THE NEW BIG BROTHER

China and Digital Authoritarianism

A Democratic Staff Report
Prepared for the use of the
Committee on Foreign Relations
United States Senate
July 21, 2020

THE NEW BIG BROTHER

China and Digital Authoritarianism

A Democratic Staff Report
Prepared for the use of the
Committee on Foreign Relations
United States Senate
July 21, 2020

TABLE OF CONTENTS

Letter of Transmittal

United States Senate,
Committee on Foreign Relations,
July 21, 2020

Dear Colleagues: The growth and development of the digital domain worldwide has fundamentally changed how individuals, companies, and nations interact, work, and communicate – and with it the structure of global governance. Digitally-enabled technologies ranging from the Internet to mobile communications to emerging technologies, such as artificial intelligence, are accelerating the transmittal and receiving of information, enabling greater trade interactions and economic development, securing communications for our military and our allies, and aiding in the development of even newer, more capable technologies, amongst many other benefits. The United States has not only played a primary role in developing these new technologies, but it has worked to ensure the digital domain operates with openness, stability, reliability, interoperability, security, and respect for human rights.

These principles are under threat from authoritarian regimes, however, which see the advent of new technologies in a far more sinister light: as a means of surveilling and controlling populations, stifling the free flow of information, ensuring the survival of their governments, and as tools for malign influence campaigns worldwide. While multiple authoritarian governments have begun to utilize the digital domain in this manner, the People's Republic of China is at the forefront of developing and expanding a new, different, and deeply troubling governance model for the digital domain: digital authoritarianism.

The rise of this new and worrying model of digital authoritarianism holds the potential to fundamentally alter the character of the digital domain. The People's Republic of China is pressing forward—at times with astounding speed and focus—to build and expand digital authoritarianism through economic, political, diplomatic, and coercive means at home and abroad. The Chinese Communist Party is fostering digital authoritarianism within China's borders by developing an intrusive, omnipresent surveillance state that uses emerging technologies to track individuals with greater efficiency and bolstering its censorship apparatus to ensure information considered detrimental to the regime does not reach its citizens.

The government is shaping a legal system to strengthen the Party's manipulation of the tools of digital authoritarianism and expending vast sums of money to prop up Chinese companies that develop products that enable its authoritarian governance model. On the international level, China is exporting digitally enabled products and the training and expertise to other countries in an attempt to sway other nations to adopt this alternative, authoritarian model for the digital domain. As we have seem time and time again, with examples ranging from Marriott's pull-down menu to the NBA to Zoom's suspension of U.S. host accounts, China is seeking to utilize its newfound clout to reshape the rules of the road in cyberspace away from a free, unfettered, and secure environment to one that facilitates the growth of authoritarianism.

The United States, as the leader of the free world, must stand up for the principles and values that animate the international community and push back against the expansion of digital authoritarianism, using our economic prowess, unmatched innovative and scientific spirit, and ability to bring like-minded countries together. If the United States fails to lead the international community in assuring that governance of the digital domain is consistent with principles and values

that benefit all, then it will be China, not the international community at large, which will shape the future of the digital domain.

Given the critical importance of this issue for the future of global governance—and the clear need for the United States to reassert leadership within this space—I directed Senate Foreign Relations Committee staffers Michael Schiffer and Daniel Ricchetti to conduct a comprehensive study of China's effort to build and expand its model for digital authoritarianism and lay out recommendations for the U.S. government to consider. The report uses primary document research, news and subject-matter analysis, and interviews from both former government officials and nongovernmental experts. I want to thank Doug Levinson, Laura Truitt, Nina Russell, Nadhika Ramachandran, Elizabeth Shneider, and the SFRC Democratic Staff for their work on this report. I would also like to thank Julie Smith, Amy Studdart, and Tommy Ross for reviewing this report and the Congressional Research Service for their contributions.[1]

The report's comprehensive analysis of China's digital authoritarianism describes how the People's Republic of China is successfully developing and implementing its malign governance model internally and, increasingly, making inroads with other countries to also embrace its new digital doctrine. It further illustrates how the expansion of digital authoritarianism in China and abroad has drastic consequences for U.S. and allied security interests, the promotion of human rights, and the future stability of cyberspace. Consequently, the report calls for a series of both Congressional and Executive actions designed to counter China's efforts to expand its model of digital authoritarianism; to strengthen U.S. technological innovation; and, to reinvigorate our diplomatic endeavors around the globe on digital issues. I believe these recommendations are readily available for adoption and implementation by both Democrats and Republicans. Without bipartisan support and the full backing of the United States government, the American people will be far less secure in the digital domain in the years ahead, see a further breakdown of fundamental human rights, and witness the erosion of a free, stable, reliable, and secure digital domain while China's digital authoritarianism is allowed to flourish. American leadership on these issues has been sorely lacking the past three years. It is my sincere hope that this report will serve as a useful bipartisan rallying point for my colleagues in Congress so that we can work together to arrest the erosion of our position and to reassert American leadership and values on the world stage.

Sincerely,

Robert Menendez
Ranking Member

[1] The conclusions of the report do not necessarily reflect the views of the Congressional Research Service.

Preface on the Coronavirus

When the Senate Foreign Relations Committee Democratic Staff was first tasked with drafting this report, a consensus was emerging that the January 2018 National Defense Strategy's depiction of the "reemergence of long-term strategic competition" against such great power rivals as Russia and China would indeed be the "central challenge" to U.S. interests and security for the balance of the twenty-first century.[2] The Trump administration's characterization of the United States and China entering a "new era of strategic competition" received broad bipartisan support in the Senate as a largely accurate characterization – even if significant differences remained about how to structure U.S. national security policy accordingly.

Moreover, the suites of new and emergent digital technologies that are remaking the face of the U.S. and the global economies—including 5G infrastructure, social media, block-chain, digital surveillance, and genomics and biotechnology—are all widely acknowledged as being on the cutting edge of this new competition and fundamental for U.S. national security in the twenty-first century. Concerns regarding these emergent technologies are embedded in questions about the different, and competing, governance models for their use and control. These differing governance models are shaped by the form and nature of democratic and authoritarian states, which are continually developing, innovating, and operating in the digital space. Areas of competition between democratic and authoritarian states therefore encompass concerns about secure supply chains, privacy, human rights, standards, and the rules of the road for how these technologies would be used by the international community, including sharp power practices for technologies that shape and negotiate culture, education, and the media and are situated at the intersection of diplomacy, influence, and technology.

This report primarily examines how China's repressive government is creating a model of digital authoritarianism for the digital space and what it is doing to both strengthen the model in its own country and expand it internationally. However, the onset of the COVID-19 pandemic in December 2019 has raised a new set of questions about the state and nature of security challenges facing the United States in the twenty-first century, great power competition, and the diffusion and distribution of power in the international system. Moreover, the COVID-19 pandemic has stimulated additional questions about the governance of new and emergent digital technologies and the ways in which democratic and authoritarian states will seek to use them, for good or ill. Due to the fact that research, outside interviews, and the vast majority of the drafting of this report occurred before the outbreak of COVID-19, this report does not delve into how the novel coronavirus is shaping or may shape the future of the digital space as it pertains to digital authoritarianism. However, the connection between COVID-19 and digital authoritarianism is an important subject to examine in the future. This preface is intended to signal the significance of this topic and provide a brief roadmap for what issues may arise moving forward.

One key issue regarding COVID-19 and the digital space is that several democratic states, including South Korea and Taiwan, have adopted privacy practices to combat COVID-19 that previously were regarded as overbearing, all in the service of public health and responsive governance.[3] Meanwhile,

---

[2]Secretary of Defense James Mattis, *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge*, U.S. Department of Defense, Jan. 2018, at 2.

[3] Anthony Kuhn, "South Korea's Tracking Of COVID-19 Patients Raises Privacy Concerns," *NPR*, May 2, 2020; Milo Hsieh, "Coronavirus: Under surveillance and confined at home in Taiwan," BBC, Mar. 24, 2020.

China's extensive use of surveillance technologies, both to manage its own COVID-19 outbreak and to continue suppressing internal dissent and exerting control in Xinjiang and Tibet, has only served to exemplify the malign use of these tools in the hands of a government that is not answerable to its people. In many cases, the underlying technology and platforms used by different governments are the same or largely similar; it is governance models, political culture, transparency, norms of behavior, and the rule of law that separate the public good from political oppression. Questions regarding the use of these technologies have become only more serious, and the implications more clear, in the face of the pandemic.

Furthermore, these questions are not confined to matters of domestic policy. As the COVID-19 pandemic has progressed, an intense competition for global influence has emerged, with China and Russia seeking to use their digital toolkits to exploit the debates over the public health challenges the pandemic has created in the United States, Europe, and elsewhere. The purpose of controlling such a narrative is to make democracy look less attractive than a "capable" authoritarian model and to use the pandemic to attack the fabric of the democratic system itself.

As the COVID-19 pandemic has all too well illustrated, the brave new world of digital technological use and misuse is already upon us, and policymakers now need to move quickly to determine what sort of people—and what sort of governance—we will have in it.

Executive Summary

In an era in which rising authoritarianism is working to undermine the fabric of democratic institutions globally, the Internet and connected technologies represent a continually evolving domain that will fundamentally shape the future of politics, economics, warfare, and culture. Cyberspace remains relatively undefined and open to new rulemaking, standardization, and development. The United States has been and remains the premier digital innovator on the globe, and as such the primary entity capable of shaping the future of the digital environment. However, China's rapid rise in key fields, investment in new digital technologies, efforts abroad, and attempts at dominating international rule-making bodies are positioning it to erode the United States' leadership on technological issues and reconfigure the standards of the domain away from free, democratic values.

China has the largest number of Internet users on the planet, with more than 800 million Chinese citizens connected to some form of Internet.[4] Chinese technology companies such as Huawei and ZTE are at the forefront of developing and implementing fifth-generation (5G) telecommunications infrastructure. Chinese patent publications have surged in emerging technology fields such as artificial intelligence (AI), machine learning, and deep learning.[5] China's Belt and Road Initiative (BRI) contains an effort "to create a 'digital Silk Road' that will allow it to shape the future of the global Internet—and reinforce the Chinese Communist Party's leadership at home for decades to come."[6] These endeavors underline that China understands the importance of the digital domain to its domestic political stability and economic, political, and military rise, and wants to lead the globe in shaping the future of the digital world. It further demonstrates that China is executing a long-term plan to dominate the digital space.

While China's rise in the digital space is concerning to the United States in and of itself, an additional pressing issue facing not only the United States but the free world at large is how China is influencing and reshaping the Internet in its own political image. China's government structure can be defined as a repressive, authoritarian regime. In its 2020 Freedom of the World ratings, Freedom House labeled China as "not free" and described the regime as "increasingly repressive in recent years."[7] Despite China's authoritarian style of governing, the country's rise as a major economic and political player in the international sphere is providing the communist regime with increased status among other nations. As journalist Richard McGregor notes, China is pushing "the idea that

---

[4] François Godement et al., "The China Dream Goes Digital: Technology in the Age of Xi," *European Council of Foreign Relations*, Oct. 25, 2018; "China has 854 mln internet users: report," *Xinhua*, Aug. 30, 2019.

[5] World Intellectual Property Organization, *WIPO Technology Trends 2019: Artificial* Intelligence (Geneva: World Intellectual Property Organization, 2019), at 32; Louise Lucas & Richard Waters, "China and US Compete to Dominate Big Data," *Financial Times*, May 1, 2018.

[6] Stewart M. Patrick & Ashley Feng, "Belt and Router: China Aims for Tighter Internet Controls with Digital Silk Road," *The Internationalist* (blog), *Council of Foreign Relations*, July 2, 2018, https://www.cfr.org/blog/belt-and-router-china-aims-tighter-internet-controls-digital-silk-road; "Vision and Actions on Jointly Building Silk Road Economic Belt and 21st-Century Maritime Silk Road," *National Development and Reform Commission, Ministry of Foreign and Affairs and Ministry of Commerce of the People's Republic of China, with State Council Authorization*, March 2015, https://reconasia-production.s3.amazonaws.com/media/filer_public/e0/22/e0228017-7463-46fc-9094-0465a6f1ca23/vision_and_actions_on_jointly_building_silk_road_economic_belt_and_21st-century_maritime_silk_road.pdf.

[7] "Freedom of the World 2020: China," *Freedom House,* https://freedomhouse.org/country/china/freedom-world/2020 (last visited May 20, 2020).

authoritarian political systems are not only legitimate but can outperform Western democracies."[8] China's growing influence on the digital sphere is no different, as it enables China to promote an alternative model for the digital domain based on state control.

This model stands in stark contrast to what the United States and its allies espouse: a free and open Internet that encourages the free flow of information and commerce in ways that advance innovation and market-driven economic growth. Increasingly, other foreign nations, including Ecuador, Serbia, Zimbabwe, Uzbekistan, Kyrgyzstan, and Pakistan have or are looking to acquire Chinese information and communications technologies (ICT) and integrate them into their national infrastructures, opening up potential opportunities for abuse.[9] **China's efforts to advance and proliferate its ICT hardware and systems, both in China and overseas, represent not only a desire to continually expand its economy, but also a push to establish, expand, internationalize, and institutionalize a model for digital governance that this report describes as "digital authoritarianism."**[10]

Definition - Digital Authoritarianism
The use of ICT products and services to surveil, repress, and manipulate domestic and foreign populations.[11]

China's rise as a key player in the digital domain that uses its influence to promote digital authoritarianism presents fundamental security, privacy, and human rights concerns for the United States and the international community at large. Most troubling, China is working to undermine our democratic institutions and values. Due to the fundamental risks associated with the rise of China's digital authoritarianism, the Senate Foreign Relations Committee (SFRC) Democratic Staff examined the subject for the past year in an effort to provide a holistic study of the threats posed to the United States, our allies, and the international community. As part of its analysis, SFRC Democratic Staff reviewed primary source materials including reports, studies, and official Chinese government releases, as well as news sources, and conducted interviews with former U.S. government officials and non-governmental experts who work in the fields of human rights, technology, cybersecurity or China policy.

The examination conducted by SFRC Democratic Staff offers concerning insights about how China is leveraging new technologies to assert increased control over its population and strengthening its ties with other nations around the globe. This report underscores, for example, how China's government employs facial recognition technology and big data analysis tools to identify, discriminate, incarcerate, and "re-educate" Uyghurs living in Xinjiang, essentially creating a police state that flouts basic human rights and civil liberties. China is not just using these tools at home; it is also working to export its high-tech tools and authoritarian principles throughout the globe. While

[8] Richard McGregor, "Xi Jinping's Ideological Ambitions," *The Wall Street Journal,* Mar. 2, 2018.
[9] Paul Mozur et al., "Made in China, Exported to the World: The Surveillance State," *The New York Times*, Apr. 24, 2019; Abdi Latif Dahir, "China is exporting its digital surveillance methods to African countries," *Quartz Africa*, Nov. 1, 2018; Yau Tsz Yan, "China taking Big Brother to Central Asia," *Eurasianet*, Sept. 6, 2019, https://eurasianet.org/china-taking-big-brother-to-central-asia; "Chinese facial recognition tech installed in nations vulnerable to abuse," *CBS News*, Oct. 16, 2019; Justin Sherman, "U.S. Diplomacy Is a Necessary Part of Countering China's Digital Authoritarianism," *Lawfare*, Mar. 17, 2020, https://www.lawfareblog.com/us-diplomacy-necessary-part-countering-chinas-digital-authoritarianism.
[10] Alina Polyakova & Chris Meserole, "Exporting Digital Authoritarianism: The Russian and Chinese Models," *The Brookings Institution*, Aug. 2019.
[11] *See, e.g.,* Alina Polyakova & Chris Meserole, "Exporting Digital Authoritarianism: The Russian and Chinese Models," *The Brookings Institution*, Aug. 2019.

these examples are emblematic of the rise of China's digital authoritarianism, the fundamental takeaway of this report is that **if left unchecked, China, not the U.S. and our allies, will write the rules of the digital domain, opening the doors for digital authoritarianism to govern the Internet and associated technologies.**

This report provides an incisive examination of the key aspects of China's digital authoritarianism, the insidious nature of its proliferation inside China, the damage it is causing around the globe, and proposed legislative solutions and other measures the United States could adopt. In **Chapter 1**, the report describes China's internal model for digital authoritarianism and how China implements digital authoritarianism domestically. The chapter is divided into four subsections, with each subsection highlighting a specific aspect of China's digital authoritarianism model. The first subsection deals with China's "surveillance state," including how China utilizes artificial intelligence, facial recognition technologies, biometrics, surveillance cameras, and big data analytics to profile and categorize individuals quickly, track movements, predict activities, and preemptively take action against those considered a threat in both the real world and online. The second subsection looks into China's digital censorship apparatus and the tools that the Chinese government uses to control flows of data, such as the use of the "Great Firewall" to oversee information and block foreign technology platforms in China. The third subsection delves into China's legal system and how the government is implementing new laws that further strengthen the government apparatus that allows China's digital authoritarianism to flourish. Lastly, subsection four studies China's massive investments in companies that develop new technologies that are both predicated on and aid China's authoritarian principles.

Chapter 2 examines how China is exporting its digital technologies around the globe as a means of increasing its influence in other nations and, more dangerously, expanding the technologies and methods used for digital authoritarianism. This chapter looks at (1) China's export of underlying digital infrastructure technologies and (2) China's global proliferation of systems and technologies that run on those digital infrastructure technologies, thus advancing China's model for social control. Additionally, the chapter provides case studies of countries around the globe to demonstrate how China is integrating its technologies into these countries and how said integration impacts each nation.

Chapter 3 details China's efforts at strengthening its involvement and influence in intergovernmental fora. The chapter looks into how China is increasingly using fora such as the United Nations (UN), World Trade Organization (WTO), and other standards-setting bodies to push a Chinese-centric digital domain. China's involvement in these bodies is directly impacting the future rules of the road for cyberspace, and at a time when the United States seems to be receding from its traditional role as leader of the free world, China is filling the gap.

Chapter 4 elucidates the report's conclusions and policy recommendations. The recommendations focus on government actions, especially by Congress, to address and counter China's rise as a technological power and its desire to proliferate its model of digital authoritarianism. This section recommends legislation that establishes a public-private consortium aimed at creating a United States 5G alternative to Chinese technologies, legislation which institutes a Digital Rights Promotion Fund to help organizations push back against China's use and weaponization of mass surveillance, and legislation that would found a cyber military service academy. The report calls for the President to lead a coalition of countries to counter China's digital authoritarianism and push for a free, stable, unfettered, and secure digital domain. These recommendations stem from the understanding that

Congress has a special responsibility, as the constitutionally mandated lawmaking body of the United States, to develop and institute laws that protect against the rise and spread of China and digital authoritarianism. Such a role is especially important at a time when the executive branch has done little to combat digital authoritarianism, leaving the United States, our allies, our partners, and the global community at risk from the proliferation of digital authoritarianism.

This report contains two annexes. Annex 1 discusses the Trump administration's various cyber efforts and how these efforts have been deficient in countering China's continued rise as both a global geopolitical player and technological rival. Annex 2 provides an explanation of the 5G battle occurring between the United States and China. This overview highlights how China is attempting to dominate the 5G space and the present gaps in U.S. policy regarding this critical issue.

Chapter 1: Building the Model for Digital Authoritarianism Inside China

In his October 18, 2017 opening address to the 19th National Congress of the Chinese Communist Party (CCP, or the Party), General Secretary of the Communist Party of China and President of the People's Republic of China (PRC) Xi Jinping articulated a vision for restrictions in the digital domain. In the address, Xi stated:

> We will maintain the right tone in public communication…We will provide more and better online content and put in place a system for integrated internet management to ensure a clean cyberspace. We will implement the system of responsibility for ideological work… distinguish between matters of political principle, issues of understanding and thinking, and academic viewpoints, but we must oppose and resist various erroneous views with a clear stand.[12]

Xi's statement shows the CCP's broad objective: bolstering development of the Internet while mitigating the threats the Internet poses to CCP rule. Xi placed particular emphasis on the intent to ensure the CCP's control of ideas in cyberspace **by limiting access to information and ideas that run counter to the Party's ideology.** The promotion and preservation of CCP control of China's own digital domain undergirds the CCP's entire digital authoritarianism model. For the CCP to continue moving towards its long-term objectives of becoming the dominant player in the cyber domain and expanding its influence abroad, it must first ensure that it has pacified Chinese citizens and purged dissent. **In simple terms, China's digital authoritarianism starts at home.**

To accomplish this goal, the CCP has developed a unique model for digital authoritarianism implemented through a combination of technologies, regulations, and policies in four areas: (1) surveilling and tracking Chinese citizens, (2) exploiting and blocking data and content stored or transmitted on the digital domain, (3) implementing authoritarian cyber laws, and (4) directing massive investments in new technologies to secure the Party's future. The CCP uses these tools in concert with one another to shape the Chinese digital domain into a repressive, controlled space that stifles dissent, controls individual movement, curtails expression, flouts basic human rights for Chinese individuals, and helps enable and sustain the CCP's authoritarian rule.

