weapons. They are, however, superior to kinetic industrial era techniques in at least two ways. First, they are less expensive. Developing the bases, navies, and air forces necessary to project power globally costs trillions of dollars and is, at least currently, something only the United States can accomplish. Malware is less expensive and allows poor countries to project power cheaply. Second, information-based attacks on critical infrastructure can be calibrated and conducted in low-intensity situations. Thus, a country that might fear attacking the United States with conventional or nuclear weapons might be willing to conduct cyber attacks on critical infrastructure that it believes could work below the threshold that would elicit a violent response from America. Such capabilities could plausibly be used to coerce or deter the United States.[15] The Department of Homeland Security has repeatedly warned that China and Russia have infected U.S. critical infrastructures with malware that could be used in this manner.[16]

The third target for information operations involves populations. In recent decades, firms have acquired access to most individuals in most countries (through social media) and developed AI technologies to manipulate targets' purchasing behaviors. More recently, nations have begun using similar methods to manipulate targets' political preferences and passions. A growing body of literature suggests that humans are susceptible to these techniques.

At present, China is the leader in the technology associated with state-centric manipulation of political behavior. Using its close relationship with Chinese Internet service providers, the Chinese government has developed methods to manipulate information, thought, and political activity within its borders and, increasingly, in other nations.[17] Like China, Russia has experimented with these methods at home and abroad. Over time, both countries are likely to increase and refine their technologies and techniques. While it is unclear how effective these techniques will be in the long term as a tool of political control used against Western populations, the success of Chinese computer-based political-psychological operations against Chinese citizens and of Russian actions in Europe and North America suggest a clear danger. The 20th-century Soviet information operations that led to the global rise of communism represent a possible low-technology precedent that bears consideration. Just as the Soviet Union once persuaded over half the planet's population to abandon that era's dominant political systems in favor of communism, today's autocratic information operations have the potential to do enormous harm to the current liberal world order.

Race for Three Information Technologies

Given the ways IT can be used in geopolitical competition, if an autocratic Great Power was to gain complete control over cyberspace, eventually it would gain the wealth and military power to set the rules for the international system in much the same way the United States now does. Analogously, a major power gaining unfettered access to the world's computer networks today would be similar to the Soviet Union gaining control of Western Europe's industrial capacity during the Cold War.

To date, despite ongoing efforts, neither China nor Russia has gained unfettered access to Western networks. They have failed to do so largely because of the immense resources that governments and private industry dedicate to computer defenses. The battle for access is a constant struggle to control the domain that is played out every time a new piece of software or hardware is added to a network. It involves attempts to find holes in operating systems, commercial software, phone apps, hardware, and nearly everything associated with the growing Internet of Things. This contest is reminiscent of trench warfare during World War I in that it is a persistent whole-of-nation contest played out daily in millions of individual duels among individuals, firms, and agencies for small advantages, and what is won one day is often lost the next.

While battles in cyberspace are often for small and fleeting advantage, several contests occurring today are likely to have large and enduring results that will determine which Great Power dominates cyberspace for future decades.

The First Contest: 5G

The first major contest for control of cyberspace involves the fifth-generation wireless communications technologies supporting cellular data networks, generally known as 5G.[18] For much of the coming decade at least, this technology will provide the backbone for future cell phone communication and for the Internet of Things.[19] This includes technologies such as self-driving cars, supervisory control and data acquisition infrastructure, and the networks that military systems depend on. A country able to dominate 5G systems potentially will have access to and a good deal of control over most information flowing through cyberspace.[20]

The nearly unfettered access that 5G dominance provides to user information goes beyond simple data collection. A country with this type of access can use it to map critical systems throughout an adversary's territory. It gains real-time intelligence about the physical and network location of individuals and systems.[21] It could deny or corrupt information received by human or machine users, civilian or military (once such systems are installed nationally, a military would be hard pressed not to use them). These capabilities would vastly increase the ability of the controlling nation to conduct espionage, sabotage machines that are connected to digital networks, and perform a range of operations involved with conducting social-psychological operations against adversaries' populations.