The Surveillance State: How China Tracks its Citizens

The CCP regime has long depended on its ability to track and surveil China's population to ensure its survival and promulgate its authoritarian rule. The Party has used various methods to surveil individuals living in China since the inception of the communist regime. Digital tools provide the CCP with a range of new options that greatly enhance its ability to monitor citizens, turning China into a surveillance state. Emerging technologies such as facial recognition, biometrics, and other cutting edge tools enable China to profile and categorize individuals quickly in massive quantities, track movements, and preemptively take action against those considered a threat in both the real

[12] Xi Jinping, General Secretary of the Chinese Communist Party (CCP) and President of the People's Republic of China (PRC), "Secure a Decisive Victory in Building a Moderately Prosperous Society in All Respects and Strive for the Great Success of Socialism with Chinese Characteristics for a New Era," Speech Delivered at the 19th National Congress of the Communist Party of China, Oct. 28, 2017, http://www.xinhuanet.com/english/download/Xi_Jinping's_report_at_19th_CPC_National_Congress.pdf.

world and online.[13] The aforementioned technologies are combined with repressive regulations and burgeoning, omnipresent monitoring tools such as the Social Credit System currently being rolled out by the Chinese state.[14] This combination of technologies, tools, and regulations creates a structure where practically all citizens are surveilled, and those considered problematic to the regime face massive civil and political repression, including "mass arbitrary detention, forced political indoctrination, restrictions on movement, and religious oppression" as seen in Xinjiang.[15]

Facial recognition technology is a key tool used by the Party to monitor citizens. Chinese authorities combine traditional video surveillance with innovative big data analytics tools to allow the government to monitor its 1.4 billion citizens.[16] China is a world leader in the video surveillance industry. For example, two Chinese companies, the Hangzhou Hikvision Digital Technology Company (Hikvision) and the Zhejiang Dahua Technology Company (Dahua), together control one-third of the global market for video surveillance.[17] Companies such as Hikvision and Dahua have aided the buildout of an extensive closed-circuit television (CCTV) infrastructure in China.[18] China currently is deploying more than 200 million cameras throughout the country, and an estimated 560 million are expected to be installed by 2021.[19] The cameras themselves are useful to Chinese authorities, but the integration of cameras with burgeoning artificial intelligence (AI) programs, which allows authorities to churn through massive amounts of data and identify individuals more rapidly, makes the system far more effective and repressive.[20]

China is quickly emerging as a global leader in integrating artificial intelligence and facial biometric data to bolster surveillance capabilities. Chinese companies, ranging from older industry stalwarts such as Hikvision to newer startups like Yitu Technology (Yitu) and Megvii Technology Limited (Megvii), are using emerging technologies to analyze vast troves of images and information

---

[13] *See, e.g.,* Paul Mozur, "One Month, 500,000 Face Scans: How China is Using A.I. to Profile a Minority," *The New York Times*, Apr. 14, 2019; Josh Chin & Clément Bürge, "Twelve Days in Xinjiang: How China's Surveillance State Overwhelms Daily Life," *The Wall Street Journal*, Dec. 19, 2017.

[14] Christina Zhou and Bang Xiao, "China's Social Credit System is pegged to be fully operational by 2020 — but what will it look like?," *ABC News*, Jan. 1, 2020; Hollie Russon Gilman & Daniel Benaim, "China's Aggressive Surveillance Technology Will Spread Beyond Its Borders," *New America*, Aug. 23, 2018, https://www.newamerica.org/weekly/chinas-aggressive-surveillance-technology-will-spread-beyond-its-borders/; Steve Mollman, "China's new weapon of choice is your face," *Quartz*, Oct. 5, 2019

[15] Maya Wang, *China's Algorithms of Repression: Reverse Engineering a Xinjiang Police Mass Surveillance App*, Human Rights Watch, at 1 (May 2019); Steve Mollman, "China's new weapon of choice is your face," *Quartz*, Oct. 5, 2019; Hollie Russon Gilman & Daniel Benaim, "China's Aggressive Surveillance Technology Will Spread Beyond Its Borders," *New America*, Aug. 23, 2018, https://www.newamerica.org/weekly/chinas-aggressive-surveillance-technology-will-spread-beyond-its-borders/.

[16] World Bank, "China," https://data.worldbank.org/country/china (last visited Apr. 28, 2020).

[17] Editorial, *Konzept: 13 Tipping Points in 2018*, Deutsche Bank Research (January 2018), at 34, https://www.dbresearch.com/PROD/RPS_EN-PROD/PROD0000000000459680/13_Tipping_points_in_2018.pdf.

[18] Danielle Cave et al., "Mapping more of China's tech giants: AI and surveillance," *Australian Strategic Policy Institute*, Nov. 28, 2019, https://www.aspi.org.au/report/mapping-more-chinas-tech-giants; Chris Buckley & Paul Mozur, "How China Uses High-Tech Surveillance to Subdue Minorities," *The New York* Times, May 22, 2019; Ben Dooley, "Chinese Firms Cash in on Xinjiang's Growing Police State," *Agence France-Presse*, June 27, 2018.

[19] Amanda Lentino, "This Chinese Facial Recognition Start-Up Can Identify A Person in Seconds," *CNBC*, May 16, 2019; *The Economist*, "China: Facial Recognition and State Control," Oct. 24, 2018, https://www.youtube.com/watch?v=lH2gMNrUuEY (last visited Apr. 28, 2020); Thomas Ricker, "The US, like China, has about one surveillance camera for every four people, says report," *The Verge*, Dec. 9, 2019, https://www.theverge.com/2019/12/9/21002515/surveillance-cameras-globally-us-china-amount-citizens.

[20] Emily Feng, "How China Is Using Facial Recognition Technology," *NPR*, Dec. 16, 2019.

processed by cameras to strengthen facial recognition programs.[21] These programs support the underlying capabilities used to develop the databases that China's government and public security officials draw on to identify and monitor individuals. The databases rely on machine learning, a process in which "engineers feed data to artificial intelligence systems to train them to recognize patterns or traits."[22] The technology, however, is still imperfect. Accurate hits on recognizing individual faces depend on environmental factors, including lighting and the positioning of cameras.[23]

Technical flaws have not dissuaded the Chinese government from vastly expanding the scope and use of artificial intelligence for policing and surveillance, and the technology's efficacy continues to improve. The Chinese government aims to have a video surveillance network that is "omnipresent, fully networked, always working and fully controllable" by 2020.[24] Chinese government investment in these technologies is also slated to continue growing, with one expert stating that China's police is preparing to "spend an additional $30 billion in the coming years on techno-enabled snooping."[25] As China perfects these tools, it will acquire even more invasive capabilities for surveilling its people.

The CCP further augments its surveillance system with other important techniques that amplify surveillance capabilities. Chinese officials throughout the country are collecting and collating biometric data, such as DNA samples, fingerprints, voice samples, and blood types.[26] In a report on Xinjiang, Human Rights Watch (HRW) wrote that collecting this information "is part of the government's drive to form a 'multi-modal' biometric portrait of individuals and to gather ever more data about its citizens."[27]

The Chinese government has also extracted vast amounts of private data by using technologies to monitor activities and communications conducted over the Internet. For example, Chinese authorities force specific mobile applications on individuals in or entering Xinjiang.[28] One of these apps, Fengcai, downloads "all your text messages, contacts, call log history, calendar entries, and

---

[21] Australian Strategic Policy Institute, "Yitu," (last visited June 5, 2020), https://chinatechmap.aspi.org.au/#/company/yitu; Australian Strategic Policy Institute, "Megvii," (last visited June 5, 2020), https://chinatechmap.aspi.org.au/#/company/megvii; Danielle Cave et al., "Mapping more of China's tech giants: AI and surveillance," *Australian Strategic Policy Institute*, Nov. 28, 2019, https://www.aspi.org.au/report/mapping-more-chinas-tech-giants.

[22] Paul Mozur, "One Month, 500,000 Face Scans: How China is Using A.I. to Profile a Minority," *The New York Times*, Apr. 14, 2019.

[23] *Id.*

[24] Simon Denyer, "China's Watchful Eye," *The Washington Post*, Jan. 7, 2018.

[25] Paul Mozur, "Inside China's Dystopian Dreams: A.I., Shame and Lots of Cameras," *The New York Times*, July 8, 2018.

[26] Sigal Samuel, "China is installing a secret surveillance app on tourists' phones," *Vox*, July 3, 2019, https://www.vox.com/future-perfect/2019/7/3/20681258/china-uighur-surveillance-app-tourist-phone; Sui-Lee Wee, "China Uses DNA to Track Its People, With the Help of American Expertise," *The New York Times*, Feb. 21, 2019; Maya Wang, *China's Algorithms of Repression: Reverse Engineering a Xinjiang Police Mass Surveillance App*, Human Rights Watch, at 15 (May 2019); Phoebe Zhang, "China 'world's worst' for invasive use of biometric data," *South China Morning Post*, Dec. 5, 2019, https://www.scmp.com/news/china/society/article/3040710/china-worlds-worst-invasive-use-biometric-data.

[27] Maya Wang, *China's Algorithms of Repression: Reverse Engineering a Xinjiang Police Mass Surveillance App*, Human Rights Watch, at 15 (May 2019).

[28] Sigal Samuel, "China is Installing a Secret Surveillance App on Tourists' Phones," *Vox*, July 3, 2019; Joseph Cox, "China Is Forcing Tourists to Install Text-Stealing Malware at its Border," *Vice*, July 2, 2019, https://www.vice.com/en_us/article/7xgame/at-chinese-border-tourists-forced-to-install-a-text-stealing-piece-of-malware.

installed apps…this sensitive data is then sent, unencrypted, to a local server."[29] Chinese authorities employ Wi-Fi sniffers, which collect unique identifying information of networked devices, like laptops and smartphones, and can be used to read people's emails.[30] Each of these new technologies and mechanisms, whether cutting-edge facial recognition software or a smartphone app, offers Chinese authorities useful information to help surveil the population. The consequences of China's accelerated development of technologies to strengthen the surveillance state are dire.

China's authoritarian use of surveillance technology is particularly pervasive and intrusive in Xinjiang autonomous region in northwest China. Xinjiang is home to 25 million people, of which approximately eleven million are Muslim Uyghurs.[31] In this region, China has deployed its surveillance apparatus on a massive scale in an effort to track the population living there.[32] While this apparatus affects everyone in Xinjiang, it has disproportionately targeted Uyghurs and other Muslim minorities. Chinese officials believe Uyghurs hold "extremist and separatist ideas."[33] China's targeting has led to extreme political and religious repression against these groups.[34]

Since 2014, China has promulgated an extensive surveillance ecosystem throughout Xinjiang as part of its "Strike Hard Campaign against Violent Terrorism."[35] China has placed a large amount of surveillance equipment along streets and neighborhoods, including at checkpoints in major metropolitan zones. Chinese authorities use them primarily to monitor Uyghurs.[36] By combining the cameras with facial recognition technology, Chinese authorities can increasingly track Uyghur activity down to the individual level.

Omnipresent monitoring has essentially stifled Uyghur freedom of movement in the region and eliminated any semblance of personal privacy. Simple activities, such as an individual tracked by a camera traversing farther than 300 meters from designated safe areas (often designated as an

---

[29] Sigal Samuel, "China is Installing a Secret Surveillance App on Tourists' Phones," *Vox*, July 3, 2019.
[30] Charles Rollet, "In China's Far West, Companies Cash in on Surveillance Program that Targets Muslims," *Foreign Policy*, June 13, 2018; Human Rights Watch, "Big Data Fuels Crackdown in Minority Region," February 26, 2018, https://www.hrw.org/news/2018/02/26/china-big-data-fuels-crackdown-minority-region.
[31] Michael Hardy, "In Xinjiang, Tourism Erodes the Last Traces of Uyghur Culture," *Wired*, Apr. 4, 2020, https://www.wired.com/story/xinjiang-uyghur-culture-tourism/; Bryan Wood & Brennan Butler, "What is happening with the Uighurs in China," *PBS News Hour*, Oct. 4, 2019.
[32] Lindsay Maizland, "China's Repression of Uighurs in Xinjiang," *Council on Foreign Relations*, updated June 30, 2020, https://www.cfr.org/backgrounder/chinas-repression-uighurs-xinjiang; U.S. Department of State, "2018 Report on International Religious Freedom: China: Xinjiang," May 23, 2019, https://www.state.gov/reports/2018-report-on-international-religious-freedom/china-includes-tibet-xinjiang-hong-kong-and-macau/xinjiang/ (last visited July 10, 2020); Sheena Chestnut Greitens et al., "Understanding China's 'preventive repression' in Xinjiang," *The Brookings Institution*, Mar. 4, 2020.
[33] Lindsay Maizland, "China's Repression of Uighurs in Xinjiang," *Council on Foreign Relations*, updated June 30, 2020, https://www.cfr.org/backgrounder/chinas-repression-uighurs-xinjiang.
[34] *Id.;* U.S. Department of State, "2018 Report on International Religious Freedom: China: Xinjiang," May 23, 2019, https://www.state.gov/reports/2018-report-on-international-religious-freedom/china-includes-tibet-xinjiang-hong-kong-and-macau/xinjiang/ (last visited July 10, 2020); Sheena Chestnut Greitens et al., "Understanding China's 'preventive repression' in Xinjiang," *The Brookings Institution*, Mar. 4, 2020.
[35] Charles Rollet, "In China's Far West, Companies Cash in on Surveillance Program that Targets Muslims," *Foreign Policy*, June 13, 2018; Jérôme Doyon, "Counter Extremism in Xinjiang: Understanding China's Community-Focused Counter-Terrorism Tactics," *War on the Rocks*, Jan. 14, 2019, https://warontherocks.com/2019/01/counter-extremism-in-xinjiang-understanding-chinas-community-focused-counter-terrorism-tactics/; Maya Wang et al., *"Eradicating Ideological Viruses": China's Campaign of Repression Against Xinjiang's Muslims*, Human Rights Watch, at 4 (Sept. 2018).
[36] Chris Buckley et al., "How China Turned a City into a Prison," *The New York Times*, Apr. 4, 2019; Ben Westcott, "Chinese government loads surveillance app onto phones of visitors to Xinjiang: report," *CNN*, July 3, 2019.

individual's home or workplace) triggers an alert to police of the individual's movement.[37] At key transit checkpoints, Chinese authorities use face scans to determine whether Uyghurs can travel by cross-referencing the photo taken at a checkpoint to internal databases.[38]

Surveillance also negatively affects Uyghurs' ability to practice their faith freely. The *Agence France-Presse* found that, in 2018, Hikvision won a contract for its cameras to watch 967 mosques in Xinjiang's Moyu county alone, and that authorities use these cameras to "ensure that imams stick to a 'unified' government script."[39]

In addition to video surveillance, Uyghurs must accept other repressive controls that impinge on their basic human rights in order to not run afoul of authorities. From 2016 to 2017, Uyghurs were tricked into providing biometric data to authorities as part of a misleading government health program in Xinjiang labeled "Physicals for All."[40] Tahir Imin, a Muslim who participated in the health check, underscored the repressive nature of the supposed health screenings, saying that authorities told him he did not have the right to ask about the test results after they drew his blood, scanned his face, recorded his voice, and took his fingerprints.[41] The forced acquisition of Mr. Imin's physical and genetic data underlines China's desire to scoop new data from those living in Xinjiang and file it for future use.

Chinese public security authorities also vigorously monitor telecommunications devices used by Uyghurs. Various news outlets report that the Chinese government mandates Uyghurs install an application on electronic devices that allows the government to surveil their online activities, a fundamental intrusion on online privacy.[42] The application, called JingWang, is specifically "built with no safeguards in place to protect the private, personally identifying information of its users" and capable of scanning and sending information stored on a device to a remote server.[43] While Chinese authorities state that the purpose of the application is to detect what authorities deem to be illegal terroristic or religious material, Sophie Richardson, the China Director of Human Rights Watch, rightly asserts that the application is simply a new technical mechanism for gathering vast quantities of data on people.[44] The total effect of these systems is a repressive, authoritarian regime

---

[37] Adile Ablet & Alim Seytoff, "Authorities Testing Facial-Recognition Systems in Uyghur Dominated Xinjiang Region," *Radio Free Asia*, Jan. 25, 2018.
[38] Darren Byler, "I researched Uighur society in China for 8 years and watched how technology opened new opportunities – then became a trap," *The Conversation*, Sept. 18, 2019, https://theconversation.com/i-researched-uighur-society-in-china-for-8-years-and-watched-how-technology-opened-new-opportunities-then-became-a-trap-119615; Paul Mozur, "One Month, 500,000 Face Scans: How China is Using A.I. to Profile a Minority," *The New York Times*, Apr. 14, 2019.
[39] Ben Dooley, "Chinese Firms Cash in on Xinjiang's Growing Police State," *Agence France-Presse*, June 27, 2018.
[40] Sui-Lee Wee, "China Uses DNA to Track Its People, With the Help of American Expertise," *The New York Times*, Feb. 21, 2019.
[41] *Id.*
[42] Joseph Cox, "Chinese Government Forces Residents To Install Surveillance App With Awful Security," *Vice*, Apr. 9, 2018, https://www.vice.com/en_us/article/ne94dg/jingwang-app-no-encryption-china-force-install-urumqi-xinjiang.
[43] *Id.*
[44] Joseph Cox, "Chinese Government Forces Residents To Install Surveillance App With Awful Security," *Vice*, Apr. 9, 2019, https://www.vice.com/en_us/article/ne94dg/jingwang-app-no-encryption-china-force-install-urumqi-xinjiang; Yi Shu Ng, "China forces its Muslim minority to install spyware on their phones," *Mashable*, July 21, 2017, https://mashable.com/2017/07/21/china-spyware-xinjiang/#p2_q.Fw.DOqd.

designed to deprive Uyghurs and other ethnic minorities of their rights, turning cities such as Urumqi and Kashgar into veritable prison cities.[45]

The various elements of the surveillance apparatus in Xinjiang on their own provide important data to Chinese authorities, **but it is the centralization and rapid recall of the collected data that gives the authoritarian system increasing control and power.** This ability exists thanks in large part to the digital nature of the surveillance system, in which masses of data about individuals in Xinjiang are collected into central databases and rendered quickly retrievable by authorities, allowing them to uncover supposedly concerning behavior or respond swiftly to a situation.

China uses this digital process in Xinjiang, with police accessing information located on centralized servers from a mobile application.[46] The Integrated Joint Operations Platform (IJOP) is a central system developed by a subsidiary of China Electronics Technology Group Corporation (CETC), a major state-owned defense technology company in China. It integrates information from different "sources or machine sensors," such as video surveillance cameras or stolen Internet data, into "a massive dataset of personal information, and of police behavior and movements in Xinjiang."[47]

The centralized IJOP database syncs with the IJOP app, which authorities can access on a mobile device.[48] IJOP subsequently analyzes the data, although it is important to note that the level in which big data analytics plays a role in dissecting the data is unknown, and uses them to identify and predict patterns of behavior and, when necessary, notify police of people whom the data system categorizes as requiring investigation or even detention.[49] The IJOP app is the mechanism authorities use to communicate with the central information system and supplements the information going into the IJOP system, providing what Human Rights Watch (HRW) China Senior Researcher Maya Wang describes as "three broad functions: [the app] collects data, reports on suspicious activities or circumstances, and prompts investigative missions."[50] The IJOP sends alerts to police or government authorities to investigate suspicious activity, and through the app, authorities can send new information back to the IJOP, providing even more data to the system.[51] It

---

[45] *See* Chris Buckley et al., "How China Turned a City into a Prison," *The New York Times*, Apr. 4, 2019; Josh Chin & Clément Bürge, "Twelve Days in Xinjiang: How China's Surveillance State Overwhelms Daily Life," *The Wall Street Journal*, Dec. 19, 2017.

[46] Maya Wang, *China's Algorithms of Repression: Reverse Engineering a Xinjiang Police Mass Surveillance App*, Human Rights Watch, at 21 (May 2019); Human Rights Watch, "How Mass Surveillance Works in Xinjiang, China," May 2, 2019, https://www.hrw.org/video-photos/interactive/2019/05/02/china-how-mass-surveillance-works-xinjiang#:~:text=The%20Human%20Rights%20Watch%20report,of%20its%20%E2%80%9CStrike%20Hard%20Campaign (last visited July 10, 2020).

[47] Maya Wang, *China's Algorithms of Repression: Reverse Engineering a Xinjiang Police Mass Surveillance App*, Human Rights Watch, at 20 (May 2019).

[48] Human Rights Watch, "How Mass Surveillance Works in Xinjiang, China," May 2, 2019, https://www.hrw.org/video-photos/interactive/2019/05/02/china-how-mass-surveillance-works-xinjiang#:~:text=The%20Human%20Rights%20Watch%20report,of%20its%20%E2%80%9CStrike%20Hard%20Campaign (last visited July 10, 2020).

[49] Maya Wang, *China's Algorithms of Repression: Reverse Engineering a Xinjiang Police Mass Surveillance App*, Human Rights Watch, at 1, 19, 21, 22, 29 (May 2019).

[50] Nazish Dholakia, Media Desk Officer, Human Rights Watch, Interview with Maya Wang, "Interview: China's 'Big Brother' App," *Human Rights Watch*, May 1, 2019, https://www.hrw.org/news/2019/05/01/interview-chinas-big-brother-app.

[51] Nazish Dholakia & Maya Wang, "Interview: China's 'Big Brother' App - Unprecedented View into Mass Surveillance of Xinjiang's Muslims," *Human Rights Watch*, May 1, 2019, https://www.hrw.org/news/2019/05/01/interview-chinas-big-brother-app.

is through this cyclical, data-driven process that authorities in Xinjiang can truly implement digital authoritarianism in the region, as the sheer amount of information collected by authorities and the ability to understand that information in detail offer the Chinese government "the possibility of real-time, all-encompassing surveillance" that flouts basic human rights to privacy.[52]

The surveillance system in Xinjiang has aided in the detention of possibly more than 2 million Uyghurs, ethnic Kazakhs, and members of other Muslim groups in Xinjiang, according to the U.S. State Department.[53] Chinese officials have labeled these detention facilities as "vocational skills training centers" to "deradicalize" those suspected of extremism.[54] However, these centers are little more than arbitrary prison camps designed for political indoctrination. Uyghurs and other ethnic minorities imprisoned in internment camps are subject to abuse, squalid and unsanitary living conditions, lack of sleep and food, and forced political indoctrination.[55] In her account to *CNN*, Sayragul Sauytbay, a former employee at one of the detention facilities in Xinjiang who fled to Kazakhstan, recalls a CCP official telling her the primary objective of the detention system was to "turn the best of them [Uyghurs and other minorities] into Hans, while repressing and destroying the bad."[56] Sauytbay further describes that she suspected numerous human rights abuses, including sexual violence against female inmates and injections for non-compliant individuals.[57] Child separation due to forced detentions or exile is also a regular occurrence. Researcher Adrian Zenz highlights this separation process, writing that "[a]ccounts of Xinjiang Turkic Muslims in exile, including former detainees and their relatives, indicated that children as young as 2 years, with both parents in either internment or exile, were put into state welfare institutions or kept full-time in educational boarding facilities."[58] These accounts underline how China's surveillance state in Xinjiang abets the CCP's overt attempts to forcefully assimilate its ethnic minority populations into complying with the authoritarian government model proffered by Beijing.