Traditionally, the United States has been able to purchase IT equipment from autocratic adversaries without much fear that they will be able to exploit the hardware; the end users have retained physical control of most of the software and hardware. But 5G is different in that it pushes far more functionality from the user to the supplier. For instance, in a 5G environment, the apps on a phone might reside entirely on servers in Beijing. Moreover, in so far as a 5G provider uses proprietary software to perform a range of controls conducted by hardware in earlier wireless technology, the provider now largely controls access and control of information passing through its system. In certain places in China where 5G is well established, this ability sometimes reaches the point where customers no longer need handsets. Distributed cameras and microphones in places such as hotel lobbies or sidewalks identify users and respond directly to commands, completely removing any possibility of user-supplied defense or control. In general, the more bandwidth becomes available, the more control can be pushed from the user to the company supplying the service.[22]

Over the past two decades, China has enacted a national industrial policy that, among other things, seeks to make China the global leader in communications technology in general and 5G in particular. China's industrial strategy aims to make the nation the world leader in 5G by supporting national champions, Huawei in particular, via direct funding from the state (mainly via subsidized loans) and by a campaign to steal cutting-edge telecommunications technology from Western firms and provide that technology to its champions for free. The overall effect has been to cut Huawei's cost of producing goods far below that of its competition, thereby allowing it to undercut the prices of Western competitors. As a result, Huawei is able to sell 5G technology at rates far below those of other nations—in some cases, as much as 60 percent below market rates.[23] With the exception of countries such as the United States that eschew Huawei's high-quality/low-cost services out of concerns about national security, most nations in the world installing 5G are installing Huawei systems.

Huawei's 5G dominance of global networks will not result in China instantly dominating cyberspace. If Huawei acts too aggressively on China's interests, countries are likely to spend the money necessary to replace Huawei's systems with hardware built in other countries. More than that, although China is currently using 5G within its own borders to control the flow of information, it will take time to develop and adapt software, tactics, techniques, and procedures that work abroad. Yet, over time, China will be able to become ever more aggressive as countries become increasingly dependent on Huawei's goods and services. At some scale, China will be able to get away with virtually any use of 5G networks because the price of replacing the network will become too high. Two years ago, Congress was barely able to force a handful of small U.S. telecoms to divest themselves of Huawei's hardware. In the future, China will be able to extract significant geopolitical information rents from countries that are dependent on its systems.[24]

The Second Contest: Quantum

The second major contest for control of cyberspace involves the race for quantum technology.[25] Because quantum computers are able to perform a range of operations at rates that greatly exceed older processing technology, they hold out the possibility of being able to break existing encryption.[26] This ability would not only render current encryption obsolete but also most likely allow its holder to decrypt decades of older encoded messages. Because encryption is generally the single point of failure in all computerized defenses, having this capability would vastly increase its holder's power.[27]

For decades, quantum computing has been the Holy Grail of computer technology but has always been out of reach. Over the past 2 years, however, several companies have introduced computers with limited quantum capabilities.[28] While none of these companies so far has advertised the ability to break codes, this technology is within reach. While it might seem that quantum technology would equally aid both encryption and decryption, this is not the case. For practical reasons, the technology will do much more to aid decryption than encryption, and it is likely that the country to win the race to produce and utilize the technology will gain a significant advantage in the contest to control the cyber domain.[29] Beyond this scenario, while both China and the West have many state secrets, the West simply has immensely more secrets than China—both Western industry and militaries depend on encryption in ways China's industry and military do not.

Over the past few years, the United States has invested considerably in quantum technology, but recently China has begun to spend vastly more. While the United States is probably ahead in this race—at least as far as industry is concerned, with IBM and Google fielding computers with limited quantum capability—that lead is unlikely to last.[30] Given forecasted spending trends, China is likely to finish the race to utilize quantum technology in support of national security goals well ahead of the United States.[31] When it does, its ability to steal industrial secrets and infect and sabotage critical civilian and military systems will vastly increase.

The Third Contest: Artificial Intelligence

The third major contest for control of cyberspace involves AI and has two main implications for national security.[32] The first involves the potential for AI use in computer defenses. In recent years, AI has proved capable of vastly increasing both the offensive and defensive cyber capabilities by finding and exploiting or plugging gaps in defenses. The second involves social-psychological applications. Currently, firms are developing AI to create psychological profiles of individuals to market goods and services to them.[33] AI applications are capable of processing vast amounts of information on individuals and conducting psychological experiments on large populations in order to discover how to predict and manipulate their actions and beliefs. Experiments have demonstrated that this type of AI is often vastly better at predicting individual subjects' decisions than even subjects' friends and spouses.[34]

Over the past half-decade, both Russia and China have taken advantage of AI for political purposes. The full extent of these operations is not public, but China is generally believed to spend vast resources on experimenting with AI to monitor and control its own population, and Russia has made ample use of marketing AI supplied by Facebook and other companies to target and manipulate foreign populations' political beliefs and passions. As AI advances, its potential for this type of social-political manipulation is likely to increase considerably.[35]

At present, both the United States and China are investing heavily in AI research. However, from the perspective of national security, China has two significant advantages. The first is that China's political and economic systems allow it to provide much more data to government and corporate users than is the case in the United States.[36] This data is a critical asset in creating practical applications for AI. Second, for the purposes of national security, the U.S. Government invests far less in this technology than does the Chinese government.[37] Thus, while U.S. and Chinese companies are able to compete on a somewhat even basis, China's government has a nearly unassailable lead over the U.S. Government in terms of how each uses AI in geopolitical information.[38]

The Big Picture and the Red Queen: The Problem with Current U.S. Defense Policy

The outcomes of the three technology contests will be critical to the larger contest for cyberspace. Looked at individually, each does not tell the whole story about China's overall strategy to gain control of information networks or how it will use them in geopolitics. China promulgated a broad manufacturing plan, Made in China 2025, that focuses on specific Chinese government support for these critical technologies for future Chinese dominance, but that aims for much more.[39]

Regarding China's overall plan to gain control of cyberspace and dominate the information contest of the future, the three technologies are best seen as the tip of a much larger iceberg. According to the notion propounded by many Soviet and Chinese geopolitical strategists and also behind the U.S. third offset strategy, the United States defeated the Soviet Union in the Cold War because it was able to make up for its shortcomings in manpower and industrial capacity with advantages in science and technology.[40]

To stay ahead in technologies such as the three described, China has dedicated enormous resources to education in science, technology, engineering, and mathematics (STEM). This policy has both a domestic and foreign component. At home, China produces around eight times as many STEM graduates as does the United States. Abroad, in 2016, 43 percent of students in U.S. science and engineering schools were Chinese. In computer-related U.S. college programs, only 21 percent were American.[41]

The skills these students bring home, combined with the technology Chinese businesses and intelligence agencies steal from U.S. and allied countries, create a Red Queen problem for U.S. technology.[42] The faster the United States runs, the faster it must run to stay ahead. Since new U.S. technology is immediately taught to Chinese citizens by U.S.

professors and stolen by Chinese hackers, U.S. technological ingenuity and investment are not likely to overcome China's lead in manpower and industrial capacity the way it overcame that of the Soviet Union three decades ago. Because China has invested heavily in controlling the global flow of information, China freely garners the benefits of U.S. public and private investment in science and technology. As a result, it is free to focus its own investments into 5G, quantum capabilities, AI, and other technologies that will expand its ability to control the global information flow.[43] As a result, the United States cannot win the geopolitical information age contest simply by spending more on research. The Cold War paradigm will not work in the current era.

The Way Ahead: Prioritizing Information Over Physical Conflict

There have been several attempts to address the technology problems described in this chapter. The Department of Defense's third offset strategy attempted to address these issues by investing in new technology faster than China.[44] The National Security Strategy defines specific technologies the United States will pursue to keep its lead, particularly singling out those related to information technology.[45] The National Cyber Strategy further focuses on key information technologies the United States will pursue in its competition with Russia and China.