While the authoritarian nature of the Chinese government's operations—especially against Uyghurs—in Xinjiang is alarming by itself, a second disturbing trend is the fact that China is supporting the development and use of technologies that conduct surveillance along racial and ethnic lines. Experts cited by the *New York Times* described China's usage of facial recognition to track Uyghurs as "the first known example of a government intentionally using artificial intelligence

---

[52] Nazish Dholakia & Maya Wang, "Interview: China's 'Big Brother' App - Unprecedented View into Mass Surveillance of Xinjiang's Muslims," *Human Rights Watch*, May 1, 2019, https://www.hrw.org/news/2019/05/01/interview-chinas-big-brother-app; United Nations, *UN Declaration of Human Rights*, *United* Nations, 3rd Session, (Dec. 10, 1948), https://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/eng.pdf. Article 12 of the UN Declaration of Human Rights states that "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks." *Id.*

[53] U.S. Department of State, "2018 Report on International Religious Freedom: China: Xinjiang," May 23, 2019. https://www.state.gov/reports/2018-report-on-international-religious-freedom/china-includes-tibet-xinjiang-hong-kong-and-macau/xinjiang/ (last visited July 10, 2020).

[54] Eva Dou, "China Acknowledges Re-Education Centers for Uighurs," *The Wall Street Journal,* Oct. 10, 2018.

[55] Matt Rivers & Lily Lee, "Former Xinjiang Teacher Claims Brainwashing and Abuse Inside Mass Detention Centers," *CNN*, May 9, 2019.

[56] *Id.*

[57] *Id.*

[58] Adrian Zenz, "Break Their Roots: Evidence for China's Parent-Child Separation Campaign in Xinjiang," *The Journal of Political Risk, Vol. 7, No. 7* (July 2019), http://www.jpolrisk.com/break-their-roots-evidence-for-chinas-parent-child-separation-campaign-in-xinjiang/.

for racial profiling."[59] China accomplishes racial classification by instructing facial recognition AI to categorize individuals based on social definitions of race or ethnicity.[60] While Beijing argues that sorting individuals via race or ethnicity is necessary to combat terrorism or quell "ethnic violence" in Xinjiang, China's use of emerging technologies and big data for racial profiling sets a terrifying precedent for how to effectively repress vulnerable populations and serves as a potential model for other authoritarians around the globe.[61]

In Xinjiang, Chinese government and police authorities retain what amounts to near absolute control of the entire ICT domain, and, through that control, have been able to repress and subjugate Uyghurs and other ethnic minorities in the region. It is important to note that, while all of China experiences some form of surveillance due to the CCP's authoritarian principles, the severity of controls in Xinjiang are not yet fully present throughout the rest of China. However, Xinjiang is the proving ground for China's digital authoritarianism model, and it serves as a clear example of how the CCP plans to use the digital domain to maintain and strengthen its authoritarian hold over the entire country. This plan may start to come into focus as early as 2020, as the Chinese government begins to implement a unified Social Credit System that captures all 1.4 billion citizens.[62]

China's Social Credit System is an intrusive tool used by all levels of the Chinese government to regulate corporate and citizen behavior. Various entities at the local or city level, such as police departments or health bureaus, gather swaths of behavioral information and data on individuals.[63] This data, which can range from jaywalking to donating blood, is then submitted to local databases.[64] Relevant information collected on individuals is also sent to the national level via the National Credit Information Sharing Platform (NCISP), in which the central government maintains a master database that other state agencies can access.[65] With this information on hand and a whole-of-government approach, the Social Credit System allows China to more robustly manage individual behavior and punish those deemed problematic by placing them on blacklists or no-fly lists.[66] Although presented in a more sanitized manner to entire Chinese populace, the Social Credit System opens up greater opportunities for the Chinese government to oppress all citizens in a manner similar to what the people in Xinjiang face, and the rapidity with which the government is moving forward in implementing these new authoritarian models of surveillance shows how important the issue is to the CCP.

The Censorship Apparatus: Exploiting and Blocking Digital Content

China's burgeoning surveillance state offers CCP authorities the ability to observe and maintain social control over its citizens and represents a fundamental component of its digital

---

[59] Paul Mozur, "One Month, 500,000 Face Scans: How China is Using A.I. to Profile a Minority," *The New York Times,* Apr. 14, 2019.
[60] *Id.*
[61] *Id.*
[62] Interview of Georgette Kerr, Vice President of Plurus Strategies, Aug. 16, 2019; World Bank, "China" https://data.worldbank.org/country/china (last visited Apr. 28, 2020).
[63] Kendra Schaefer & Ether Yin, *Understanding China's Social Credit System*, Trivium China, at 24 (Sept. 23, 2019), http://socialcredit.triviumchina.com/wp-content/uploads/2019/09/Understanding-Chinas-Social-Credit-System-Trivium-China-20190923.pdf.
[64] *Id.*
[65] *Id.* at 3, 24.
[66] *Id.*

authoritarianism model. A second, equally identifiable aspect of China's internal digital authoritarianism is the CCP's efforts at controlling flows of data. The CCP has spent decades building tools, mechanisms, and the infrastructure needed to cultivate a system for direct control of the content accessed by those in China. China's control over content has stunted political movements and silenced public criticism domestically by stifling access to a free Internet and tailoring CCP propaganda so that it efficiently targets the Chinese population.[67]

One of the fundamental fears of China's leadership when Internet access first arose in China in the 1990s was the technology's potential to introduce uncontrolled sources of information that could undermine CCP control by providing Chinese citizens with greater access to uncensored information and easier, more rapid communication.[68] To combat the possibility of the Internet operating as a democratizing force in China, China's Ministry of Public Security initiated the Golden Shield Project and debuted it in 2000.[69] Also known as the Great Firewall, it is central to the CCP's censorship efforts and uses a set of Internet traffic screening tools to filter out websites and content deemed inappropriate for China's Internet.[70] These tools span technical mechanisms, such as DNS poisoning, blocking the use of virtual private networks (VPN), and blocking IP addresses, to more human-based oversight, including monitors employed by the Ministry of Public Security.[71] Since its inception, the Great Firewall in China has developed into a complex censorship apparatus, essentially creating an entirely separate version of the Internet.[72]

More recently, Chinese companies have begun implementing emerging technologies, such as AI, to strengthen these censorship capabilities further through the automation of its monitoring and censorship processes.[73] China has also developed a culture of self-censorship.[74] The Chinese government requires Chinese firms to self-regulate content on their servers and platforms. For example, the *New York Times* noted in 2010 that major technology companies such as Baidu "employ throngs of so-called Web administrators to screen their search engines, chat rooms, blogs and other

---

[67] *See, e.g.,* Michael Anti, "Behind the Great Firewall of China," *TedGlobal2012* (video), *TED*, June 2012, https://www.ted.com/talks/michael_anti_behind_the_great_firewall_of_china/transcript?language=en#t-128890; Kenneth Roth, "China's Global Threat to Human Rights," *Human Rights Watch Global Report*, 2020.

[68] *See, e.g.,* Ping Punyakumpol, "The Great Firewall of China: Background," *Torfox* (A Stanford Project), *Stanford University*, June 1, 2011, https://cs.stanford.edu/people/eroberts/cs181/projects/2010-11/FreedomOfInformationChina/the-great-firewall-of-china-background/index.html; Nina Hachigian, "China's Cyber-Strategy," Foreign Affairs (Mar./Apr. 2001).

[69] Ping Punyakumpol, "The Great Firewall of China: Background," *Torfox* (A Stanford Project), *Stanford University*, June 1, 2011.

[70] *Id.*

[71] Oliver Farnan et al., "Poisoning the Well – Exploring the Great Firewall's Poisoned DNS Responses," *WPES '16: Proceedings of the 2016 ACM on Workshop on Privacy in the Electronic Society*, Oct. 2016, at 95, https://dl.acm.org/doi/pdf/10.1145/2994620.2994636; Cate Cadell, "Amid VPN crackdown, China eyes upgrades to Great Firewall," *Reuters*, July 20, 2017; Robert McMahon & Isabella Bennett, "U.S. Internet Providers and the 'Great Firewall of China,'" *Council on Foreign Relations*, Feb. 23, 2011; Marty Hu, "The Great Firewall: a technical perspective," Torfox (A Stanford Project), *Stanford* University, May 30, 2011, https://cs.stanford.edu/people/eroberts/cs181/projects/2010-11/FreedomOfInformationChina/author/martyhu/index.html.

[72] *See, e.g.,* "China Media Bulletin: 2019 internet freedom trends, Shutterstock censorship, Huawei "safe cities" (No. 140)," *Freedom House*, https://freedomhouse.org/report/china-media-bulletin/2020/china-media-bulletin-2019-internet-freedom-trends-shutterstock (last visited July 10, 2020).

[73] Yuan Yang, "Artificial intelligence takes jobs from Chinese web censors," *Financial Times*, May 22, 2018.

[74] Ping Punyakumpol, "The Great Firewall of China: Background," *Torfox* (A Stanford Project), *Stanford University*, June 1, 2011, https://cs.stanford.edu/people/eroberts/cs181/projects/2010-11/FreedomOfInformationChina/the-great-firewall-of-china-background/index.html

content for material that flouts propaganda directives."[75] A Chinese state media report said in 2013 that the government then employed approximately two million civilians who monitor social media and other Internet traffic to prevent social unrest and criticism of the government.[76]

The consequences of China's government enforcing tight censorship include (1) a population that is unaware of, or unable to acquire, accurate information about its government's policies and actions; and (2) continued consolidation of CCP rule. The Great Firewall has blocked digital news media content created by major international outlets not approved by the CCP.[77] According to Freedom House's analysis of Chinese censorship directives, China heavily censors news ranging from health and safety to "taboo subjects" such as the Cultural Revolution and Tiananmen Square.[78] Freedom House states that censorship against international news outlets is so prevalent that:

> Many international news outlets, especially those with Chinese-language websites, are blocked. For example, the *New York Times*, *Reuters*, and the *Wall Street Journal* have been censored for years, while the websites of the *Washington Post* and the *Guardian* were newly blocked in June 2019, likely as part of the government's efforts to tighten its grip on the flow of information surrounding the 30th anniversary of the Tiananmen Square crackdown.[79]

This censorship has aided the CCP's efforts to ensure that those living in China only receive information approved by the Party, a fundamental aspect of maintaining its status in China's public domain.

U.S. social media platforms such as Facebook, Instagram, Twitter, WhatsApp, Pinterest, and YouTube have also been blocked entirely from China's servers.[80] While censorship of these platforms has had the intended effect of barring many of those living in China from accessing information that would be deemed offensive to the Party, this censorship has also generated a second critical outcome. **Foreign technology platforms are restricted from operating in China, allowing Chinese platforms that offer similar services to thrive and expand into new markets.[81] Thanks to this market inefficiency, China now retains some of the most valuable Internet companies in the world by market capitalization, including Alibaba, Tencent, and Baidu.**[82] These companies essentially provide the panoply of Internet services wanted in China.

---

[75] Michael Wines et al., "China's Censors Tackle and Trip Over the Internet," *The New York Times*, Apr. 7, 2010.
[76] Katie Hunt & CY Xu, "China 'employs 2 million to police internet,'" *CNN,* Oct. 7, 2013; Google Translate: "Internet public opinion analyst: It's note about deleting posts," *Beijing News*, Oct. 3, 2013, http://epaper.bjnews.com.cn/html/2013-10/03/content_469152.htm?div=-1.
[77] Gerry Shih, "China adds Washington Post, Guardian to 'Great Firewall' blacklist," *The Washington Post*, June 8, 2019.
[78] "Freedom on the Net 2019: China," *Freedom House*, https://freedomhouse.org/country/china/freedom-net/2019 (last visited May 15, 2020); Sarah Cook, "The News China Didn't Want Reported in 2017," *The Diplomat*, Jan. 27, 2018.
[79] "Freedom on the Net 2019: China," *Freedom House*, https://freedomhouse.org/country/china/freedom-net/2019 (last visited May 15, 2020); Gerry Shih, "China adds Washington Post, Guardian to 'Great Firewall' blacklist," *The Washington Post*, June 8, 2019.
[80] "Freedom on the Net 2019: China," *Freedom House*, https://freedomhouse.org/country/china/freedom-net/2019 (last accessed May 15, 2020); Sherisse Pham, "China adds Pinterest to list of banned sites," *CNN*, Mar. 17, 2017; GreatFire.Org, "Censorship of Alexa Top 1000 Domains in China," https://en.greatfire.org/search/alexa-top-1000-domains (last visited June 26, 2020).
[81] *See, e.g.,* Tim Wu, "China's Online Censorship Stifles Trade, Too," *The New York Times*, Feb. 4, 2019.
[82] J. Clement, "Market value of the largest internet companies worldwide 2019," *Statista*, June 3, 2020, https://www.statista.com/statistics/277483/market-value-of-the-largest-internet-companies-worldwide/; Tim Wu,

Alibaba offers e-commerce services, and Tencent delivers social media, entertainment, and gaming, negating the need for other platforms where information flows freely.[83] The consequences of this are a Chinese population that is reliant on platforms that further cement the CCP's control of the digital domain.

China's censorship extends beyond simply separating China's Internet from outside information. China's censors are using offensive tools and aggressive tactics that reach far beyond scrubbing and blocking data to ensure robust censorship. Citizen Lab, an interdisciplinary laboratory based at the University of Toronto, asserts that the Chinese government used an attack tool, which they label the "Great Cannon," to extend the reach of China's censorship.[84] The Great Cannon, while co-located within the Great Firewall, is a "separate offensive system" that "hijacks traffic to (or presumably from) individual IP addresses, and can *arbitrarily replace unencrypted content as a man-in-the-middle*."[85] China used the Great Cannon to conduct Distributed Denial of Service (DDoS) attacks on servers rented by GreatFire.org, an advocacy nonprofit that challenges China's Great Firewall, and GitHub pages run by GreatFire.org in 2015.[86]

China's use of an offensive cyber tool for censorship purposes is revelatory because it shows China taking action beyond its borders to ensure censorship within its borders. China is also cracking down on tools that ordinary Chinese citizens use to overcome the Great Firewall, such as virtual private networks.[87] In January 2019, the *Financial Times* showed how China is cracking down on individual use of VPN tools. The *Financial Times* highlighted how a Chinese man, Zhu Yunfeng, received a significant fine for accessing foreign websites and using the VPN Lantern, as well as how another individual, Pan Xidian, received a jail sentence for VPN use and composing "inappropriate" Twitter posts.[88] Providers of these tools are receiving even stiffer sentences, such as Wu Xiangyang, who in 2017 received a five and a half year jail sentence and 500,000 yuan fine (approximately $70,650) for selling software that circumvented China's Internet censorship controls.[89] The result of these efforts is a censorship system that can rely on a variety of continually evolving tools to ensure that online and social media users can be targeted if they post comments that the government and Party deem politically sensitive. Everyday citizens consequently retain fewer avenues to acquire non-CCP approved information.

"China's Online Censorship Stifles Trade, Too," *The New York Times*, Feb. 4, 2019; Simon Denyer, "China's Scary Lesson to the World: Censoring the Internet Works," *The Washington Post*, May 23, 2016.

[83] Australian Strategic Policy Institute, "Tencent," https://chinatechmap.aspi.org.au/#/company/tencent (last visited June 5, 2020); Australian Strategic Policy Institute, "Alibaba," https://chinatechmap.aspi.org.au/#/company/alibaba (last visited June 5, 2020).

[84] Bill Marczak et al., *China's Great Cannon*, The Citizen Lab, Munk School of Global Affairs and Public Policy, University of Toronto (Apr. 10, 2015), https://citizenlab.ca/2015/04/chinas-great-cannon/.

[85] *Id.*

[86] *Id.*

[87] Cisco, "What Is a VPN? - Virtual Private Network," https://www.cisco.com/c/en/us/products/security/vpn-endpoint-security-clients/what-is-vpn.html (last visited June 7, 2019). A virtual private network, or VPN, is an encrypted connection over the Internet from a device to a network. The encrypted connection helps ensure that sensitive data is safely transmitted. It prevents unauthorized people from eavesdropping on the traffic and allows the user to conduct work remotely. *Id.*

[88] Yuan Yang, "China Turns Up Heat on Individual Users of Foreign Websites," *Financial Times*, Jan. 7, 2019.

[89] Benjamin Haas, "Man in China Sentenced to Five Years' Jail for Running VPN," *The Guardian*, Dec. 21, 2017.

The Legal System: China's Implementation of Authoritarian Cyber Laws

In a position paper titled "China's Digital Rise – Challenges for Europe," authors Kristin Shi-Kupfer and Mareike Ohlberg of the Mercator Institute for China Studies note that, when developing new technologies, an unofficial Chinese government slogan is "first develop, then regulate."[90] This unofficial slogan demonstrates that the government has prioritized the maturation of its emerging digital technologies and then, as they are integrated into society, regulates their use as needed. With China's continued rise in this domain, the Chinese government now is increasingly implementing stringent rules and regulations to ensure that the cyber domain remains compliant with Party strictures. The regulations China has implemented recently expand government control over cyberspace at the legal level, making its myriad authoritarian actions to quell dissent and promote Chinese propaganda seem lawful.

In November 2016, the 24th Session of the Standing Committee of the 12th National People's Congress passed the Cybersecurity Law of the People's Republic of China, fundamentally altering the cyber landscape in China.[91] Coming into effect on June 1, 2017, and enforced by the Cyberspace Administration of China (CAC) and other related ministries, the law affords government entities broad authority to regulate and control the digital environment in China.[92] In addition to the Cybersecurity Law, the Chinese government is layering various regulations on top of it to give the law both more clarity and teeth.[93]

While the Cybersecurity Law and relevant additional regulations put forth a variety of new stipulations on individuals and companies, there are a few provisions of the law and related regulations that are especially emblematic of China's effort at increasing social and political control of the digital domain. One of these is the repeated vague references in the Cybersecurity Law to national security needs, opening individuals and organizations to intrusive and potentially abusive reviews of cyber activity.[94] According to Georgette Kerr, a cyber-expert at Plurus Strategies, "the law and associated directives have compelled network operators to cooperate with law enforcement in addressing vaguely defined threats to national security [and] established intrusive national security reviews," seen in clauses such as Article 28.[95] Article 28 states that "network operators shall provide technical support and assistance to public security organs and national security organs that are

---

[90] Kristin Shi-Kupfer & Mareike Ohlberg, *China's Digital Rise: Challenges for Europe,* Mercator Institute for China Studies, Vol. 7, at 9 (Apr. 2019), https://www.merics.org/sites/default/files/2019-04/MPOC_No.7_ChinasDigitalRise_web_3.pdf.

[91] IT Advisory KPMG China, "Overview of China's Cybersecurity Law," *KPMG*, Feb. 2017, at 4, https://assets.kpmg/content/dam/kpmg/cn/pdf/en/2017/02/overview-of-cybersecurity-law.pdf; Samuel Stolton, "Chinese cybersecurity law is a 'loaded weapon,' senior US official says," *Euractiv*, Feb. 27, 2019, https://www.euractiv.com/section/cybersecurity/news/chinese-cybersecurity-law-is-a-loaded-weapon-senior-us-official-says/.

[92] Interview of Georgette Kerr, Vice President of Plurus Strategies, Aug. 16, 2019; Samm Sacks, "China's Cybersecurity Law Takes Effect: What to Expect," *Lawfare*, June 1, 2017, https://www.lawfareblog.com/chinas-cybersecurity-law-takes-effect-what-expect.

[93] Samm Sacks, "China's Cybersecurity Law Takes Effect: What to Expect," *Lawfare*, June 1, 2017, https://www.lawfareblog.com/chinas-cybersecurity-law-takes-effect-what-expect; Samm Sacks et al., "China's Cybersecurity Reviews for 'Critical' Systems Add Focus on Supply Chain, Foreign Control (Translation)," *New America*, May 24, 2019, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinas-cybersecurity-reviews-critical-systems-add-focus-supply-chain-foreign-control-translation/.

[94] Interview of Georgette Kerr, Vice President of Plurus Strategies, Aug. 16, 2019.

[95] *Id.*

safeguarding national security and investigating criminal activities in accordance with the law."[96] **The law in effect uses national security as a legal mechanism to assert its authoritarian control over data flows in China in new ways.** The law additionally affords the government even more dystopian powers in special circumstances dictated by the State Council. Under Article 58 of the law, authorities can "take temporary measures regarding network communications in a specially designated region, such as limiting such communications," further underscoring how the 2017 law fully empowers the Chinese government to control the digital domain anytime the government claims such control is necessary.[97]

The implementation of the Cybersecurity Law also imposes serious controls and restrictions on foreign companies operating in China. Jack Wagner, an Asia analyst at PGI Intelligence writing in *The Diplomat*, notes that "several of the provisions… have become a cause for concern among foreign companies."[98] For example, Wagner highlights data localization rules in the law, under which foreign companies would need to store data on Chinese servers.[99] Due to data localization laws, firms would either need to "invest in new data servers in China which would be subject to government spot-checks, or incur new costs to hire a local server provider, such as Huawei, Tencent, or Alibaba, which have spent billions in recent years establishing domestic data centers as part of Beijing's 12th Five-Year Plan (2011-2015)."[100] Neither of these options are positive for companies looking to operate in China, as they open up sensitive information to intrusive snooping by Chinese authorities.

Another key issue stemming from China's burgeoning legal structures pertaining to the digital domain is the continued erosion of online anonymity. Samm Sacks and Paul Triolo, writing in *Lawfare*, describe how the CAC added four regulations in August and September of 2017 regarding online activity that effectively reduce online anonymity. These four regulations are 1) the Internet Forum Service Management Regulation, 2) the Internet Threat Comments Service Management Regulation, 3) the Internet User Public Account Information Services Management Regulation, and 4) the Management Rules of Internet Group Information Services.[101] The regulations disallow online anonymity by requiring "foreground voluntary name, background real name." This requirement means that users can choose a screen name or appear anonymous, but their actual identity information will still be stored with the Ministry of Public Security.[102] Sacks and Triolo note that, by reducing anonymity online, Chinese authorities receive more real data to add to their burgeoning databases on citizen behavior such as the Social Credit System, and by extension, further their oversight of the population.[103] Similarly, in November 2018, the government implemented new regulations granting "the Ministry of Public Security (MPS) broad powers over the computer networks of companies in China."[104] The rule, labeled "Regulations on Internet Security Supervision

---

[96] Rogier Creemers et al., "Translation: Cybersecurity Law of the People's Republic of China [Effective June 1, 2017]," *New America*, June 29, 2019, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/.