The problem with these approaches is not their specific proposals; it is more that they are written from an industrial era perspective. They tend to portray the contest for control of information and information technology as one more aspect of *national security policy* rather than the emerging foundation of future *geopolitical power*. While it is true that traditional industrial power projection capability will play a central role in small state competition for the foreseeable future, where China and Russia are concerned, information power is more likely than industrial power to determine the outcomes of long-term geopolitical contests.[46]

A basic idea expressed—and then for the most part ignored—in each of the U.S. security policy documents referenced above is that the United States could do more to reduce threats to its interests and increase its geopolitical influence by solving information-based problems than by increasing its kinetic military power. Stopping Chinese intellectual property theft must be first on the agenda because little else will work until this problem is solved. This problem has been with us for a long time.[47] Securing U.S. networks against industrial espionage would considerably bolster the U.S. economy and decrease Chinese piracy-based economic growth. Further increasing the U.S. military lead over Russia or China does neither. Securing U.S. critical infrastructure against cyber attacks from Russia, China, Iran, and North Korea would significantly increase U.S. defenses and decrease each state's ability to deter or compel the United States in a crisis. More kinetic power would increase defenses and crisis bargaining power only marginally, if at all. Perhaps most important, no amount of investment in industrial era technology would do much to defend against the damage being done by autocratic states' political-psychological operations or help the United States respond with information operations with American characteristics.

America's long-time policy of paying lip service to the transition from the industrial to the information era—while mainly resourcing industrial era technologies and methods—was merely a curiosity when the United States was at its unipolar apex and did not face Great Power competitors. That period is over. Today, the United States faces two autocratic rivals that are actively pioneering ways of using information age technologies and strategies to undermine the U.S.-led liberal international order. If the United States hopes to win this competition, it will need to change its approach. It will need to rethink the importance of defending its citizens, its firms, and its military from being quietly exploited by foreign militaries using steadily advancing cyber methods. It will need to resource its pursuit of key technologies that it has long prioritized on paper while paying whatever it takes to prevent adversaries from stealing that technology. It will have to decide how it will prevent adversaries from building and dominating the world's information networks and supply chains. Most important, it will have to change its mindset in such a way as to understand that it must defend virtual property and territory as it currently does to protect physical space. The industrial age is over, and it is time U.S. defense policy comes to terms with the emerging reality.

Notes

[1] Jonah Blank, "China Bends Another American Institution to Its Will," *The Atlantic*, October 10, 2019, available at <www.theatlantic.com/international/archive/2019/10/nba-victim-china-economic-might/599773/>.

[2] Richard B. Andres, "Cyber Conflict and Geopolitics by Richard B. Andres," *Great Decisions 2019*, Foreign Policy Association, 2019.

[3] Andrew F. Krepinevich, *The Military-Technical Revolution: A Preliminary Assessment* (Washington, DC: Center for Strategic and Budgetary Assessments, 1992), 6.

[4] Timothy L. Thomas, *Decoding the Virtual Dragon: Critical Evolutions in the Science and Philosophy of China's Information Operations and Military Strategy—The Art of War and IW* (Fort Leavenworth, KS: Foreign Military Studies Office, 2007).

[5] For an overview of early Chinese thinking on this topic, see Timothy L. Thomas, "Nation-State Cyber Strategies: Examples from China and Russia," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: NDU Press, 2009).

[6] On the Three Warfares doctrine, see Sangkuk Lee, "China's 'Three Warfares': Origins, Applications, and Organizations," *Journal of Strategic Studies* 37, no. 2 (2014), 198–221. For an overview of China's information-industrial policy, see William C. Hannas, James Mulvenon, and Anna B. Puglisi, *Chinese Industrial Espionage: Technology Acquisition and Military Modernization* (Abingdon, UK: Routledge, 2013). For an overview of underlying Chinese information and industrial strategy, see Dean Cheng, *Cyber Dragon: Inside China's Information Warfare and Cyber Operations* (Santa Barbara, CA: Prager, 2016); Gregory C. Allen, *Understanding China's AI Strategy: Clues to Chinese Strategic Thinking on Artificial Intelligence and National Security* (Washington, DC: Center for New American Security, February 2019), available at <www.cnas.org/publications/reports/understanding-chinas-ai-strategy>.

[7] Cheng, *Cyber Dragon*. See also Jacqueline Newmyer, "The Revolution in Military Affairs with Chinese Characteristics," *Journal of Strategic Studies* 33, no. 4 (August 2010), 483–504.

[8] Richard Andres, "Air Power and Cyber," in *Routledge Handbook of Air Power*, ed. John Andreas Olsen (Abingdon, UK: Routledge, 2018), 203–214.

[9] Such defenses include censorship, data localization, and cross-border data flow limits. See "Digital Trade," Congressional Research Service, March 29, 2019, available at <https://crsreports.congress.gov/product/pdf/IF/IF10770>; Elsa Kania, "China: Active Defense in the Cyber Domain," *The Diplomat*, June 12, 2015, available at <https://thediplomat.com/2015/06/china-active-defense-in-the-cyber-domain/>.

[10] IP Commission, *The IP Commission Report: The Report of the Commission on the Theft of American Intellectual Property* (Seattle: National Bureau of Asian Research, 2013), available at <http://ipcommission.org/report/IP_Commission_Report_052213.pdf>.

[11] IP Commission, *Update to the IP Commission Report: The Theft of American Intellectual Property: Reassessments of the Challenge and United States Policy* (Seattle: National Bureau of Asian Research, 2017), available at <http://ipcommission.org/report/IP_Commission_Report_Update_2017.pdf>.

[12] Jamie Crawford, "The U.S. Government Thinks China Could Take Down the Power Grid," CNN, November 21, 2014, available at <www.cnn.com/2014/11/20/politics/nsa-china-power-grid/index.html>.

[13] "An Interview with Paul M. Nakasone," *Joint Force Quarterly* 92 (1st Quarter 2019), 4–9, available at <https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-92/jfq-92_4-9_Nakasone-Interview.pdf>.

[14] Jeffrey Engstrom, *Systems Confrontation and System Destruction Warfare: How the Chinese People's Liberation Army Seeks to Wage Modern Warfare* (Santa Monica, CA: RAND, 2018), available at <https://www.rand.org/pubs/research_reports/RR1708.html>.

[15] "An Interview with Paul M. Nakasone."

[16] Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (New York: Penguin, 2010), 158.

[17] Chris Buckley and Paul Mozur, "How China Uses High-Tech Surveillance to Subdue Minorities," *New York Times*, May 22, 2019, available at <www.nytimes.com/2019/05/22/world/asia/china-surveillance-xinjiang.html>.

[18] *National Strategy to Secure 5G of the United States of America* (Washington, DC: The White House, March 2020), available at <www.whitehouse.gov/wp-content/uploads/2020/03/National-Strategy-5G-Final.pdf>.

[19] Of note—and an example of Moore's law of technological progress—while most consumers still have yet to upgrade to 5G wireless service around the world and its deployment is

still only in roll-out stages, Beijing is already signaling plans to develop 6G technology. See Peter Suciu, "5G Is Old News: China Wants 6G for Its Military," *The National Interest*, April 28, 2020, available at <https://nationalinterest.org/blog/buzz/5g-old-news-china-wants-6g-its-military-148806>.

[20] Tom Wheeler, "5G in Five Not So Easy Pieces," Brookings, July 9, 2019, available at <https://www.brookings.edu/research/5g-in-five-not-so-easy-pieces/>.

[21] Huawei argues that it would not share information with the Chinese Communist Party; however, China's Counter-Espionage Law of 2014 and National Intelligence Law in 2017 require companies to comply with requests from intelligence services. See Daniel Harsha, "Huawei, a Self-Made World-Class Company or Agent of China's Global Strategy?" Ash Center for Democratic Governance and Innovation at Harvard University, available at <https://ash.harvard.edu/huawei-self-made-world-class-company-or-agent-chinas-global-strategy>.

[22] For a discussion of how China uses these capabilities domestically, see Kai-Fu Lee, *AI Superpowers: China, Silicon Valley, and the New World Order* (Boston: Houghton Mifflin Harcourt, 2018).