[97] *Id.*

[98] Jack Wagner, "China's Cybersecurity Law: What You Need to Know," *The Diplomat*, June 1, 2017.

[99] *Id.*

[100] *Id.*

[101] Samm Sacks & Paul Triolo, "Shrinking Anonymity in Chinese Cyberspace," *Lawfare*, Sept. 25, 2017, https://www.lawfareblog.com/shrinking-anonymity-chinese-cyberspace.

[102] *Id.*

[103] *Id.*

[104] Insikt Group, "China's New Cybersecurity Measures Allow State Police to Remotely Access Company Systems," *Recorded Future*, Feb. 8, 2019, https://www.recordedfuture.com/china-cybersecurity-measures/.

and Inspection by Public Security Organs," provides MPS with new opportunities to conduct on site and remote site inspections of company computers, copy user information, have police backup during inspections to ensure company compliance, and monitor company adherence to censorship laws.[105]

Although the Chinese government may be reacting to some valid cybersecurity concerns in building and growing the legal frameworks surrounding cyber activity, it is no accident that this framework simultaneously provides legitimacy to China's authoritarian actions in the digital domain. As seen above, the various laws and regulations implemented by the Chinese government provide censors, law enforcement, intelligence agencies, and other entities with legal cover to impinge on privacy rights and conduct undue searches and seizures of information contained or passed in cyberspace. **The ramifications of the promulgation of China's digital laws include the establishment of an Internet governance framework that ensures, at the most fundamental level, CCP regime survival and operates as a direct contrast to the systems and laws promulgated by the U.S. and its allies.**

China's Investment in Technologies Predicated on Authoritarian Principles

China's growing promotion of digital authoritarianism has coincided with its rise as a technological leader. These technologies, as demonstrated above, make surveillance and censorship both easier and stronger than ever before for CCP authorities. **As such, the rise of digital authoritarianism in China is facilitated by the continued development of new technologies consistent with authoritarian principles.** Consequently, the CCP continues to emphasize investment and innovation in new technologies, which will further strengthen its ability to exercise authoritarian rule in China.[106]

China's focus on investing in cyber and digital technologies comes from the highest echelons of CCP leadership, who have advocated new technologies as critical to China's rise as a global power. The Made in China 2025 initiative was a state-led industrial policy intended "to make China dominant in global high-tech manufacturing" by using "government subsidies, mobiliz[ing] state-owned enterprises, and pursu[ing] intellectual property acquisition to catch up with—and then surpass—Western technological prowess in advanced industries."[107] The policy prioritizes ten major sectors, of which one is new information technology.[108] Made in China 2025 operated as a ten-year plan driving China's industrial development, and its prioritization of the technologies within the digital domain accentuates the CCP's desire to strengthen Chinese-made ICT products and services. Additionally, China's Internet Plus policy, also unveiled in 2015, "aims to capitalize on China's huge

---

[105] *Id.*

[106] *See, e.g.,* Sophia Yan, "Chinese surveillance grows stronger with technology that can recognise people from how they walk," *Telegraph*, Nov. 6, 2018; Statement of William Carter, Deputy Director and Fellow, Technology Policy Program, *Chinese Advances in Emerging Technologies and their Implications for U.S. National Security*, Hearing before the U.S. House of Representatives Armed Services Committee, Jan. 9, 2018, at 2, 6.

[107] James McBride & Andrew Chatzky, "Is 'Made in China 2025' a Threat to Global Trade?" *Council on Foreign Relations,* May 13, 2019. *See also* Emily Crawford, "Made in China 2025: The Industrial Plan that China Doesn't Want Anyone Talking About," *PBS*, May 7, 2019.

[108] Press Release, State Council of the People's Republic of China, "Made in China 2025," May 19, 2015, http://english.www.gov.cn/policies/latest_releases/2015/05/19/content_281475110703534.htm.

online consumer market by building up the country's domestic mobile Internet, cloud computing, massive amounts of data (big data), and the Internet of Things sectors."[109]

CCP leaders have also delivered statements further backing China's emphasis on developing its cyber capabilities. General Secretary Xi, in an October 9, 2016 Politburo meeting on cyber and IT issues, asserted that China "must accelerate the advancement of domestic production, indigenous and controllable substitution plans, and the building of secure and controllable information technology systems."[110] Wang Huning, a member of the Standing Committee of the Politburo, relayed Xi's stance on information technology development in December 2017, saying "[CCP] General Secretary Xi Jinping emphasized the need to…deepen Internet and information technology, build a cyber superpower, and advance society through a digital China; and to advance Internet, big data, artificial intelligence, and data economy, etc."[111]

In addition to highlighting China's desire to strengthen information technologies, CCP leaders' statements often denote the need for sanitizing cyberspace from what the Party believes to be toxic content. Chen Yixin, the Secretary-General of the CCP's Legal Affairs Commission, highlighted this priority in January 2019, stating that a "small incident can form into a vortex of public opinion" on the Internet.[112] Zhuang Rongwen, Vice Minister of the Central Propaganda Department, and Director of the Central Cybersecurity and Informatization Office and State Internet Information Office, provided additional context to China's desire to control the digital domain in September 2018 with the assertion that:

> The Internet has become a main battlefield, main battleground, and most forward position in propaganda and public opinion work. To grasp leadership authority in online ideological work, we must not only give full rein to the main force role of Party members, cadres, and mainstream media editors, pushing the main forces onto the main battlefield; we must also give full rein to the dominant role of the majority of Internet users, and fight a people's war for the governance of the online environment.[113]

To CCP leadership, the digital domain is a space that must be controlled by the Party. As such, development of new digitally enabled technologies must operate in line with Party

---

[109] Meia Nouwens & Helena Legarda, *Emerging technology dominance: what China's pursuit of advanced dual-use technologies means for the future of Europe's economy and defence innovation*, China Security Project at MERICS and The International Institute for Strategic Studies, at 5 (Dec. 2018); Press Release, State Council of the People's Republic of China, "China unveils Internet Plus action plan to fuel growth," July 4, 2015, http://english.www.gov.cn/policies/latest_releases/2015/07/04/content_281475140165588.htm.

[110] Michael Martina, "Xi Says China Must Speed Up Plans for Domestic Network Technology," *Reuters*, Oct. 9, 2016. *See also* "The Political Bureau of the Central Committee of the Communist Party of China Conducted the 36th Collective Study on the Implementation of the Cyber Power Strategy," *Xinhua News Agency*, Oct. 9, 2016, http://www.gov.cn/xinwen/2016-10/09/content_5116444.htm (translated from Chinese).

[111] Graham Webster et al., "Wang Huning's Speech at the 4th World Internet Conference in Wuzhen," *New America*, Dec. 13, 2017, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/wang-hunings-speech-4th-world-internet-conference-wuzhen/.

[112] Chris Buckley, "2019 Is a Sensitive Year for China. Xi is Nervous," *The New York Times*, Feb. 25, 2019.

[113] Rogier Creemers et al., "Translation: China's New Top Internet Official Lays Out Agenda for Party Control Online," *New America*, Sept. 24, 2018, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinas-new-top-internet-official-lays-out-agenda-for-party-control-online/.

principles. Without such control, CCP leaders fear these technologies could weaken the CCP's hold over its citizens.

The CCP has implemented industrial policies with massive investments in technology and lucrative conditions for Chinese firms operating in digital fields. China's research and development spending grew by more than 17% each year from 2010 to 2017 and in 2018 hit a record high of 2.19 percent of GDP.[114]

These investments have only continued to accelerate. China has spent incredible amounts of resources bolstering startups working in the surveillance field. The *New York Times* reported that, in May 2018, "the upstart A.I. company SenseTime raised $620 million, giving it a valuation of about $4.5 billion. Yitu raised $200 million [in June 2018]. Another rival, Megvii, raised $460 million from investors that included a state-backed fund created by China's top leadership."[115] The European Union Chamber of Commerce in China, in its "China Manufacturing 2025" report, tells a similar story of how China is boosting its domestic telecommunications industry. The report notes that:

> The Chinese Government has used a variety of policy instruments to support the development of its domestic telecommunications equipment industry. One of the most prominent has been the use of catalogues of domestic high-technology products, as well as an equivalent list for exports. Firms whose products are included in these catalogues receive benefits, such as preferential tax rates and low-interest loans from state-owned banks.[116]

China's firms have found that operating in zones that promulgate digital authoritarianism in China is an extremely profitable business. In Xinjiang, Hikvision received approximately $290 million for security related contracts, including a "social prevention and control system" and a program implementing facial-recognition surveillance in and around mosques.[117] Combined with Dahua's own contracts in Xinjiang, Hikvision and Dahua have won "at least $1.2 billion in government contracts for 11 separate, large-scale surveillance projects across Xinjiang."[118] The fact that Chinese firms are receiving such strong returns for working in fields that fundamentally promote authoritarian rule in China highlight Chinese leadership's willingness to invest in technologies that enable greater social and digital control.

China's leadership firmly believes that the country is on a path towards becoming a global power capable of exerting influence practically anywhere, and that a core aspect of achieving this goal is

---

[114] "China's spending on R&D rises to historic high," *Xinhua* News, Sept. 7, 2019, http://www.xinhuanet.com/english/2019-09/07/c_138373248.htm; Niall McCarthy, "China Is Closing The Gap With The U.S. In R&D Expenditure," *Forbes*, Jan. 20, 2020; Zhang Jun, "Will China Be the Next Tech Powerhouse? Maybe with the Next 20 Years of Sustained Investment," *South China Morning Post*, Aug. 1, 2018, https://www.scmp.com/comment/insight-opinion/united-states/article/2157728/will-china-be-next-tech-powerhouse-maybe-next.

[115] Paul Mozur, "Inside China's Dystopian Dreams: A.I., Shame and Lots of Cameras," *The New York Times*, July 8, 2018.

[116] *China Manufacturing 2025*, European Union Chamber of Commerce in China, at 26 (2017), http://docs.dpaq.de/12007-european_chamber_cm2025-en.pdf.

[117] Ben Dooley, "Chinese Firms Cash in on Xinjiang's Growing Police State," *Agence France-Presse*, June 27, 2018. *See also* Chris Buckley & Paul Mozur, "How China Uses High-Tech Surveillance to Subdue Minorities," *The New York Times*, May 22, 2019.

[118] Charles Rollet, "In China's Far West, Companies Cash in on Surveillance Program that Targets Muslims," *Foreign Policy*, June 13, 2018.

dominance in the digital domain. For China's government, this dominance starts at home, and its current policies and investments underscore the CCP's focus on strengthening the domestic base for information technologies.

Chapter 2: Exporting Digital Authoritarianism – China on the Global Cyber Stage

China's leadership is increasingly confident that its governing model for the digital space represents the future of the domain and is doing its best to convince governments around the world that this is the case. Digital authoritarianism in China is enabling the CCP to impose considerable control over its population and the information accessible to those in the country, providing the regime with increased security from democratizing forces and further opportunities for economic and technological growth. As China continues to perfect the tools that comprise its model of digital authoritarianism, its leaders have become more aware of the geopolitical and economic benefits of exporting both the technologies and the methods of digital authoritarianism to perpetuate its model of extensive censorship and automated surveillance.[119]

Chinese leaders are using information and communications technology (ICT) and digital media to increase their power abroad as well as at home, including by building on the Belt and Road Initiative's (BRI) infrastructure, trade, training, and investment links between China and more than 60 other countries.[120] At the first BRI forum in May 2017, Chinese President Xi Jinping announced that China would integrate big data into the multi-billion dollar BRI enterprise to create the "digital silk road of the 21st century."[121] China has also begun to install fiber optic networks across the globe, setting the stage to assert its presence in the ICT sector and facilitate the export of digital authoritarianism.[122]

When examining China's digital efforts abroad, a subtle yet important distinction between China's fundamentally economic activities and its more subversive and damaging endeavors that aid in the expansion of digital authoritarianism must be made. While China's attempts to gain a larger market in the digital domain and to outcompete the United States in certain technological spaces represent a significant concern for U.S. economic interests, those efforts within a free international market do not necessarily represent a national security concern. What does raise critical national security concerns is when China's digital efforts erode democratic values and enable the rise of digital authoritarianism around the world. At best, China is selling digital technology that has remarkable capacity for surveillance and control to authoritarian or authoritarian-leaning countries with no second thought for the consequences. At worst, China is pairing its economic investment with aggressive outreach and training on Internet governance and domestic regulations to further inculcate authoritarian values and methods of social control.

---

[119] Adrian Shahbaz, *Freedom of the Net 2018: The Rise of Digital Authoritarianism*, Freedom House (Oct. 31, 2018), https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism.

[120] Andrew Chatzky & James McBride, "China's Massive Belt and Road Initiative," *Council on Foreign Relations*, last updated Jan. 28, 2020, https://www.cfr.org/backgrounder/chinas-massive-belt-and-road-initiative; Adrian Shahbaz, *Freedom of the Net 2018: The Rise of Digital Authoritarianism*, Freedom House (Oct. 31, 2018), https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism.

[121] Xi Jinping, CCP General Secretary, Remarks at "Work Together to Build the Silk Road Economic Belt and the 21st Century Maritime Silk Road," Beijing, May 14, 2017; Andrew Chatzky & James McBride, "China's Massive Belt and Road Initiative," *Council on Foreign Relations*, last updated Jan. 28, 2020, https://www.cfr.org/backgrounder/chinas-massive-belt-and-road-initiative.

[122] Adrian Shahbaz, *Freedom of the Net 2018: The Rise of Digital Authoritarianism*, Freedom House (Oct. 31, 2018), https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism; Susan Crawford, "China Will Likely Corner the 5G Market—and the US Has No Plan," *Wired*, Feb. 20, 2019.

Exporting Technologies and Expanding Digital Authoritarianism

The Digital Silk Road announcement only formalized efforts already underway by China to expand into foreign markets. For example, in 2015, China's third-largest telecom company, China Telecom Group (CTG), announced the creation of its Africa and Middle East headquarters, having already expanded its network capabilities in the UAE, South Africa, Kenya, Egypt, and Nigeria.[123] It planned to continue growing its network through deals with local companies such as the Wananchi Group, East Africa's leading telecommunications operator.[124]

The CTG announcement marks just one of the steps China and Chinese businesses have taken to extend into the developing world, efforts met with increasing success. Not only has China been willing to go into smaller, under-served markets, Chinese companies have been able to offer more cost-effective equipment than Western companies, as well as financial support that comes directly from the Chinese government.[125] According to Mark Natkin, founder and managing director of the Beijing-based consultancy Marbridge, Chinese telecom vendors "identified opportunities in developing nations" where they could "leverage their price advantage to develop relationships that vendors from rich countries [couldn't] be bothered with."[126] He goes on to describe China's approach as a long-term strategy based on building the core network and banking on the likelihood that doing so gives its companies a foothold to win follow-on contracts for upgrades and expansions.[127]

Huawei, the subject of many headlines during the past few years, is a prime example. In 1996, the Chinese government gave Huawei the status of "national champion" and ensured it would have easy access to financing and high levels of government subsidies—$222 million in government grants in 2018.[128] Government support has enabled Huawei to offer prices for its network equipment that are below other companies' prices, allowing Huawei to quickly gain market advantage. In the Netherlands, for example, Huawei undercut its competitor, the Swedish firm Ericsson, by underbidding for a contract to provide network equipment for the Dutch national 5G network by 60 percent.[129] Two industry officials who spoke to *The Washington Post* on the condition of anonymity held that Huawei's price was so low that, absent the subsidies the company had been provided,

---

[123] Rudradeep Biswas, "Global: China Telecom Global Expands Footprint in Africa and Middle East," *Telecom Talk*, June 9, 2015, https://telecomtalk.info/global-china-telecom-global-expands-in-africa-and-middle-east/137520/.
[124] *Id.*; "CTG Signs Deal with Wananchi Group for Major Fiber Infrastructure Construction Project," *China Telecom Group*, Mar. 18, 2015, https://www.chinatelecomglobal.com/data/file/2016/20160509171658535.pdf.
[125] Executive Research Associates, *China in Africa: A Strategic Overview,* at 51 (Oct. 2009), https://www.ide.go.jp/library/English/Data/Africa_file/Manualreport/pdf/china_all.pdf
[126] Marbridge Consulting, "Management," https://www.marbridgeconsulting.com/management.html (last visited June 1, 2020); Executive Research Associates, *China in Africa: A Strategic Overview*, at 50 (Oct. 2009).
[127] Executive Research Associates, *China in Africa: A Strategic Overview,* at 50 (Oct. 2009).
[128] Lindsay Maizland & Andrew Chatzky, "Huawei: China's Controversial Tech Giant," *Council on Foreign Relations*, June 12, 2019; Ellen Nakashima, "U.S. pushes hard for a ban on Huawei in Europe, but the firm's 5G prices are nearly irresistible," *The Washington Post*, May 29, 2019; Jeffrey Melnik, "China's 'National Champions' Alibaba, Tencent, and Huawei," *Education About Asia*, Vol. 24, Fall 2019, https://www.asianstudies.org/wp-content/uploads/chinas-national-champions-alibaba-tencent-and-huawei.pdf.
[129] Lindsay Maizland & Andrew Chatzky, "Huawei: China's Controversial Tech Giant," *Council on Foreign Relations*, June 12, 2019; Ellen Nakashima, "U.S. pushes hard for a ban on Huawei in Europe, but the firm's 5G prices are nearly irresistible," *The Washington Post*, May 29, 2019.

Huawei would have been unable to even produce the necessary network parts.[130] Some countries also receive low-interest loans from Chinese state-owned banks to use Huawei equipment.[131]

The result has been near-complete dominance in some regions. For example, in Africa Huawei has built about 70 percent of the 4G networks, and in cases such as Zambia, it is developing the country's entire telecommunications infrastructure.[132] More broadly, Chinese technology now serves as the "backbone of network infrastructure" in several African countries, and Chinese firms like Huawei, ZTE, and China Telecom are the major players in erecting the infrastructure needed for next generation technologies across the African continent.[133] In Kenya alone, Huawei has built more than 3,500 mobile base stations (the antennas that receive and transmit radio frequencies which make mobile communications possible) and installed 4,000 kilometers of fiber optic cable.[134]

Today, Huawei operates in more than 170 countries and is the second-largest smartphone seller in the world, just behind Samsung, but ahead of Apple.[135] Robert Atkinson, President of the Information Technology and Innovation Foundation (ITIF), a U.S. think tank, states that Huawei's research and development investments surpass any other company worldwide.[136] Beyond consumer electronics, Huawei offers telecommunications equipment and cloud services.[137] Furthermore, Huawei owns more patents for 5G infrastructure than any of its competitors.[138]

Huawei's investments in research and development have positioned it to build the next-generation 5G infrastructure in Africa, Asia, and Latin America. Alarmingly, even governments close to the

---

[130] Ellen Nakashima, "U.S. pushes hard for a ban on Huawei in Europe, but the firm's 5G prices are nearly irresistible," *The Washington Post*, May 29, 2019.
[131] Lindsay Maizland & Andrew Chatzky, "Huawei: China's Controversial Tech Giant," *Council on Foreign Relations*, June 12, 2019.
[132] Amy Mackinnon, "For Africa, Chinese-Built Internet Is Better Than No Internet at All," *Foreign Policy*, Mar. 19, 2019; Wesley Rahn, "Will China's 5G 'Digital Silk Road' Lead to an Authoritarian Future for the Internet?," *DW*, Apr. 26, 2019.
[133] Chiponda Chimbelu, "Investing in Africa's tech infrastructure. Has China won already?," *DW*, May 3, 2019.
[134] Huawei, *Huawei Kenya Sustainability Report 2018*, (2018), at 8, https://www.huawei.com/minisite/explore-kenya/pdf/huawei_kenya_csd_report_v2.pdf; "Huawei Kenya launches first Sustainability Report Highlighting Efforts to Expand Broadband Nationwide and Solutions to Drive Kenya's Digital Transformation," Huawei, Sept. 7, 2019, https://www.huawei.com/ke/press-events/news/ke/2019/huawei-kenya-launches-first-sustainability-report; Ericsson, "Base stations and networks," https://www.ericsson.com/en/about-us/sustainability-and-corporate-responsibility/responsible-business/radio-waves-and-health/base-stations-and-networks (last visited June 30, 2020). As a note, there are different numbers provided regarding the number of mobile base stations built by Huawei from these two citations. The 2018 report states that the number of stations built is 3,500, while the press release gives the number 3,5000. This report assumes that the number 3,5000 is a typographical error and uses the number of 3,500.
[135] Huawei, "About Huawei," https://www.huawei.com/us/about-huawei (last visited June 1, 2020); Jusy Hong, "Global smartphone shipments fall for seventh consecutive quarter in Q2, even with limited impact from US Huawei ban," *Informa*, Aug. 5, 2019, https://technology.informa.com/616273/global-smartphone-shipments-fall-for-seventh-consecutive-quarter-in-q2-even-with-limited-impact-from-us-huawei-ban; Counterpoint, "Global Smartphone Market Share: By Quarter," https://www.counterpointresearch.com/global-smartphone-share/ (last visited June 30, 2020).
[136] Wesley Rahn, "Will China's 5G 'Digital Silk Road' Lead to an Authoritarian Future for the Internet?," *DW*, Apr. 26, 2019; Information Technology & Innovation Foundation, "Robert D. Atkinson," https://itif.org/person/robert-d-atkinson (last visited June 1, 2020).
[137] Lindsay Maizland & Andrew Chatzky, "Huawei: China's Controversial Tech Giant," *Council on Foreign Relations*, June 12, 2019; Huawei, "About Huawei Cloud," https://www.huaweicloud.com/en-us/about/about_us.html (last visited June 30, 2020).
[138] Lindsay Maizland & Andrew Chatzky, "Huawei: China's Controversial Tech Giant," *Council on Foreign Relations*, June 12, 2019; *Who is leading the 5G patent race*, IPlytics, at 4 and 5 (Nov. 2019), https://www.iplytics.com/wp-content/uploads/2019/01/Who-Leads-the-5G-Patent-Race_2019.pdf.

United States are weighing whether to integrate Huawei technologies into their infrastructure despite security concerns. For example, the ruling party of Germany in early 2020 backed a position paper that pushed for more stringent regulation of foreign technologies in its 5G networks but did not ban the use of Huawei components.[139] Furthermore, Germany's three primary telecommunications firms, while deciding to remove Huawei from its core networks, will continue to utilize Huawei technologies on peripheral radio access networks.[140] Brazil, another U.S. partner, faces an upcoming decision on whether Huawei should be further involved in Brazil's infrastructure as Brazil prepares to auction spectrum for 5G in late 2020.[141] In July 2019, Brazil's Vice President Hamilton Mourao told reporters that the country would not restrict Huawei on 5G, extending a decade-long relationship.[142] In an example of that relationship, Huawei supports an Internet of Things laboratory in São Paulo state and is looking to build a smartphone assembly plant.[143] While security concerns have been raised by Eduardo Bolsonaro, a lawmaker and son of Brazil's president, it remains to be seen how Brazil manages Huawei's involvement in its domestic 5G moving forward, especially in light of Foreign Minister Ernesto Araujo reportedly arguing for a Huawei 5G ban to President Bolsonaro.[144] Meanwhile, Mexico and Argentina plan to start Latin America's first 5G networks in 2020 and are considering allowing Huawei participation.[145]

Huawei's 5G push continues to see success in other countries, especially ones in China's Belt and Road Initiative, highlighting the company's ability to dominate the 5G space by providing networks for prices estimated to be 30 percent less than its competitors.[146] For example:

- Malaysia is not barring Huawei from spectrum bids relating to its 5G rollout, saying that security decisions will be made by its "own safety standards";[147]
- In Thailand, Huawei offered to build a tech training center in Bangkok as a means of enticing Thailand to allow Huawei to build its 5G network;[148]
- In Italy, Huawei offered to provide cloud computing services that would link Italian hospitals both with each other and with hospitals in Wuhan in response to the COVID-19 pandemic;[149]

---

[139] Andreas Rinke, "Merkel's conservatives stop short of Huawei 5G ban in Germany," *Reuters*, Feb. 11, 2020.
[140] Douglas Busvine & Thomas Seythal, "Telefonica Deutschland picks Ericsson for 5G core network," *Reuters*, June 2, 2020.
[141] Anthony Boadle, "Huawei role in Brazil 5G up to national security chief: regulator," *Reuters*, Feb. 18, 2020.
[142] "Defying US, Brazil Allows Huawei to Move Forward with 5G Network," *Al Jazeera*, July 15, 2019.
[143] Oliver Stuenkel, "Huawei Heads South: The Battle over 5G Comes to Latin America," *Foreign Affairs*, May 10, 2019.
[144] Anthony Boadle, "Huawei role in Brazil 5G up to national security chief: regulator," *Reuters*, Feb. 18, 2020; Eduardo Baptista, "China-Brazil trade on track, but Huawei tension may be threat to relations," *South China Morning Post*, June 21, 2020, https://www.scmp.com/news/china/article/3089903/china-brazil-trade-track-huawei-tension-may-be-threat-relations.
[145] Oliver Stuenkel, "Huawei Heads South: The Battle over 5G Comes to Latin America," *Foreign Affairs*, May 10, 2019; Andres Schipani et al., "Latin America resists US pressure to exclude Huawei," *Financial Times*, June 9, 2019.
[146] Lindsay Maizland & Andrew Chatzky, "Huawei: China's Controversial Tech Giant," *Council on Foreign Relations*, June 12, 2019.
[147] Joseph Sipalan & Krishna N. Das, "Malaysia to choose 5G partners based on own security standards," *Reuters*, Feb. 17, 2020.
[148] Apornrath Phoonphongphiphat, "Huawei sweetens 5G offer in Thailand with tech training center," *Nikkei Asian Review*, November 18, 2019, https://asia.nikkei.com/Spotlight/5G-networks/Huawei-sweetens-5G-offer-in-Thailand-with-tech-training-center;
Takashi Kawakami, "China closes in on 70% of world's 5G subscribers," *Nikkei Asian Review*, May 12, 2020, https://asia.nikkei.com/Spotlight/5G-networks/China-closes-in-on-70-of-world-s-5G-subscribers.
[149] Theresa Fallon, "China, Italy, and Coronavirus: Geopolitics and Propaganda," *The Diplomat*, Mar. 20, 2020.

- Unnamed sources reported in March 2020 that as part of its 5G rollout, France's cybersecurity agency, ANSSI, will allow Huawei equipment to be used for non-core elements of France's network;[150]
- Russia is building out its 5G network with Huawei's help;[151]
- *The Washington Post* reported that Huawei is building out North Korea's wireless network.[152] Huawei stated that it does not have a business presence in North Korea, but did not dispute the reporting done by *The Washington Post*;[153]
- Even some small U.S. rural telecom companies have used Huawei equipment.[154]

By building out so much of the digital infrastructure in the developing world, China could end up dominating a large portion of the global communications market, positioning it to potentially pressure other governments or conduct espionage.[155] Indeed, multiple governments that purchase or rely on Chinese technologies also enact tough restraints on free speech or engage in illiberal activities, such as spying on political opponents, and there have been suspicious data transfers from Chinese-built IT systems.[156] For example, in 2017, technicians working at the African Union headquarters in Addis Ababa, Ethiopia, discovered that servers in the building, built by a Chinese company with Chinese funding, had for years been transmitting massive quantities of data to China, making even the most sensitive material vulnerable to Chinese exploitation.[157] Despite these incidents and diplomatic warnings, however, many countries—both developing and developed—calculate that access to low-cost, good-quality data networks and hardware outweighs the potential risks.

As noted above, China's export and infrastructure efforts around the globe represent an economic concern for the United States. However, China's export of digital technology in and of itself is not the key issue, as it is only the groundwork upon which digital authoritarianism can flourish. What really advances this censorship and surveillance system is China providing countries with social control systems that run on exported digital technologies, including relevant training and expertise.

---

[150] Mathieu Rosemain & Gwénaëlle Barzic, "Exclusive: France to allow some Huawei gear in its 5G network – sources," *Reuters*, Mar. 12, 2020.
[151] Zak Doffman, "Huawei Just Launched 5G In Russia With Putin's Support: 'Hello Splinternet'," *Forbes*, Sept. 1, 2019.
[152] Ellen Nakashima et al., "Leaked documents reveal Huawei's secret operations to build North Korea's wireless network," *The Washington Post*, July 22, 2019; Emily Stewart, "A New Reason to Worry About Huawei: It's Been Building North Korea's Wireless Networks," *Vox*, July 22, 2019, https://www.vox.com/recode/2019/7/22/20704196/huawei-north-korea-washington-post-sanctions-panda.
[153] Ellen Nakashima et al., "Leaked documents reveal Huawei's secret operations to build North Korea's wireless network," *The Washington Post*, July 22, 2019.
[154] Jeanne Whalen, "Huawei helped bring Internet to small-town America. Now its equipment has to go," *The Washington Post*, Oct. 10, 2019.
[155] See, e.g., Zak Doffman, "CIA Claims It Has Proof Huawei Has Been Funded By China's Military and Intelligence," *Forbes*, Apr. 20, 2019; Isobel Asher Hamilton, "Researchers Studied 25,000 Leaked Huawei Resumes and Found Troubling Links to the Government and Spies," *Business Insider*, July 8, 2019, https://www.businessinsider.com/huawei-study-finds-connections-between-staff-and-chinese-intelligence-2019-7.
[156] Steven Feldstein, "When it Comes to Digital Authoritarianism, China is a Challenge – But Not the Only Challenge," *War on the Rocks*, Feb. 12, 2020, https://warontherocks.com/2020/02/when-it-comes-to-digital-authoritarianism-china-is-a-challenge-but-not-the-only-challenge/; Josh Chin, "The Internet, Divided Between the U.S. and China, Has Become a Battleground," *The Wall Street Journal*, Feb. 9, 2019.
[157] Joan Tilouine & Ghalia Kadiri, "A Addis-Abeba, le siège de l'Union africaine espionné par Pékin," *Le Monde*, Jan. 26, 2018, https://www.lemonde.fr/afrique/article/2018/01/26/a-addis-abeba-le-siege-de-l-union-africaine-espionne-par-les-chinois_5247521_3212.html; Mailyn Fidler, "African Union Bugged by China: Cyber Espionage as Evidence of Strategic Shifts," *Council on Foreign Relations*, Mar. 7, 2018.

In its report, *Freedom on the Net 2018*, Freedom House highlights how, during 2018, the Chinese government hosted media officials from dozens of countries for seminars on its system of censorship and surveillance.[158] Outside experts have little visibility into the details of these trainings, but governments who participate frequently return home to pass cybersecurity laws very similar to those in China.[159] Furthermore, Chinese companies have supplied many governments—at least some of which have poor human rights records or a tendency towards autocracy—with advanced facial recognition technology and data analytics tools that can be easily exploited by repressive governments and intelligence services.[160] For example:

- The Chinese startup CloudWalk is partnering with the Zimbabwean government on a mass facial recognition program in Zimbabwe;[161]
- Huawei is advising Kenya on its information and communication technology (ICT) Master Plan and Vision 2030;[162]
- In Mauritius, Huawei is installing 4,000 cameras;[163]
- Zambia is spending $1 billion on Chinese-made telecommunications, broadcasting, and surveillance technology;[164]
- Chinese start-up Yitu bid for a contract for facial recognition cameras in Singapore and opened its first international office in Singapore in January 2019.[165]

These examples highlight a few Chinese efforts to expand digital authoritarianism. To more fully show how China's approach of economic advancement and authoritarian outreach is extending digital authoritarianism to new countries, this report delves into four case studies that underscore China's efforts to not only provide technologies to other nations, but also to work with these countries to perfect methods of social control that imitate China's own patterns of digital authoritarianism.

Case Study: Venezuela

The regime of disputed Venezuelan president Nicolas Maduro takes full advantage of Chinese hardware and services in its effort to control Venezuelan citizens. Venezuela has Internet and

---

[158] Adrian Shahbaz, *Freedom on the Net 2018: The Rise of Digital Authoritarianism*, Freedom House (Oct. 31, 2018), https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism.

[159] *Id.*. Vietnam, Uganda, and Tanzania all introduced cybersecurity laws resembling China's following such seminars. *Id. See Also* Abdi Latif Dahir, "China is Exporting its Digital Surveillance Methods to African Countries," *Quartz Africa*, Nov. 1, 2018; Josh Chin, "The Internet, Divided Between the U.S. and China, Has Become a Battleground," *The Wall Street* Journal, Feb. 9, 2019.

[160] Daniel Benaim and Hollie Russon Gilman, "China's Aggressive Surveillance Technology Will Spread Beyond Its Borders," *Slate*, Aug. 9, 2018.

[161] Shan Jie, "China exports facial ID technology to Zimbabwe," *Global Times*, Apr. 12, 2018, http://www.globaltimes.cn/content/1097747.shtml; Abdi Latif Dahir, "China is Exporting its Digital Surveillance Methods to African Countries," *Quartz Africa*, Nov. 1, 2018.

[162] Abdi Latif Dahir, "China is Exporting its Digital Surveillance Methods to African Countries," *Quartz Africa*, Nov. 1, 2018; Huawei, "Kenya," https://www.huawei.com/us/about-huawei/sustainability/win-win-development/social-contribution/seeds-for-the-future/kenya (last visited June 7, 2020).

[163] Sheridan Prasso, "China's Digital Silk Road is Looking More Like an Iron Curtain, *Bloomberg,* Jan. 10, 2019.

[164] *Id.*

[165] Anna Gross et al., "Chinese tech groups shaping UN facial recognition standards," *Financial Times*, Dec. 1, 2019; Amanda Lentino, "This Chinese facial recognition start-up can identify a person in seconds," *CNBC*, May 16, 2019.

mobile networking equipment, intelligent monitoring systems, and facial recognition technology developed and installed by Chinese companies, and regime officials have traveled to China to participate in seminars on information management.[166] The regime uses these technologies to censor and control its critics by blocking social media platforms and political content, using pro-regime commentators to manipulate online discussions, stifling content critical of Maduro, increasing surveillance of citizens, tracking and detaining government critics, and accessing the data of human rights organizations.[167]

ZTE helped the regime create Venezuela's *Carnet de la Patria* (Fatherland Card). Critics have labeled the card as a new option for the Maduro regime to exert increased social control over its population (such as determining who receives subsidized food or health services), especially against those the regime considers political opponents.[168] The initial idea began more than a decade ago as a standardized ID for voting or opening a bank account.[169] However, as Venezuela's economic and political crisis deepened, the regime used it to track *Comités Locales de Abastecimiento y Producción* (Local Committees for Supply and Production, or CLAP) boxes, the subsidized food packages the government began distributing in 2016.[170] ZTE in 2017 also received an undisclosed portion of $70 million to build out a centralized database and mobile payment system for the card in an effort to bolster "national security."[171] By late 2018, a team of ZTE employees was embedded in a special unit of Venezuela's state telecommunications company that oversees the management of the database.[172] According to employees of the entity that manages the card system, the database stores birthdays, family information, employment and income, property owned, medical history, state benefits received, presence on social media, political party membership, and voting records.[173] To encourage people to sign up for the card, the Maduro regime has granted "cash prizes to cardholders for performing civic duties, like rallying voters."[174] However, the regime also made it mandatory for anyone wanting to receive public benefits such as medicine, subsidized fuel, and pensions.[175] Once the card became the way to sign up for much-needed services, its adoption was generally assured, and the Maduro regime claims that over half of the population retains a Fatherland Card.[176]

---

[166] Angus Berwick, "How ZTE Helps Venezuela Create China-Style Social Control," *Reuters Investigates*, Nov. 14, 2018; Paul Mozur et al., "Made in China, Exported to the World: The Surveillance State," *The New York Times*, Apr. 24, 2019.
[167] "Venezuela / Protests: UN and IACHR Rapporteurs condemn censorship, arrests and attacks on journalists," *UN Human Rights – Office of the High Commissioner*, Apr. 26, 2017, https://www.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=21535&LangID=E; Angus Berwick, "How ZTE Helps Venezuela Create China-Style Social Control," *Reuters Investigates*, Nov. 14, 2018; "Freedom on the Net 2019: Venezuela," *Freedom House*, https://freedomhouse.org/country/venezuela/freedom-net/2019 (last visited July 10, 2020); Moises Rendon & Arianna Kohan, "The Internet: Venezuela's Lifeline," *Center for Strategic and International Studies*, Dec. 4, 2019.
[168] Laura Vidal, "Venezuelans fear 'Fatherland Card' may be a new form of social control," *The World*, Dec. 28, 2018, https://www.pri.org/stories/2018-12-28/venezuelans-fear-fatherland-card-may-be-new-form-social-control.
[169] Angus Berwick, "How ZTE Helps Venezuela Create China-Style Social Control," *Reuters Investigates*, Nov. 14, 2018.
[170] Jim Wyss & Cody Weddle, "Venezuela's Maduro aims to turn empty stomachs into full ballot boxes," *Miami Herald*, May 16, 2018. *See also* Press Release, U.S. Department of Treasury, "Treasury Disrupts Corruption Network Stealing From Venezuela's Food Distribution Program, CLAP," July 25, 2019.
[171] Angus Berwick, "How ZTE Helps Venezuela Create China-Style Social Control," *Reuters Investigates*, Nov. 14, 2018.
[172] *Id.*
[173] *Id.*
[174] *Id.*
[175] *Id.*
[176] *Id.*; Jim Wyss & Cody Weddle, "Venezuela's Maduro aims to turn empty stomachs into full ballot boxes," *Miami Herald*, May 16, 2018.

Using information gathered through enrollment and card transactions, the regime is creating and growing a database that could be a powerful tool for identifying, harassing, and silencing Maudro's critics. Current and former employees of Cantv, Venezuela's state telephone and Internet provider, told *Reuters* that the card still only records if a person voted—not how they voted—but there is evidence that government agencies are tracking whether government employees are voting.[177] ZTE is also supporting the Maduro regime by taking on projects that government-owned enterprises can no longer manage. As of 2015, ZTE was helping build six emergency response centers monitoring Venezuela's major cities, and since 2016 it has been working to centralize the government's video surveillance.[178]

Case Study: Central Asia

In April 2019, the Uzbek government signed a $1 billion deal with Huawei to expand surveillance operations in the country.[179] At the time, the capital city of Tashkent had 883 cameras that authorities used to record and analyze movements while automatically reporting road violations such as speeding.[180] Under the new agreement, Huawei will upgrade the cameras to "digitally manage political affairs."[181] Similarly, Huawei aided the implementation of Tajikistan's "safe city" project in Dushanbe in 2013, providing $22 million (primarily a $20.91 million loan) for the installation of cameras along roads and overseeing monuments and parks.[182] China also owns TK mobile, one of the five telecommunications providers in Tajikistan, and Huawei is the main technology supplier for Kyrgyzstan's top telecommunication providers.[183] Although the Kyrgyz government withdrew from Huawei's $60 million "safe cities" project in March 2018, it later chose a Russian company, Vega, to implement the first phase of a similar traffic monitoring system in November 2018.[184]

Case Study: Ecuador

The Ecuador example illustrates how, even if democratic institutions prevail, vestiges of China's influence persist. Former Ecuadorian President Rafael Correa, the autocratic leftist and ally of former Venezuelan President Hugo Chavez, left office in 2017 but the surveillance system he installed remains in use.[185] Correa learned of China's surveillance technology after Ecuadorian

---

[177] Angus Berwick, "How ZTE Helps Venezuela Create China-Style Social Control," *Reuters Investigates*, Nov. 14, 2018.
[178] *Id.*
[179] "Huawei and CITIC Guoan invest over US$1 billion to develop Uzbekistan's digital infrastructure," *Xiangshi Xinwen Wang* (*Detailed News)* via *Silu Xin Guancha (Silk Road New Observer)*, Apr. 26, 2019, http://web.siluxgc.com/UZ/20190426/16656.html (translated from Chinese); Yau Tsz Yan, "Smart Cities or Surveillance? Huawei in Central Asia," *The Diplomat*, Aug. 7, 2019.
[180] Yau Tsz Yan, "Smart Cities or Surveillance? Huawei in Central Asia," *The Diplomat*, Aug. 7, 2019.
[181] *Id.*
[182] *Id.*; Liu Ruowei, "Millions of Roads, Safety First: The Central Asian 'Safe City' project is here!," *Silu Xin Guangcha (Silk Road New Observer)* on WeChat, Feb. 13, 2019, https://mp.weixin.qq.com/s/z3l_UHX40W8OIJi61HaomA (translated from Chinese).
[183] Yau Tsz Yan, "Smart Cities or Surveillance? Huawei in Central Asia," *The Diplomat*, Aug. 7, 2019; "Announcement on providing guarantee for holding subsidiaries," *ZTE Corporation*, May 11, 2019, https://www.zte.com.cn/mi_imgs/global/investor_relations/349268/P020120917408589110191.pdf.
[184] Yau Tsz Yan, "Smart Cities or Surveillance? Huawei in Central Asia," *The Diplomat*, Aug. 7, 2019; "The Kyrgyz government suddenly announced the termination of the "smart city" project, China's Huawei has not yet responded," *Kabar*, Mar. 18, 2015, http://cn.kabar.kg/news/2-8/ (translated from Chinese); "Vega successfully completes first round of Safe City program in Bishkek," *Vega*, May 20, 2019, https://www.vega.su/press-room/?ELEMENT_ID=2216 (translated from Russian).
[185] "Ecuador 'rejects unlimited election terms', blocking Correa return," *BBC*, Feb. 5, 2018.

officials visiting Beijing for the 2008 Olympics received a tour of Beijing's surveillance system.[186] Three years later, the Ecuadorian government began installing a system of high-powered cameras throughout the country for the stated purpose of reducing crime.[187] This system sends images to 16 monitoring centers that employ more than 3,000 people.[188] China guaranteed state funding and loans for the project, and in return, Ecuador committed to exporting "large portions of its oil reserves" to China, underscoring another key point: China's utilization of predatory lending and technological knowledge to receive other benefits.[189]

Two Chinese companies, Huawei and China National Electronics Import & Export Corporation (CEIEC), primarily built Ecuador's surveillance system.[190] In addition to recording events, the monitoring system offers Ecuadorian authorities the ability to track phones and, according to the *New York Times*, may be equipped with facial-recognition capabilities in the future.[191] As part of the process of fully integrating these technologies into Ecuador's infrastructure, China engaged in a training operation in which Ecuadorian officials visited China and Chinese engineers educated Ecuadorian engineers on how to manage the system.[192] The Ecuador project created a toehold in the region: Ecuador's decision to install the equipment prompted the Venezuelan and Bolivian governments to follow suit, and soon after, Venezuela installed a larger version that aimed to include 30,000 cameras.[193]

Although Correa's successor, President Lenin Moreno, has worked to reverse many of Correa's autocratic policies, the surveillance system is still operational and holds the potential for abuse. When *New York Times* reporters had the opportunity to see in person the 800-camera operation in Quito, there were only 30 police officers available to check camera footage, and anecdotal reports suggest crimes continue to take place in plain view of cameras.[194] Moreover, the recordings are also available to Ecuador's domestic intelligence agency, the National Intelligence Secretariat (SENAIN), which has a history of harassing and tracking political opponents.[195] Indeed, given the small number of police available to monitor crime-prone locations, the system is probably better suited to spying on individuals than fending off criminality.