[23] On state funding, see Henry Tugendhat, "Banning Huawei's 5G Won't Halt China's Tech Revolution," *The Guardian*, January 30, 2020, available at <www.theguardian.com/commentisfree/2020/jan/30/banning-huawei-5g-china-tech-revolution-free-market>. On Huawei undercutting competitors, see Alex Capri, "Beijing's Global 5G Ambitions Threaten to Disrupt Telecoms," *Nikkei Asian Review*, August 31, 2018, available at <https://asia.nikkei.com/Opinion/Beijing-s-global-5G-ambitions-threaten-to-disrupt-telecoms>.

[24] The Chinese Communist Party has a history of using economic threats to censor U.S. companies' and individuals' speech. See Jennifer Pan and Margaret Roberts, "These 3 Factors Explain Why the NBA and Other Companies Struggle to Push Back Against Chinese Censorship," *Washington Post*, October 16, 2019, available at <www.washingtonpost.com/politics/2019/10/16/these-factors-explain-why-nba-other-companies-struggle-push-back-against-chinese-censorship/>.

[25] Quantum technology has numerous national security implications beyond those tied to cyberspace and information technology.

[26] See Princeton University's Center for Information Technology Policy, *Implications of Quantum Computing for Encryption Policy*, Encryption Working Group Paper (Washington, DC: Carnegie Endowment for International Peace, April 25, 2019), available at <https://carnegieendowment.org/2019/04/25/implications-of-quantum-computing-for-encryption-policy-pub-78985>. For a more detailed discussion, see Richard A. Clarke and Robert K. Knake, *The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats* (New York: Penguin Press, 2019), chapter 16.

[27] E.B. Kania and J.K. Costello, "Quantum Technologies, U.S.-China Strategic Competition, and Future Dynamics of Cyber Stability," *2017 International Conference on Cyber Conflict* (Washington, DC: Institute of Electrical and Electronics Engineers, 2017), 89–96.

[28] David Grossman, "Did Google Just Achieve Quantum Supremacy?" *Popular Mechanics*, September 23, 2019, available at <www.popularmechanics.com/technology/a29190975/google-quantum-supremacy/>.

[29] The usual argument is that encryption is used by billions of users, whereas decryption is used by only a handful of intelligence organizations. As a result, it will be easier for a small number of intelligence agencies working on decryption to obtain expensive new quantum devices than for the general public to obtain use of quantum computers.

[30] Paul Smith-Goodson, "Quantum USA vs. Quantum China: The World's Most Important Technology Race," *Forbes*, October 11, 2019, available at <www.forbes.com/sites/moorinsights/2019/10/10/quantum-usa-vs-quantum-china-the-worlds-most-important-technology-race/>.

[31] Tim Johnson, "China Speeds Ahead of U.S. as Quantum Race Escalates, Worrying Scientists," *McClatchy DC*, October 23, 2017, available at <www.mcclatchydc.com/news/nation-world/national/national-security/article179971861.html>; Smith-Goodson, "Quantum USA vs. Quantum China."

[32] For a general discussion of these security and related threats posed by artificial intelligence (AI), see U.S. National Security Commission on Artificial Intelligence (NSCAI), *Interim Report* (Washington, DC: NSCAI, November 2019), 11–13.

[33] For an overview of the national security implications of AI, see Clarke and Knake, *The Fifth Domain*.

[34] Frank Luerweg, "The Internet Knows You Better than Your Spouse Does," *Scientific American*, March 14, 2019, available at <www.scientificamerican.com/article/the-internet-knows-you-better-than-your-spouse-does/>.

[35] Regarding China's resourcing, see Tiffany Lo, "Big Brother Is Watching You! China Installs 'The Worlds Most Advanced Video Surveillance System' with over 20 Million AI-Equipped Street Cameras," *Daily Mail*, September 25, 2017, available at <www.dailymail.co.uk/news/article-4918342/China-installs-20-million-AI-equipped-street-cameras.html>. On the Russian use of Facebook and other commercial AI, see Alina Polyakova, "Weapons of the Weak: Russia and AI-Driven Asymmetric Warfare," Brookings, November 15, 2018, available at <https://www.brookings.edu/research/weapons-of-the-weak-russia-and-ai-driven-asymmetric-warfare/>.