Case Study: Zimbabwe

China is also leveraging the deployment of surveillance technology overseas to improve its products' functionality. Studies have shown that facial recognition systems developed in Western nations tend

---

[186] Paul Mozur et al., "Made in China, Exported to the World: The Surveillance State," *The New York Times*, Apr. 24, 2019.
[187] *Id.*
[188] *Id.*
[189] *Id.*; Clifford Krauss & Keith Bradsher, "China's Global Ambitions, Cash and Strings Attached," *The New York Times*, July 24, 2015.
[190] Paul Mozur et al., "Made in China, Exported to the World: The Surveillance State," *The New York Times*, Apr. 24, 2019.
[191] *Id.*
[192] *Id.*
[193] *Id.*; "Venezuela will replicate the Ecuadorian model of the Integrated Security System Ecu-911," *National Service for Risk and Emergency Management of Ecuador*, Dec. 25, 2013, https://www.gestionderiesgos.gob.ec/venezuela-replicara-modelo-ecuatoriano-del-sistema-integrado-de-seguridad-ecu-911/.
[194] Paul Mozur et al., "Made in China, Exported to the World: The Surveillance State," *The New York Times*, Apr. 24, 2019.
[195] *Id.*

to perform better on Caucasian faces and those developed in East Asian nations tend to perform better on their respective populations.[196] While Western technology companies are grappling with how to teach machines about race, their Chinese counterparts are using their customer base in Africa to help develop advanced capabilities that differentiate by race.[197] For example, in March 2018, the Zimbabwean government agreed to a partnership to develop facial recognition programs in the country with CloudWalk Technology, a startup located in Guangzhou.[198] Additionally, Zimbabwe entered into a Memorandum of Understanding with Hikvision in which the Chinese company would donate facial recognition cameras and software for use at border posts, airports, and state entry points in Zimbabwe.[199] Partnerships such as these provide Chinese companies with the opportunity to develop and refine their databases with different ethnicities and demographics, in Zimbabwe's case a majority-Black population, while enticing the country with technological modernization.[200] A key consequence of such partnerships, according to *Quartz* reporter Lynsey Chutel, is Chinese companies "getting ahead of US and European developers" on facial recognition.[201]

A Global Challenge

The situations described above are key examples of how China is using economic and, more importantly, geopolitical and outreach tools to stimulate the growth of digital authoritarianism in new markets and nations. Although most China tech-watchers agree that the use of Chinese surveillance and censorship systems around the world is growing, they differ on how many are in use, and, given the proliferation of Chinese-built telecommunications equipment, how widely their use may ultimately reach. According to Steven Feldstein, former Deputy Assistant Secretary of State at the Bureau for Democracy, Human Rights, and Labor, "Huawei alone is responsible for providing AI [artificial intelligence] surveillance technology to at least fifty countries worldwide."[202] When Huawei's efforts are combined with Hikvision, Dahua, and ZTE's efforts, Chinese companies supply AI surveillance technology in sixty-three countries, thirty-six of which are part of BRI.[203] Experts are still trying to assess the long-term consequences of China's technological expansion; Feldstein also notes that China is exporting AI-equipped surveillance technology to governments ranging from closed authoritarian systems to flawed democracies.[204] In an article on the proliferation of Chinese-made surveillance systems, *Foreign Policy* cites a Huawei study, which has been removed

---

[196] P. Jonathon Phillips et al., *An Other-Race Effect for Face Recognition Algorithms*, Association for Computing Machinery (Feb. 2011), https://dl.acm.org/doi/10.1145/1870076.1870082; Steve Lohr, "Facial Recognition is Accurate, if You're a White Guy," *The New York Times*, Feb. 9, 2018; Clare Garvie & Jonathan Frankle, "Facial-Recognition Software Might Have a Racial Bias Problem," *The Atlantic*, Apr. 7, 2016.

[197] Lynsey Chutel, "China is Exporting Facial Recognition Software to Africa, Expanding its Vast Database," *Quartz Africa*, May 25, 2018.

[198] *Id.*; Zhang Hongpei, "Chinese Facial ID Tech to Land in Africa," *Global Times*, May 17, 2018, http://www.globaltimes.cn/content/1102797.shtml; Shan Jie, "China exports facial ID technology to Zimbabwe," *Global Times*, April 12, 2018, http://www.globaltimes.cn/content/1097747.shtml.

[199] Farai Mudzingwa, "Government Acknowledges Facial Recognition System In The Works," *TechZim*, June 13, 2018, https://www.techzim.co.zw/2018/06/government-acknowledges-facial-recognition-system-in-the-works/.

[200] Lynsey Chutel, "China is Exporting Facial Recognition Software to Africa, Expanding its Vast Database," *Quartz Africa*, May 25, 2018.

[201] *Id.*

[202] Steven Feldstein, "The Global Expansion of AI Surveillance," *Carnegie Endowment for International Peace*, Sept. 17, 2019.

[203] *Id.*.

[204] *Id.;* Steven Feldstein, "China is Exporting AI Surveillance Technology to Countries Around the World," *Newsweek*, Apr. 23, 2019.

from the company's website, in which "the company boasted that it had already deployed its 'Safe City' system in 230 cities around the world, for more than 90 national or regional governments."[205]

Due to China's efforts at proliferating the technologies and methodologies of digital authoritarianism, the United States finds itself in an intensifying battle over the global ICT sector. China's export of ICT infrastructure, its ability to deliver lower-priced, reliable access to telecommunications network technology, and its competitive edge in 5G combine to mount a strong challenge to the U.S. to become the biggest provider of 5G services to the world. Not only do these efforts provide China with a competitive edge both commercially and, in a potential conflict, militarily, they also offer even greater leverage to push client countries to adopt the Chinese approach to the Internet and the regulation of speech. Consequently, the United States must proactively defend a free, democratic model for the digital domain and Internet governance and push back against China's malign activities abroad.

However, it is not enough for the United States to take a purely defensive posture against China's digital authoritarianism. **It is critical that the United States government stimulate technological innovation in the United States by increasing government research and development funding, adopting a more extensive industrial policy, developing and attracting superior talent to the United States' technology sector, strengthening bilateral and multilateral technology initiatives with like-minded allies and partners, and ensuring a competitive advantage for domestic companies in overseas markets**. By doing so, the United States and its allies can open up more opportunities to create and deploy emerging technologies that can outcompete Chinese products and services and thereby undercut its ability to export digital authoritarianism. If the United States does not develop and implement an all-encompassing strategy for combatting China and its cyber efforts, the United States will cede the global cyber domain to our Pacific adversary and open up a future in which digital authoritarianism becomes the global norm, leaving the United States and its allies vulnerable and placing countless more individuals under the thumb of digital authoritarianism.

[205] Bojan Stojkovski, "Big Brother Comes to Belgrade," *Foreign Policy*, June 18, 2019.

Chapter 3: Institutionalizing Digital Authoritarianism – China at International Fora

In addition to using heavily-subsidized technology to purchase political influence in countries around the world, China continues to use diplomacy and various international domains to further its authoritarian goals. Its objective: to set the rules and norms around the governance of digital technologies. From the United Nations (UN) to the World Trade Organization (WTO), China has used its political and economic muscle to shape the international standards surrounding the digital domain in favor of a more authoritarian view of the world.

Since General Secretary Xi came into power in 2012, the cyber realm has become an increasingly important strategic domain.[207] Adam Segal of the Council on Foreign Relations wrote that, since then, the CCP's goals have been threefold: "limit the threat that the Internet and the flow of information may pose to domestic stability and regime legitimacy; shape cyberspace to extend Beijing's political, military, and economic influence; and counter US advantages in cyberspace while increasing China's room to maneuver."[208]

According to a report prepared for the United States-China Economic and Security Review Commission in 2018, China uses:

> [A] comprehensive techno-nationalist strategy that coordinates Chinese efforts to gain leading roles in international standards organizations while also using state funding to allow Chinese companies to undersell their competitors in developed economies and win infrastructure contracts in developing markets, ensuring that its indigenously-developed technologies and standards become widely adopted with or without international recognition.[209]

Above all else, China is heavily focused on ensuring its digital sovereignty, as indicated by its presence as the second "principle" (following "peace" as the first) in their 2017 International Strategy of Cooperation on

Definition - Digital Sovereignty

At the Opening Ceremony of the International Workshop on Information and Cyber Security in June 2014, Vice Foreign Minister Li Baodang stated that sovereignty in cyberspace, which this report refers to as digital sovereignty, comprises the following factors: "states['] own jurisdiction over the ICT infrastructure and activities within their territories; national governments are entitled to making public policies for the Internet based on their national conditions; no country shall use the Internet to interfere in other countries' internal affairs or undermine other countries' interests."[206]

---

[206] Press Release, Vice Foreign Minister Li Baodong, "Address by Vice Foreign Minister Li Baodong at the Opening Ceremony of the International Workshop on Information and Cyber Security," June 5, 2014, https://www.fmprc.gov.cn/mfa_eng/wjbxw/t1162458.shtml.

[207] *See, e.g.,* James A. Lewis & Simon Hansen, *China's Cyberpower – International and domestic priorities,* Australian Strategic Policy Institute, at 1 (Nov. 2014), https://s3-ap-southeast-2.amazonaws.com/ad-aspi/import/SR74_China_cyberpower.pdf?R7nGofs8ZdT2nhDIb6NqAekikBTLuC9m.

[208] Adam Segal "Chinese Cyber Diplomacy in a New Era of Uncertainty," *Hoover Institution*, June 2017, https://www.hoover.org/sites/default/files/research/docs/segal_chinese_cyber_diplomacy.pdf.

[209]John Chen et al., *China's Internet of Things,* Research Report Prepared on Behalf of the U.S.-China Economic and Security Review Commission, by SOS International (SOSi), at 69 (Oct. 2018).

Cyberspace.[210] In the strategy, the Cyberspace Administration of China (CAC) and the Ministry of Foreign Affairs argues for digital sovereignty and states that "[n]o country should pursue cyber hegemony."[211] It appears, as evidenced by its efforts in a number of different international forums, that China's idea of not pursuing "cyber hegemony" applies to every country other than China.

The United Nations

At the United Nations, China has played a counterproductive role in efforts to build consensus on a free and fair future of cyberspace. China's behavior echoes its consistent undermining of UN efforts that could highlight its own poor human rights record.[212]

In 2011, China—along with Russia, Tajikistan, and Uzbekistan—submitted a draft resolution on an international code of conduct for information security to the 2011 United Nations General Assembly.[213] The resolution, which was later enhanced and resubmitted in 2015 by a slightly larger group of Shanghai Cooperation Organization (SCO) member countries, emphasizes the sovereignty and stability of individual states within the digital space to the extent that it raises significant human rights concerns, detailed below.[214] The resolution explicitly says it aims to "push forward the international debate on international norms on information security, and help forge an early consensus on this issue."[215] In other words, the resolution is China's attempt to make itself the leader on these norms.

Both the 2011 and 2015 versions of the draft resolution commit the signatories to "curbing the dissemination of information that incites terrorism, secessionism or extremism or that undermines other countries' political, economic, and social stability, as well as their spiritual and cultural environment."[216] According to Milton Mueller of the Internet Governance Project at the Georgia Institute of Technology School of Public Policy, this section would:

> [G]ive any state the right to censor or block international communications for almost any reason. Such as…Facebook mobilizations against dictators, dissident blogs, etc.

---

[210] Ministry of Foreign Affairs of the People's Republic of China, "International Strategy of Cooperation on Cyberspace – March 2017," Mar. 1, 2017, https://www.fmprc.gov.cn/mfa_eng/wjb_663304/zzjg_663340/jks_665232/kjlc_665236/qtwt_665250/t1442390.shtml.

[211] *Id.*

[212] *See, e.g.,* Lindsay Maizland, "Is China Undermining Human Rights at the United Nations?" *Council on Foreign Relations*, July 9, 2019.

[213] Letter Dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan, and Uzbekistan to the United Nations Addressed to the Secretary-General (93), *U.N. General Assembly, 66th Session*, Sept. 14, 2011, https://undocs.org/A/66/359.

[214] Letter Dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan, and Uzbekistan to the United Nations Addressed to the Secretary-General (91), *U.N. General Assembly, 69th Session*, Jan. 13, 2015, https://undocs.org/A/69/723; *See, e.g.,* Sarah McKune, "An Analysis of the International Code of Conduct for Information Security," *The Citizen Lab, Munk School of Global Affairs and Public Policy, University of Toronto*, Sept. 28, 2015, https://citizenlab.ca/2015/09/international-code-of-conduct/.

[215] *Id.*

[216] Letter Dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan, and Uzbekistan to the United Nations Addressed to the Secretary-General (93), *U.N. General Assembly, 66th Session*, Sept. 14, 2011, https://undocs.org/A/66/359. *See also* Letter Dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan, and Uzbekistan to the United Nations Addressed to the Secretary-General (91), *U.N. General Assembly, 69th Session*, Jan. 13, 2015, https://undocs.org/A/69/723.

> "Undermining the spiritual and cultural environment" in particular could be used to filter out any views a government didn't like, and could even be used for trade protectionism in cultural industries.[217]

The significant revisions between the 2011 Code of Conduct and the 2015 Code of Conduct involve several references to a report by the 2012 UN Group of Governmental Experts (GGE), *Developments in the Field of Information and Telecommunications in the Context of International Security*.[218] The GGEs, which fall under the United Nations Office for Disarmament Affairs and consist of selected member states, have initiated six separate working groups since 2004 to "examine[] existing and potential threats in the cyber-sphere and possible cooperative measures to address them," with each group's work intended to build upon the last.[219]

The GGEs have been viewed as the best tool to achieve success—albeit incremental—at the UN on democratic digital standards.[220] However, contrary to that view, the report by the GGE established in 2012 was favorably referenced by the China-led SCO's Code of Conduct resolution several times in 2015.[221] According to Sarah McKune, Senior Legal Advisor at the Citizen Lab, SCO states looked favorably on that GGE's report because of the "recognition of sovereignty and territoriality in the digital space."[222] The SCO's newfound appreciation for the 2012-13 GGE in their resolution may have led to the increased disputes in a later GGE—the 2016-2017 GGE—that collapsed discussions and prevented the Group from issuing a consensus report at its conclusion.[223] Following the 2016-17

---

[217] Milton Mueller, "Russia & China propose UN General Assembly Resolution on 'information security,'" *Internet Governance Project – Georgia Tech University*, Sept. 20, 2011, https://www.internetgovernance.org/2011/09/20/russia-china-propose-un-general-assembly-resolution-on-information-security/.

[218] *See* Letter Dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan, and Uzbekistan to the United Nations Addressed to the Secretary-General (93), *U.N. General Assembly, 66th Session*, Sept. 14, 2011, https://undocs.org/A/66/359; Letter Dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan, and Uzbekistan to the United Nations Addressed to the Secretary-General (91), *U.N. General Assembly, 69th Session*, Jan. 13, 2015, https://undocs.org/A/69/723; U.N. General Assembly, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* – Note by the Secretary-General, 68th Session, Agenda item 94 (June. 24, 2013), https://undocs.org/A/68/98.

[219] United Nations, "Developments in the Field of Information and Telecommunications in the Context of International Security – December 2018," https://www.un.org/disarmament/ict-security/ (last visited July 15, 2020). *See also* United Nations Office for Disarmament Affairs (UNODA), "Fact Sheet: Developments In the Field of Information and Telecommunications in the Context of International Security," Jul. 2019, https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/07/Information-Security-Fact-Sheet-July-2019.pdf.

[220] *See, e.g.,* John Sullivan, Deputy Secretary of State, Remarks at the "Second Ministerial Meeting on Advancing Responsible State Behavior in Cyberspace," New York, New York, Sept. 23, 2019.

[221] "Letter Dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan, and Uzbekistan to the United Nations Addressed to the Secretary-General (91)" *U.N. General Assembly, 69th Session*, Jan. 13, 2015, https://undocs.org/A/69/723; *See, e.g.*. Sarah McKune, "An Analysis of the International Code of Conduct for Information Security," *The Citizen Lab, Munk School of Global Affairs and Public Policy, University of Toronto*, Sept. 28, 2015, https://citizenlab.ca/2015/09/international-code-of-conduct/.

[222] Sarah McKune, "An Analysis of the International Code of Conduct for Information Security," *The Citizen Lab, Munk School of Global Affairs and Public Policy, University of Toronto*, Sept. 28, 2015, https://citizenlab.ca/2015/09/international-code-of-conduct/.

[223] Elaine Korzak, "UN GGE on Cybersecurity: The End of an Era?," *The Diplomat,* July 21, 2017.

GGE dissipation, the United States led a resolution to authorize the creation of a new 2019-21 GGE, which continues to meet periodically and is expected to conclude in May 2021.[224]

In addition to the GGEs, China may find another short-term mechanism to push its agenda of digital authoritarianism in the Open-Ended Working Group (OEWG). In December 2018, the UN General Assembly adopted the formation of the Internet-focused OEWG that Russia proposed.[225] The OEWG was supposedly convened "with a view to making the United Nations negotiation process on security in the use of information and communications technologies more democratic, inclusive and transparent."[226] To some, the establishment of the OEWG could be an avenue whereby China, Russia, and their SCO allies can challenge the progress made by the GGEs and attempt to influence the United Nations in favor of their more authoritarian digital policies.[227]

World Trade Organization

In addition to leveraging its global influence to shape international cyberspace guidelines at the UN, China also seeks to use its influence to subvert World Trade Organization regulations and norms on digital commerce. In contrast to the United States' focus on addressing digital trade issues, China appears unwilling to come to an agreement at the WTO over what digital trade agreements should look like, intending to halt decisions that, if enacted, could encroach on its domestic digital governance.[228] China prefers that data flows and data storage be subjects for exploratory discussions, rather than commitments.[229] Further, as Nigel Cory at the Information Technology and Innovation Foundation argued, "China's approach to digital trade is largely focused on applying existing WTO rules (which are increasingly irrelevant) and a few narrow, non-binding technical provisions."[230]

Most existing rules related to digital trade have not been updated since the United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce in 1996, almost 25 years ago.[231] The Chinese government employs the current, broad rules to its advantage. One example of this is China's heavy emphasis on data localization, which governments

---

[224] United Nations, "Group of Government Experts," Dec. 2018, https://www.un.org/disarmament/group-of-governmental-experts/; Alex Grigsby, "The United Nations Doubles Its Workload on Cyber Norms, and Not Everyone Is Pleased," *Council on Foreign Relations*, Nov. 15, 2018.

[225] Alex Grigsby, "The United Nations Doubles Its Workload on Cyber Norms, and Not Everyone Is Pleased," *Council on Foreign Relations*, Nov. 15, 2018; Elaine Korzak, "What's Ahead in the Cyber Norms Debate?," *Lawfare*, Mar. 16, 2020, https://www.lawfareblog.com/whats-ahead-cyber-norms-debate.

[226] U.N. General Assembly, *Resolution Adopted by the General Assembly on 5 December 2018 (96)*, 73rd Session, Agenda item 96 (Dec. 11, 2018), https://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/73/27.

[227] Emilio Iasiello, "OEWG or GGE – Which Has the Best Shot of Succeeding?" *Technative*, Dec. 5, 2019, https://www.technative.io/oewg-or-gge-which-has-the-best-shot-of-succeeding/.

[228] *See, e.g.,* Nigel Cory, *Why China Should be Disqualified from Participating in WTO Negotiations on Digital Trade Rules,* Information Technology and Innovation Foundation (Mar. 2019), https://itif.org/publications/2019/05/09/why-china-should-be-disqualified-participating-wto-negotiations-digital.

[229] Congressional Research Service, *Internet Regimes and WTO E-Commerce Negotiations*, at 35, Jan. 28, 2020.

[230] Nigel Cory, *Why China Should be Disqualified from Participating in WTO Negotiations on Digital Trade Rules,* Information Technology and Innovation Foundation (Mar. 2019), https://itif.org/publications/2019/05/09/why-china-should-be-disqualified-participating-wto-negotiations-digital.

[231] *Id.*; United Nations Commission on International Trade Law, *UNCITRAL Model Law on Electronic Commerce (1996) with additional article 5 bis as adopted in 1998*, https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_commerce (last visited June 15, 2020).

can use to increase control of, and capture more value from, data produced within national borders.[232]

The effects of China's protectionism on global trade are concerning because, as Daniel Castro and Alan McQuinn at the Information Technology and Innovation Foundation wrote in 2015, data protectionism like what is practiced by China threatens:

> [N]ot just the productivity, innovation, and competiveness of tech companies, but all companies with an international presence. In today's global economy, it is common for businesses to process data from customers, suppliers, and employees outside the company's home country. Data protectionism makes such data processing much more difficult, if not impossible.[233]

World Internet Conference

Eager to establish its technical prowess on the world stage, China decided to launch its own global digital technology conference in 2014, which was hosted by the Cyberspace Administration of China.[234] Titled the "World Internet Conference," its goal was to "help build a cyberspace community with a consensual shared destiny and an ethic of respecting differences."[235]

One of the Chinese government's goals in this first conference was to have attendees sign the "Wuzhen Declaration," a nine-point document that echoed several official Chinese government goals, which they hoped would become the consensus of the attendees.[236] However, events did not go according to plan. As reported by the *Wall Street Journal*, the draft:

> [W]as slipped around the midnight hour Friday under the hotel room doors of attendees. It appeared to largely reflect a singular view: the watchful language used by Chinese President Xi Jinping. Chinese officials had argued at the two-day meeting of Chinese officials and local and foreign Internet executives that Beijing should have sovereignty over the Internet in China and must keep it under tight control.[237]

The plan to push an agreement through at the last minute was not successful, and the *Wall Street Journal* reported that at the end of the conference, the Wuzhen Declaration "was left unmentioned in the final speeches."[238]

---

[232] *See, e.g.,* "Data Governance Part One: Emerging Data Governance Practices," *Foreign Policy*, May 13, 2020.
[233] Daniel Castro & Alan McQuinn, *Cross-Border Data Flows Enable Growth in All Industries*, Information Technology & Innovation Foundation, at 9 (Feb. 2015), http://www2.itif.org/2015-cross-border-data-flows.pdf. *See also* Matthieu Pélissié du Rausas et al., "Internet matters: The Net's sweeping impact on growth, jobs, and prosperity," McKinsey and Company, May 2011, http://www.mckinsey.com/insights/high_tech_telecoms_internet/internet_matters.
[234] World Internet Conference, "2014 WIC Overview," Nov. 12, 2015, http://www.wuzhenwic.org/2015-11/12/c_46284.htm.
[235] *Id.*
[236] Catherine Shu, "China Tried To Get World Internet Conference Attendees To Ratify This Ridiculous Draft Declaration," *TechCrunch*, Nov. 21, 2014, https://techcrunch.com/2014/11/20/worldinternetconference-declaration/; World Internet Conference, "Draft Wuzhen Declaration," Nov. 21 2014, https://www.scribd.com/document/247566581/World-Internet-Conference-Draft-Declaration.
[237] James T. Arredy, "China Delivers Midnight Internet Declaration Offline," *The Wall Street Journal,* Nov. 21, 2014.
[238] *Id.*

The next year, President Xi attended the second World Internet Conference in person.[239] There, Xi used his opening remarks to lament the failures of the current system of Internet governance and argue that the world should "respect the right of individual countries to independently choose their own path of cyber development, model of cyber regulation and Internet public policies, and participate in international cyberspace governance on an equal footing."[240]

The participation of international technology companies at the World Internet Conference has also been a key aspect of China's efforts within this fora, although companies' involvement in the conference has been controversial. According to the World Internet Conference's official website, "prominent Internet figures from nearly 100 countries" have attended the conferences, including representatives from technology companies.[241] Such participation drew criticism from Roseann Rife, the East Asia Research Director at Amnesty International, who has long called for technology companies to reject China's Internet rules, stating that "Chinese authorities are trying to rewrite the rules of the internet so censorship and surveillance become the norm everywhere."[242]

Fortunately for the defenders of a free and open Internet, China has not achieved its goals through the World Internet Conference. According to Adam Segal, "[d]espite a significant investment of time, money, and political capital, the reach and influence of the World Internet Conference remain limited to China's friends. Most of the heads of government that have attended are from small states or the SCO."[243]

But China does not appear deterred. The 7th World Internet Conference, tentatively scheduled for the fourth quarter of 2020, is titled the "Light of Internet" Expo.[244] The press release announcing the conference says it is "expected to be a grand event for showcasing the latest technologies, products and applications around the world."[245]

International Standards-Setting Bodies

Another realm that China seeks to influence, along with the major multilateral institutions, is global ICT standards-setting bodies. Global ICT rules of the road are set by several organizations, one of

---

[239] Adam Segal, "China's Internet Conference: Xi Jinping's Message to Washington," *Council on Foreign Relations*, Dec. 16, 2015.
[240] Xi Jinping, President of the People's Republic of China, Remarks at the "Opening Ceremony of the Second World Internet Conference," Wuzhen, China, Dec. 16, 2015, https://www.fmprc.gov.cn/mfa_eng/wjdt_665385/zyjh_665391/t1327570.shtml; *See also* Adam Segal, "Chinese Cyber Diplomacy in a New Era of Uncertainty," *Hoover Institution*, June 2017, at 9, https://www.hoover.org/sites/default/files/research/docs/segal_chinese_cyber_diplomacy.pdf.
[241] World Internet Conference, "World Internet Conference Overview of WIC," Nov. 10, 2015, http://www.wuzhenwic.org/2015-11/10/c_46113.htm (last visited July 10, 2020). *See also* Adam Segal, "Chinese Cyber Diplomacy in a New Era of Uncertainty," *Hoover Institution*, June 2017, at 10, https://www.hoover.org/sites/default/files/research/docs/segal_chinese_cyber_diplomacy.pdf.
[242] Amnesty International, Asia and the Pacific, Internet and Social Media, "Tech Companies Must Reject China's Repressive Internet Rules," Dec. 15 2015, https://www.amnesty.org/en/latest/news/2015/12/tech-companies-must-reject-china-repressive-internet-rules/ (last visited July 10, 2020).
[243] Adam Segal, "Chinese Cyber Diplomacy in a New Era of Uncertainty," *Hoover Institution*, June 2017, at 1, https://www.hoover.org/sites/default/files/research/docs/segal_chinese_cyber_diplomacy.pdf. SCO referenced in the quote is the Shanghai Cooperation Organization.
[244] World Internet Conference, "Fore-Notice on The Light of Internet Expo in the 7th World Internet Conference," Apr. 08 2020, http://www.wuzhenwic.org/2020-04/08/c_469136.htm.
[245] *Id.*

which is the 3rd Generation Partnership Project (3GPP), a private sector partnership composed of seven telecommunications standards development organizations.[246] 3GPP examines the range of technologies that make up mobile telecommunications, including radio access, core networks, cellular technologies, and services.[247] According to the U.S.-China Commission, "[t]he number of Chinese representatives serving in chair or vice chair leadership positions [in the 3GPP] rose from 9 of the 53 available positions in December 2012 to 11 of the 58 available positions in December 2017."[248] Due to this prominence in the organization's leadership, China has the capacity to influence the 3GPP to its advantage.[249]

Another entity heavily influenced by the Chinese is the International Telecommunications Union (ITU). According to its website, ITU "help[s] shape the future ICT policy and regulatory environment, global standards, and best practices to help spread access to ICT services."[250] Since 2014, the Secretary-General of the ITU has been Houlin Zhao, a former delegate at the Designing Institute of the Ministry of Posts and Telecommunications of China.[251] In addition to a former Chinese official being at the head of the ITU, Chinese firms and government research institutes held the largest number of chair and vice chair positions in the ITU's 5G-related standards-setting bodies, with eight of the 39 available leadership positions as of September 2018.[252] According to Michael O'Rielly of the U.S. Federal Communications Commission, the Chinese "have loaded up the voting to try to get their particular candidates on board, and their particular standards."[253]

Furthermore, it appears that as the head of the ITU, Secretary-General Zhao has used his position to strengthen China's digital influence around the world. The ITU-China agreement on aiding countries with communications networks resulted in ITU-China specific projects such as research and training centers for ICT in Afghanistan, a Trans-Eurasian Information Superhighway, and research and construction projects in Africa.[254] Secretary-General Zhao told *China Daily* that it is "highly likely" that he would sign another deal with the Export-Import Bank of China, and that working with China is critical for the ITU.[255] Finally, he added that China's Belt and Road is the perfect platform "to deliver services and help with ICT development around the globe by cooperating with China through the Initiative."[256]

Zhao Yonghong, Director-General of the Department of International Cooperation in the Ministry of Industry and Information Technology of the People's Republic of China, offered additional context on China's role in the ITU in September 2018. Zhao stated that the ITU should focus on "[s]trengthen[ing] the leading role of ITU in ICT technical standardization and further enhanc[ing]

---

[246] 3GPP, "About 3GPP," https://www.3gpp.org/about-3gpp (last visited July 6, 2020).
[247] *Id.*
[248] U.S.-China Economic and Security Review Commission, *2018 Annual Report to Congress*, at 455 (Nov. 2018).
[249] *Id.*
[250] International Telecommunication Union, "About International Telecommunication Union (ITU)," Feb. 19, 2020, https://www.itu.int/en/about/Pages/default.aspx.
[251] International Telecommunications Union, "Biography – Houlin Zhao," (last visited July 6, 2020), https://www.itu.int/en/osg/Pages/biography-zhao.aspx.
[252] U.S.-China Economic and Security Review Commission, *2018 Annual Report to Congress,* at 454 (Nov. 2018).
[253] Todd Shields & Alyza Sebenius, "Huawei's Clout Is So Strong It's Helping Shape Global 5G Rules," *Bloomberg,* Feb. 1, 2019.
[254] Kong Wenzheng, "ITU Vows to Join Hands with China," *China Daily*, May 24, 2019, www.chinadaily.com.cn/a/201904/24/WS5cbfbb1aa3104842260b7f2f.html.
[255] *Id.*
[256] *Id.*

its influence in the field of global standardization of emerging ICT technologies."[257] In fact, in 2012, China—along with other authoritarian regimes, like Russia and Saudi Arabia—introduced a proposal at the World Conference on International Telecommunications making ITU jurisdiction over the Internet more powerful.[258] Given China's leadership at the ITU, this proposal could strengthen China's control of the Internet.

China's strategy of using multilateral institutions to its advantage appears to have paid off at the ITU. Evidence of this success includes not only Zhao's support of Huawei, which in 2019 he defended against the United States' 5G security concerns by calling them driven by politics rather than evidence, but also China's ushering in of the proposed "New Internet Protocol" (New IP).[259] Some nations, including the United Kingdom, Sweden, and the United States, have raised concerns that China's New IP plan, if enacted, would fracture the global Internet and give state-run Internet Service Providers too much control.[260] The *Financial Times* reports that Huawei and other co-developers of New IP plan to promote the proposal at an ITU telecommunication conference in India in November 2020.[261] Zhao, as the head of the ITU, could influence whether the New IP is ratified.

However, there does appear to be some hope for democracies in the global battleground over control of international standards-setting bodies. In March 2020, the World Intellectual Property Organization—the United Nations organization created to lead the development of a balanced and effective international IP system—announced that Daren Tang, a Singapore national, won the nomination to become the new Director General.[262] Tang, who had the backing of the United States, was congratulated upon his election by Secretary Pompeo, who described him as "an effective advocate for protecting intellectual property [and] a vocal proponent of transparency and institutional integrity."[263]

The contest between Tang and his main opponent, the China-backed candidate Wang Binying, was a battle in the global digital arena between the United States and China.[264] In this case, and in what many hope will be an indication of future outcomes in the global competition between freedom and surveillance, the ideals of transparency and international cooperation won the day.

---

[257] "Top Contributors: Why China Supports ITU," *ITU News*, Sept. 20 2018, news.itu.int/top-contributors-why-china-supports-itu/.
[258] Chris Welch, "Russia, China, and Other Nations Draft Proposal to Give ITU Greater Influence Over the Internet," *The Verge,* Dec. 9 2012; Adi Robertson, "New World Order: is the UN about to take control of the internet?," The Verge, Nov. 29, 2012.
[259] Tom Miles, "Huawei Allegations Driven by Politics Not Evidence: U.N. Telecoms Chief," *Reuters,* Apr. 5 2019; Anna Gross & Madhumita Murgia, "China and Huawei Propose Reinvention of the Internet," *Financial Times,* Mar. 27 2020.
[260] Anna Gross & Madhumita Murgia, "China and Huawei Propose Reinvention of the Internet," *Financial Times,* Mar. 27 2020.
[261] *Id.*
[262] Nick Cummings-Bruce, "U.S.-Backed Candidate for Global Tech Post Beats China's Nominee," *The New York Times*, Mar. 4, 2020. *See also* The World Intellectual Property Organization, "What Is WIPO?" www.wipo.int/about-wipo/en/ (Last Visited May 21, 2020).
[263] Press Statement, U.S. Secretary of State Michael R. Pompeo, "Election of Daren Tang of Singapore as Director General of the World Intellectual Property Organization," Mar. 4 2020; Nick Cummings-Bruce, "U.S.-Backed Candidate for Global Tech Post Beats China's Nominee," *The New York Times*, Mar. 4, 2020.
[264] Nick Cumming-Bruce, "U.S.-Backed Candidate for Global Tech Post Beats China's Nominee," *The New York Times,* Mar. 4. 2020.

Chapter 4: Conclusions and Recommendations

China's new model of digital authoritarianism, its international efforts to assert economic dominance in the digital domain, and its promotion of the adoption of a Chinese-inspired model of digital governance abroad, show its desire to alter and control the future of the digital domain. As described in Chapter 1, China is altering and controlling the digital domain domestically. It has developed and employed emerging technologies and techniques, ranging from blocking online content to utilizing facial recognition technologies that strengthen its surveillance systems, in order to suppress populations, individuals, and entities not aligned with the Chinese Communist Party (CCP).

While the CCP's use of the digital domain to maintain social control is problematic for those suffering in China, China's growing digital influence on the global stage creates a broader problem for the international community as China proliferates its technologies at a rapid rate around the globe, and in countries that span the spectrum of governance. As shown in Chapter 2, even countries that are staunch U.S. allies and stand for similar democratic and human rights values are entertaining the integration of Chinese technologies into their own digital infrastructures, such as 5G telecommunications, due to low costs, lack of viable alternatives, uncertainty about the future direction of the United States, and China's robust economic and diplomatic efforts.[265] As demonstrated in Chapter 3, China is leveraging its newfound influence to shape the rules of the road for the digital domain in ways that cater to digital authoritarianism and is antithetical to the United States' vision of how the Internet and cyber-enabled technologies should be used.

Indeed, three and a half years into the Trump administration, the United States is now on the precipice of losing the future of the cyber domain to China. If China continues to perfect the tools of digital authoritarianism and is able to effectively implement them both domestically and abroad, then China, not the United States and its allies, will shape the digital environment in which most of the world operates. Additionally, if the United States continues to cede its traditional role of diplomatic and technological leadership, the global growth of China's digital authoritarianism model presents a sinister future for the digital domain. At the grand strategic scale, if digital authoritarianism flourishes, China's importance on both the digital and global stages will continue to grow, allowing China to surpass the United States in the digital space and empowering China to create the future rules for digital governance.[266]

The spread of digital authoritarianism may also affect the United States' relationships with other countries as they determine how to balance their relationships with China, especially in the face of growing pressure to mirror China's authoritarian behavior in the digital domain. Furthermore, the basic human rights of individuals around the world, including U.S. citizens, could be negatively affected by a cyber domain that is reliant on Chinese technologies and values. As seen in places such as Xinjiang, personal privacy and civil liberties are threatened by China's digital authoritarianism model.[267] The global proliferation of China's digital authoritarianism model, if unchecked, will see

---

[265] Heather Stewart & Dan Sabbagh, "UK Huawei Decision Appears to Avert Row with US," *The Guardian*, Jan. 28, 2020.

[266] *See, e.g.,* John Chen et al., *China's Internet of Things,* Research Report Prepared on Behalf of the U.S.-China Economic and Security Review Commission, by SOS International (SOSi), at 69 (Oct. 2018).

[267] *See, e.g.,* Lindsay Maizland, "China's Repression of Uighurs in Xinjiang," *Council on Foreign Relations*, updated June 30, 2020, https://www.cfr.org/backgrounder/chinas-repression-uighurs-xinjiang; U.S. Department of State, 2018 Report on

even more individuals fall under the control of authoritarians who use these technologies and techniques.

Despite China's various gains within the digital domain, such as its emerging technical capabilities and growing economic strength, there is still significant opportunity for the United States to adopt a genuinely competitive strategy and approach to China, to remain the global leader on cyberspace governance, and to reassert its leadership in areas where the technological gap between the United States and China has shrunk or disappeared. Accomplishing these goals will mark an important step in competing with China's digital authoritarianism, as opposed to merely denouncing it. Achieving the goal of securing a free digital domain and mitigating the threat of digital authoritarianism, however, will require a whole-of-government approach that leverages all aspects of the U.S. government, the private sector, and, critically, genuine partnerships with our partners and allies on the world stage. The Administration's current policy, which is detailed in Annex 1 of this report, is insufficient to combat China's digital authoritarianism, and its alienation of allies has further stunted the United States' ability to influence other countries away from China's digital authoritarianism model.

Recommendations

This report offers the following recommendations for more effective U.S. action to counter China's digital authoritarianism.

- ***Develop and Deploy Alternatives to Chinese 5G Technology with U.S. Allies****:* The United States lags behind China in developing and deploying cutting-edge 5G technologies, both domestically and abroad.[268] To provide an alternative, the U.S. should:
    - *Establish a Federally Funded Research and Development Center (FFRDC) on 5G*: Congress should pass legislation to establish an FFRDC that will examine how the United States can surpass China in the 5G development space. The FFRDC should examine U.S. technological strengths and weaknesses, as well as areas for immediate telecommunications development to provide an alternative to Chinese platforms and technologies.
    - *Create an Industry Consortium on 5G:* Congress should create a consortium comprised of leading U.S. telecommunications and technology companies that would be mandated to create the American 5G telecommunications alternative, exploring both cost-effective hardware and software solutions.
    - *Invest in Radio Access Network (RAN) Technologies:* Congress should provide new appropriations for RAN technologies.[269]

International Religious Freedom: China: Xinjiang, May 23, 2019, *available at* https://www.state.gov/reports/2018-report-on-international-religious-freedom/china-includes-tibet-xinjiang-hong-kong-and-macau/xinjiang/.

[268] Stu Woo, "In the Race to Dominate 5G, China Sprints Ahead," *The Wall Street Journal*, Sept. 7, 2019.

[269] "What are Radio Access Networks and 5G RAN?," *Verizon*, Feb. 2, 2020, https://www.verizon.com/about/our-company/5g/5g-radio-access-networks (last visited July 10, 2020). According to *Verizon,* "[c]ell phones use radio waves to communicate by converting your voice and data into digital signals to send through as radio waves. In order for your cell phone to connect to a network or the internet, it connects first through a radio access network (RAN). Radio access networks utilize radio transceivers to connect you to the cloud. Most base stations (aka transceivers) are primarily connected via fiber backhaul to the mobile core network." *Id.*

- *Establish a 5G Policy Coordinator within the White House*: The President should establish the position of a 5G Policy Coordinator tasked with coordinating the U.S. government's domestic and international 5G strategy.

❖ ***Limit the Spread of Malign Chinese Surveillance Technologies and Digital Authoritarianism****:* China is a leading developer and exporter of surveillance technologies, and continues to integrate new technologies that provide increasingly intrusive surveillance capabilities that can be misused by China or other state actors.

- *Establish a Digital Rights Promotion Fund:* Congress should establish and authorize a Digital Rights Promotion Fund, which will provide grants and investments directly to entities that support the promotion of a free, secure, stable, and open digital domain and fight against the authoritarian use of information and communications technologies. The fund will provide these groups, especially those existing in countries experiencing undue surveillance or other forms of digital authoritarianism, the resources needed to better push back against the spread of digital authoritarianism. Groups able to receive money would include:
  - Local activist organizations promoting a free digital domain and working to counter oppressive surveillance regimes in countries where digital authoritarianism is apparent or on the rise.
  - Nonprofit organizations that advocate for the adoption of international governance standards for the digital domain based on openness, transparency, and the rule of law, including the protection of human rights.
  - Think tanks and other institutional bodies that provide scholarship and policy recommendations for best paths forward to protect against the rise of authoritarian surveillance.
- *Establish an International Digital Infrastructure Corporation*: Congress should establish an independent, non-profit corporation with a clear and specific mandate to provide foreign countries with low-interest loans, grants, and other financing opportunities to purchase and implement U.S.-made digital infrastructure.
- *Authorize the Open Technology Fund*: Congress should fully authorize funds for the Open Technology Fund by passing S. 3820, the Open Technology Fund Authorization Act sponsored by Senators Robert Menendez, Marsha Blackburn, Ron Wyden, and Rick Scott.

❖ ***Strengthen the U.S. Digital Workforce****:* In order to compete and lead the digital space in the future, the United States will need an adaptable, innovative, and capable cyber workforce.

- *Establish a Cyber Service Academy*: Through legislative action, Congress should establish a new federal service academy similar to our other military service academies, with the specific aim of developing the future of our technology force. In addition to providing students a four year undergraduate education, the academy shall prepare students to become future military leaders in key digital and emerging technology fields, including robotics, artificial intelligence (AI), and cybersecurity.
- *Boost funding for STEM programs*: Congress should significantly increase federal spending on STEM programs, including Department of Defense (DoD)

funding in the National Defense Education program, funding for the National Science Foundation, and funding for the Minority Science and Engineering Improvement program within the Department of Education.

- ***Reinvigorate U.S. Diplomatic Leadership and Alliances, and Take a More Robust Role on the International Stage****:* China has made a concerted effort to change norms and practices to strengthen its position in various international fora regarding the digital domain.[270] China has additionally pushed economic development relating to technology in critical regions throughout the world.[271]
    - *Build a Coalition of Likeminded Allies on Critical Technology Issues:* The President should lead an international effort, in coordination with our allies and partners, to counter Chinese efforts to develop and proliferate digital domain products, technologies, and services that are not predicated on free, democratic values.
    - *Establish Mutual Cyber Defense Agreements*: The United States should approach likeminded nations to develop and establish mutual cyber defense and cooperation agreements that ensure national critical infrastructure, secure communications, trade relationships, and civil liberties are protected against cyber-attacks.
    - *Reassert U.S. Leadership in International Fora:* The President should establish a strategy for ensuring the United States holds chairmanships, serves as a leading voice, and operates as a key player in international fora such as the International Telecommunications Union or UN Group of Governmental Experts.
    - *Establish and Empower New Cyber Leadership within the State Department:* Congress should pass the Cyber Diplomacy Act of 2019, or similar legislation, that establishes a new office or bureau of cyber issues at the State Department, which shall report to the Under Secretary for Political Affairs.

[270] John Chen et al., *China's Internet of Things,* Research Report Prepared on Behalf of the U.S.-China Economic and Security Review Commission, by SOS International (SOSi), at 69 (Oct. 2018).
[271] *Id.*

Annex 1: Understanding the Trump Cyberspace Policy

The United States is at a crossroads in regards to countering the implementation and growth of digital authoritarianism led by the regime in China. China's efforts to bring about the rise of digital authoritarianism hold the potential to fundamentally alter the landscape of information and communications technologies, as well as the legal and institutional underpinnings of these digital technologies, in ways that are incongruent with U.S. values and detrimental to U.S. and allied economic and security interests. Issues ranging from Chinese domination of the global information infrastructure and taking advantage of communications vulnerabilities, to using new technologies to assault basic human rights, to inhibiting U.S. economic and business opportunities abroad because of unreliable and exposed digital networks are all on the table if digital authoritarianism continues to proliferate unfettered.

It is imperative for the United States to perform its role as the leading force in developing, sustaining, and promulgating a global digital order based on openness, transparency, and the rule of law, including the protection of human rights. If the United States and other democratic countries are unable or unwilling to work to reverse the concerning trend of China's rising digital authoritarianism, we will cede the future of the global digital order to China and other authoritarian regimes. This annex examines President Trump and his Administration's efforts and policies, as well as recent Congressional actions, regarding cyberspace and whether these actions effectively curb China's digital authoritarianism.