[36] See NSCAI, *Interim Report*, 17–20.

[37] See Martijn Rasser et al., *The American AI Century: A Blueprint for Action* (Washington, DC: Center for New American Security, December 2019), 9, available at <https://s3.amazonaws.com/files.cnas.org/documents/CNAS-Tech-American-AI-Century_updated.pdf?mtime=20200103081822>; NSCAI, *Interim Report*, 19.

[38] NSCAI, *Interim Report*, 1, 17–20.

[39] Released in 2015, but subsequently deemphasized in 2018 and 2019 by the Chinese government when "Made in China 2025" sparked international controversy, the document's goal was to comprehensively upgrade Chinese industry, making it more efficient and integrated so that it can occupy the highest parts of global production chains. The plan identified the goal of raising domestic content of core components and materials to 40 percent by 2020 and 70 percent by 2025. The focus for attaining dominance is aimed at 10 priority sectors: new advanced information technology, automated machine tools and robotics, aerospace and aeronautical equipment, maritime equipment and high-tech shipping, modern rail transport equipment, new energy vehicles and equipment, power equipment, agricultural equipment, new materials, and biopharma and advanced medical products. Quite clearly, dominance in new information technology was "aim #1," but within a wider construct of aims for modern technology dominance. See Scott Kennedy, "Made in China 2025," Center for Strategic and International Studies, June 1, 2015, available at <https://www.csis.org/analysis/made-china-2025>; Melissa Cyrill, "What Is Made in China 2025 and Why Has It Made the World So Nervous?" *China Briefing*, December 28, 2018, available at <www.china-briefing.com/news/made-in-china-2025-explained/>.

[40] Paul McLeary, "The Pentagon's Third Offset May Be Dead, But No One Knows What Comes Next," *Foreign Policy*, December 18, 2017, available at <foreignpolicy.com/2017/12/18/the-pentagons-third-offset-may-be-dead-but-no-one-knows-what-comes-next/>.

[41] Arthur Herman, "America's High-Tech STEM Crisis," *Forbes*, September 10, 2018, available at <www.forbes.com/sites/arthurherman/2018/09/10/americas-high-tech-stem-crisis/#f6730d8f0a25>.

[42] The hypothesis is mainly used in evolutionary biology and is based on Lewis Carroll's *Through the Looking-Glass*. It is termed *Red Queen* because populations have to "run" or evolve to stay in the same place, or else go extinct. See Leigh Van Valen, "A New Evolutionary Law," University of Chicago, 1973, available at <https://www.mn.uio.no/cees/english/services/van-valen/evolutionary-theory/volume-1/vol-1-no-1-pages-1-30-l-van-valen-a-new-evolutionary-law.pdf>.

[43] China outlines this strategy in its Medium- and Long-Term Plan for Science and Technology Development, 2006–2020. The plan calls for copying foreign innovation and focusing resources to achieve breakthroughs in targeted strategic areas of technological development and basic research. For an assessment of the plan and its outcome, see Hannas, Mulvenon, and Puglisi, *Chinese Industrial Espionage*. Private sources estimate the annual value of intellectual property stolen by China from the United States at $225 billion to $600 billion. See IP Commission, *The IP Commission Report*.

[44] McLeary, "The Pentagon's Third Offset May Be Dead, But No One Knows What Comes Next."

[45] *National Security Strategy of the United States of America* (Washington, DC: The White House, December 2017).

[46] For a similar perspective, see Michael C. Horowitz, "Artificial Intelligence, International Competition, and the Balance of Power," *Texas National Security Review* 1, no. 3 (May 2018).

[47] For example, see James Andrew Lewis, *Intellectual Property Protection* (Washington, DC: Center for Strategic and International Studies, January 2008), available at <https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/080802_LewisIntellectualProperty_Web.pdf>.