National Security Policy Documents

In September 2018, the Trump administration released its National Cyber Strategy (NCS). As a foundational policy document for the Administration, the NCS sets the stage for how the United States views the current climate within the cyber domain and how, broadly, they tackle issues that arise. The Trump administration frames the cyber domain as one where the United States is "in a continuous competition against strategic adversaries, rogue states, and terrorist and criminal networks."[272] Such a characterization builds upon the labeling in the Trump administration's National Security Strategy (NSS), which describes China's exploitation of data and its alleged attempts to spread features of its authoritarian system, including corruption and the use of surveillance technology.[273]

By framing China and the cyber domain this way, the Trump administration fits the issues contained in cyberspace within one of the principal characteristics of its national security strategy: that the United States is in a great-power competition with key adversaries. The NCS proceeds to specifically label China as one of the entities that is challenging the United States within the cyber domain.[274] While the document falls short of directly identifying the Chinese Communist Party's use of digital authoritarianism as a national security threat, the NCS articulates a need to defend against authoritarian states utilizing security or terrorism concerns to erode a free and secure Internet.[275]

The NCS breaks U.S. cyber strategy into four pillars. These pillars are:

---

[272] President Donald J. Trump, *National Cyber Strategy of the United States of America*, The White House, Sept. 2018, at 2.
[273] Congressional Research Service, Research Conducted for Committee Staff, Sept. 30, 2019.
[274] President Donald J. Trump, *National Cyber Strategy of the United States of America*, The White House, Sept. 2018, at 2.
[275] *Id.*, at 24.

1) Protect the American People, the Homeland, and the American Way of Life – involving issues such as protecting U.S. networks, critical infrastructure, and data, combatting crime, and pushing government innovation;
2) Promote American Prosperity – including promoting America's advantage in the digital economy, maintaining U.S. leadership on cyber issues, and strengthening the U.S. workforce;
3) Preserve Peace through Strength – featuring deterring malign cyber activities and enhancing norms of state behavior;
4) Advance American Influence – containing extending a free and interoperable Internet globally and building international cyber capacity.[276]

From these four platforms flow priority actions meant to target certain issues, ranging from building a proposed cyber deterrence initiative, to "promot[ing] and maintain[ing] markets for United States ingenuity worldwide," to maintaining United States leadership in emerging technologies.[277] Due to China's continued growth within the cyber domain, many of these priority actions in effect target digital authoritarianism in some way. For example, the NCS outlines a need to broadly engage global partners, international organizations, and civil society to protect Internet freedom and improve international cyber capacity.[278] Critical to this effort is the need for the U.S. to reinforce the openness, interoperability, and reliability of the Internet.[279] The plan calls for investment in the communications infrastructure and cybersecurity capacities of partner states to not only enhance the Cyber Deterrence Initiative, but also to ensure their Internet capabilities align with U.S. interests and standards of Internet freedom.[280]

There are other mechanisms espoused in the NCS that could play a role in combatting China's digital authoritarianism that are not explicitly linked to the topic. One such example is how a primary objective of "promoting American prosperity" in the NCS is to "preserve U.S. influence in the technological ecosystem and the development of cyberspace as an open engine of economic growth, innovation, and efficiency."[281] The purpose of this objective is to "foster a vibrant and resilient digital economy" through prioritizing innovation and maintaining U.S. leadership in emerging technologies.[282]

---

[276] President Donald J. Trump, *National Cyber Strategy of the United States of America*, The White House, Sept. 2018, at 6, 8, 10, 14, 16, 17, 20, 21, 24, 25, and 26; Congressional Research Service, Research Conducted for Committee Staff, Sept. 30, 2019.
[277] President Donald J. Trump, *National Cyber Strategy of the United States of America*, The White House, Sept. 2018, at 15, 21, 25.
[278] *Id.*, at 25 and 26. According the National Cyber Strategy, cyber capacity building involves "the United States build[ing] strategic partnerships that promote cybersecurity best practices through a common vision of an open, interoperable, reliable, and secure Internet that encourages investment and opens new economic markets. In addition, capacity building allows for additional opportunities to share cyber threat information, enabling the United States Government and our partners to better defend domestic critical infrastructure and global supply chains, as well as focus whole-of government cyber engagements." *Id.*
[279] *Id.*, at 24.
[280] *Id.*, at 21 and 26. Espoused in the Administration's 2018 National Cyber Strategy, the Cyber Deterrence Initiative is an effort "to build such a coalition and develop tailored strategies to ensure adversaries understand the consequences of their malicious cyber behavior." To achieve this goal, "the United States will work with like-minded states to coordinate and support each other's responses to significant malicious cyber incidents, including through intelligence sharing, buttressing of attribution claims, public statements of support for responsive actions taken, and joint imposition of consequences against malign actors." *Id.* at 21.
[281] *Id.*, at 14.
[282] *Id.*, at 14-15; Congressional Research Service, Research Conducted for Committee Staff, Sept. 30, 2019.

Another key issue put forth by the NCS to help the United States better compete in the digital marketplace and fight back against digital authoritarianism is strengthening its leadership on innovation and developing emerging technologies.[283] One of the primary aspects for driving U.S. technological development leadership is to promote the free flow of data across borders that push against authoritarian governments' attempts to localize data under the guise of national security, and, along that vein, the NCS asserts that the Administration will promote "open, industry driven standards, innovative products, and approaches that permit global innovation and the free flow of data while meeting the legitimate security needs of the U.S."[284] Additionally, the NCS aims to ensure the United States counters behavior that acts against U.S. interests, saying in its third pillar that the administration would use "all appropriate tools of national power to expose and counter the flood of online malign influence and information campaigns and non-state propaganda and disinformation."[285]

Administration Efforts

China continues to rapidly expand its digital authoritarianism model and make gains on the United States in becoming the dominant player on a range of critical technologies, placing U.S. leadership on cyber issues at risk. In response to the gains in Chinese technological development, the Trump administration has turned to punitive measures, using sanctions as a weapon against China. As China's technology sector begins to achieve global significance, several of its players have found themselves on the front lines of the U.S.-China trade war and atop U.S. sanctions lists.[286] Most notably, one of China's largest companies, Huawei, has been the target of U.S. sanctions and restrictions as the U.S. seeks to pre-empt potential cyber threats.[287] The Trump administration has referred to Huawei as a national security threat, cited the telecommunications giant's close ties to the Chinese government, its repeated intellectual property theft, and its violations of U.S. sanctions on Iran as reasons for Huawei to be excluded from U.S. markets, and encouraged others to take similar steps.[288]

Although U.S. suspicions of Huawei can be traced as far back as 2012, recent actions are supposedly meant to demonstrate a more aggressive U.S. posture towards the company and the Chinese

---

[283] Congressional Research Service, Research Conducted for Committee Staff, Sept. 30, 2019.
[284] *Id.*; President Donald J. Trump, *National Cyber Strategy of the United States of America*, The White House, Sept. 2018, at 14.
[285] Congressional Research Service, Research Conducted for Committee Staff, Sept. 30, 2019; President Donald J. Trump, *National Cyber Strategy of the United States of America*, The White House, Sept. 2018, at 21.
[286] Kiran Stacey et al., "US blacklists 28 Chinese entities in trade war escalation," *Financial Times*, October 8, 2019; Ana Swanson, "U.S. Delivers Another Blow to Huawei With New Tech Restrictions," *The New York Times*, May 15, 2020.
[287] Ana Swanson, "U.S. Delivers Another Blow to Huawei With New Tech Restrictions," *The New York Times*, May 15, 2020; Associated Press, "US Adds New Sanction on Chinese Tech Giant Huawei," *US News and World Report*, May 16, 2020.
[288] Ana Swanson, "U.S. Delivers Another Blow to Huawei With New Tech Restrictions," *The New York Times*, May 15, 2020; David Goldman, "What Did Huawei do to Land in Such Hot Water with the US?" *CNN,* May 20, 2019; Federal Communications Commission, "FCC Bars Use of Universal Service Funding for Equipment and Services Posing National Security Risks," Nov. 22, 2019; Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs; Huawei Designation; ZTE Designation, 85 Fed. Reg. 27610, Jan. 3, 2020; Dan Strumpf & Patricia Kowsmann, "U.S. Prosecutors Probe Huawei on New Allegations of Technology Theft," *The Wall Street Journal,* Aug. 29, 2019; Julian E. Barnes and Adam Satariano, "U.S. Campaign to Ban Huawei Overseas Stumbles as Allies Resist," *The New York Times*, Mar. 17, 2019.

technology sector as a whole.[289] In May 2018, the Pentagon banned the sale of Huawei and ZTE phones on U.S. military bases.[290] Later that year, Huawei's CFO (and daughter of its founder), Meng Wanzhou, was arrested in Canada at the United States' request for allegedly violating U.S. sanctions on Iran.[291] On May 15, 2019, President Trump issued Executive Order 13873 on Securing the Information and Communications Technology and Services Supply Chain, which declared:

> The threat of foreign adversaries to U.S. ICT technologies—through creating and exploiting vulnerabilities in technology and services, and "the unrestricted acquisition or use in the United States of information and communications technology or services, designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of foreign adversaries"—constitutes an "unusual and extraordinary threat to the national security, foreign policy, and economy of the United States."[292]

Following the Executive Order issuance, the United States in May 2019 placed Huawei and 68 of its affiliates on the Bureau of Industry and Security's Entity List via authorities in the Export Control Reform Act of 2018's Export Administration Regulations, and subsequently in August added 46 additional entities, in an effort to restrict their access to U.S. markets.[293] In May 2020, the administration unveiled new rules requiring foreign semiconductor makers to obtain a U.S. license to ship Huawei-designed semiconductors produced using U.S. technology to Huawei.[294] More broadly, the United States has sought to mount pressure on allies and partners such as Germany and the UK to restrict Huawei equipment in their 5G infrastructure plans due to security concerns.[295] These efforts, however, have produced mixed results at best, and may well have been counterproductive, at least in the short-term, as seen in Chapter 2 of this report.

Unfortunately, contradictory U.S. policy implementation has hampered the impact of punitive measures to change China's behavior. This contradiction can be seen in the Commerce Department's provision of temporary licenses to Huawei despite the administration's stated need and previous actions for increasing scrutiny of Huawei transactions.[296] The Commerce Department unveiled that the:

---

[289] Sean Keane, "Huawei ban timeline: Uber rival hits AppGallery store as it moves towards self-sufficiency," *CNET,* June 25, 2020; Pam Benson, "Congressional report: U.S. should 'view with suspicion' two Chinese companies," *CNN*, Oct. 8, 2012.
[290] Sean Keane, "Huawei ban timeline: Uber rival hits AppGallery store as it moves towards self-sufficiency," *CNET,* June 25, 2020; Katie Collins, "Pentagon bans sale of Huawei, ZTE phones on US military bases," *CNET*, May 2, 2018.
[291] Press Release, U.S. Department of Justice, "Chinese Telecommunications Conglomerate Huawei and Huawei CFO Wanzhou Meng Charged with Financial Fraud," January 28, 2019; Dan Bilefsky, "Extradition Hearings Begin for Meng Wanzhou, Huawei Officer Held in Canada," *The New York Times*, Jan. 20, 2020.
[292] Congressional Research Service, Research Conducted for Committee Staff, Sept. 30, 2019; President Donald J. Trump, *Executive Order on Securing the Information and Communications Technology and Services Supply Chain*, The White House, May 15, 2018; U.S. Department of Commerce - Securing the Information and Communications Technology and Services Supply Chain, 84 Fed. Reg. 65316, Nov. 27, 2019.
[293] Addition of Certain Entities to the Entity List and Revision of Entries on the Entity List, 84 Fed. Reg. 43493, Aug. 21, 2019; Addition of Entities to the Entity List, 84 Fed. Reg. 22961, May 21, 2019.
[294] Frank Bajak, "US adds new sanction on Chinese tech giant Huawei," *Associated Press*, May 16, 2020.
[295] Julian E. Barnes & Adam Satariano, "U.S. Campaign to Ban Huawei Overseas Stumbles as Allies Resist," *The New York Times*, March 17, 2019.
[296] Congressional Research Service, Research Conducted for Committee Staff, Sept. 30, 2019; Addition of Entities to the Entity List, 84 Fed. Reg. 22961, May 21, 2019.

> Bureau of Industry and Security (BIS) issued a 90-day Temporary General License to allow for the completion by August 19th of contracts entered into before May 16th. On August 15th, BIS issued an additional General License to allow for some engagement with Huawei and its affiliates to continue.[297]

While a variety of factors enter into how BIS decides whether a company should receive certain export or transfer waivers, the provision of multiple waivers to Huawei and other entities fundamentally conflicts with the Administration's stated desire to mitigate the risks associated with increased proliferation of Huawei technologies. Consequently, episodes such as this one highlight how the Administration's policy and actions are not in sync, damaging the United States' ability to push back on essential levers of China's digital authoritarianism system.

For its part, Huawei has loudly decried U.S. actions taken against the company, through both legal challenges and public statements. For example, the company filed a suit against the FCC for a ruling in November 2019 blocking the use of federal funds to purchase Huawei products, saying "it fails to offer Huawei required due process protections."[298] The company has questioned the United States' motives for targeting Huawei, asserting that the United States "is leveraging its own technological strengths to crush companies outside its own borders. This will only serve to undermine the trust international companies place in US technology and supply chains."[299] Huawei has even accused the U.S. of illegal behavior such as hacking its systems and threatening its employees.[300]

In response to the growing threats posed by digital authoritarianism, the federal government has taken steps towards improving U.S. cybersecurity capabilities. In 2018, President Trump signed the Cybersecurity and Infrastructure Security Agency Act into law, establishing the Cybersecurity and Infrastructure Security Agency (CISA) within the Department of Homeland Security (DHS).[301] CISA's mission is to "lead the National effort to understand and manage cyber and physical risk to our critical infrastructure.[302] The agency's formation is a step toward securing U.S. domestic cyber infrastructure; however, as an agency within DHS, its mandate does not extend into the international realm, and therefore is unlikely to be able to play a role in pushing back against China's spread of digital authoritarianism around the globe.

The State Department, which oversees international diplomatic efforts regarding the cyber domain, does not currently have the structure needed to effectively tackle China's growing influence in the digital sphere. In 2018, the State Department released proposals to establish a Bureau of Cyberspace Security and Emerging Technologies (CSET), which would consolidate and strengthen U.S. diplomatic efforts to secure cyberspace and digitally enabled technologies, reduce risks of cyber

---

[297] Congressional Research Service, Research Conducted for Committee Staff, Sept. 30, 2019; Temporary General License: Extension of Validity, Clarifications to Authorized Transactions, and Changes to Certification Statement Requirements, 84 Fed. Reg. 43487, August 21, 2019; Addition of Certain Entities to the Entity List and Revision of Entries on the Entity List, 84 Fed. Reg. 43493, Aug. 21, 2019.
[298] Norman Pearlstine et al., "The War Against Huawei," *Los Angeles Times*, Dec. 19, 2019; Colin Lecher, "The FCC votes to block Huawei from billions in federal aid," *The Verge*, Nov. 22, 2019.
[299] Eileen Yu, "Huawei rebukes US attempts to stymie foreign competition with chip rule," *ZDNet*, May 18, 2020.
[300] Dan Strumpf & Chuin-Wei Yap, "Huawei Accuses the U.S. of Cyberattacks and Staff Threats," *The Wall Street Journal*, Sept. 3, 2019.
[301] Cybersecurity and Infrastructure Security Agency, "About CISA," https://www.cisa.gov/about-cisa (last visited May 10, 2020).
[302] *Id.*

conflict, and boost America's cyber competitiveness.[303] In the proposal, the Bureau would operate under the office of the Under Secretary for Arms Control and International Security Affairs.[304] However, the rollout was stalled in Congress due to negotiations over the bureau's placement and a lack of clarity over its mandate.

One alternative to CSET—the Cyber Diplomacy Act of 2019—was introduced in Congress by Representatives McCaul (R-TX-10) and Engel (D-NY-16) in January 2019.[305] The Cyber Diplomacy Act would create an Office of International Cyberspace Policy (OICP), operating under the State Department's Under Secretary of Political Affairs. In addition to advising the State Department on cyberspace policy, the office would engage in diplomatic efforts to reinforce international cybersecurity, promote Internet access and freedom, and counter international cyber threats. The bill directly calls out China for promoting international norms of Internet behavior that restrict critical freedoms. In addition, the bill requires the OICP to produce annual country reports on human rights practices relating to the Internet, particularly emphasizing online censorship and political repression.[306]

[303] Sean Lyngaas, "State Department Proposes New $20.8 million Cybersecurity Bureau," *Cyberscoop,* June 5, 2019, https://www.cyberscoop.com/state-department-proposes-new-20-8-million-cybersecurity-bureau/.
[304] U.S. Department of State, Congressional Budget Justification Appendix 1: Department of State Diplomatic Engagement, Fiscal Year 2021.
[305] Cyber Diplomacy Act of 2019, H.R. 739 (116th Congress, introduced Jan. 24, 2019).
[306] *Id.*

Annex 2: The United States and 5G

One of the most prominent and pressing issues facing the United States regarding the future of the digital domain is the development and deployment of 5G telecommunications technologies. 5G technologies, following on fourth generation (4G) and LTE technologies, provide a number of improvements to the capabilities of previous generations, including increased data transfer rates in a fixed period of time, also known as bandwidth, and enhanced connectivity capabilities, such as ultra-low latency (the delay between when data is sent from one device on a network and received by another).[307] 5G technologies are deployed in new ways compared to their predecessors: while previous generations used large cell towers to transmit signals, 5G can also use small cells (radio access points) that are about the size of a picnic cooler or mini fridge, creating greater cellular density and faster deployment.[308] 5G networks are also critical to enabling the proliferation of the Internet of Things (IoT) devices.[309] Such enhanced capabilities will not only reshape cellular communications and facilitate the development of emerging technologies, but will also fundamentally alter how industries and societies that rely on connectivity to data sources operate.[310]

While the spread of 5G technologies will provide many positive impacts for society and industry, China is pursuing avenues to manipulate the capabilities endowed by these new technologies. As noted earlier in the report, China has made significant inroads in the development and deployment of 5G. China's efforts, as a number of former military leaders elucidate in an April 3, 2019, letter, present "grave concerns" to the United States, our allies, and our partners.[311] The letter states that a widely adopted Chinese-developed 5G network "provide[s] near-persistent data transfer back to China," would mean U.S. reliance on Chinese technologies for critical military communications, and will "advance a pernicious high-tech authoritarianism."[312] These comments underscore that a 5G infrastructure built on Chinese technologies will promote digital authoritarianism around the globe, and consequently, why the United States must pursue mechanisms to mitigate China's influence in this digital sphere.

As 5G technology moves closer to global deployment, the U.S. has some technological disadvantages that have both commercial and security implications. The development of 5G networks will boost the rate of implementation for new and transformative technologies ranging from autonomous vehicles to smart cities to virtual reality.[313] There is much to gain from leading the

---

[307] Qualcomm, "Everything You Need to Know about 5G," https://www.qualcomm.com/invention/5g/what-is-5g (last visited May 13, 2020); Congressional Research Service, *Fifth Generation (5G) Telecommunications Technologies: Issues for Congress*, Jan. 30, 2019, at 1.

[308] "What is Small Cell Technology?," Verizon, Aug. 8, 2018, https://www.verizon.com/about/our-company/5g/what-small-cell-technology (last visited May 14, 2020); "Why 5G Can't Succeed Without a Small Cell Revolution," PwC, https://www.pwc.com/us/en/industry/tmt/assets/5g-small-cell-revolution.pdf (last visited May 13, 2020).

[309] Murali Venkatesh, "How 5G Networking Will Unleash the Full Potential of IoT," *Oracle*, Feb. 4, 2019, https://blogs.oracle.com/iot/how-5g-networking-will-unleash-the-full-potential-of-iot.

[310] Dan Patterson & Anisha Nandi, "5G explained: How it works, who it will impact, and when we'll have it," *CBS News*, Feb. 21, 2019; PwC, "Why 5G Can't Succeed Without a Small Cell Revolution," https://www.pwc.com/us/en/industry/tmt/assets/5g-small-cell-revolution.pdf (last visited May 13, 2020).

[311] Letter from Adm. James Stavridis et al., "Statement by Former U.S. Military Leaders," Apr. 3, 2019, https://www.lawfareblog.com/document-former-military-and-intelligence-officials-letter-5g-risks.

[312] *Id.*

[313] Randal Kenworthy, "The 5G and IoT Revolution is Coming: Here's What to Expect," *Forbes Technology Council*, Nov. 18, 2019.

pack in the global telecommunications race—and much to lose by lagging behind.[314]Although Europe dominated the development and implementation of 2G technologies, and Japan led on the deployment and adoption of 3G technologies, beginning in about 2016 the United States pulled ahead and led on the development and adoption of 4G.[315] Through a first-mover advantage provided by its innovation and implementation of 4G and LTE, and complemented by its competitive mobile device technologies, the United States was able to shape the global 4G ecosystem.[316] U.S. companies took advantage of the enhanced capabilities of the new network, developing devices, apps, and services that would dominate global markets.[317] This success led to a 70% growth of the U.S. telecommunications industry between 2011 and 2014, increasing industry jobs by 80% and boosting GDP.[318]

Yet whatever advantages the U.S. had in the innovation deployment of 4G and LTE networks are beginning to narrow in the new age of wireless development. A 2019 report by the Defense Innovation Board suggests that, due to several critical shortcomings in U.S. 5G development, it is unlikely the US will win the race to 5G.[319] A critical differentiator between 4G and 5G technologies is that 5G will leverage various segments of the electromagnetic spectrum: from the low to mid-band spectrum, or "sub-6", to the high-band spectrum, or "mmWave."[320] As the spectrum bands are the fundamental layers upon which the entire 5G network and infrastructure is built, the decision to develop technologies based on lower or higher frequencies is one of the most critical near-term choices for policy-makers and involves different levels of costs and investments.[321] For example, mmWave technologies are capable of faster and more secure data transmission, but require far greater infrastructure and monetary investments to set up, while the sub-6 band can cover broader areas with less risk of interruption and is able to "leverage existing 4G infrastructure."[322] Currently, the advantages of the sub-6 band, especially on costs and broad coverage, make it the most likely

---

[314] Statement of Peter Harrell, Center for a New American Security, *5G: National Security Concerns, Intellectual Property Issues, and the Impact on Competition and Innovation*, Hearing before the United States Senate Committee on the Judiciary, May 14, 2019, at 2, https://s3.amazonaws.com/files.cnas.org/documents/Harrell-Judiciary-Testimony-May-14-2019.pdf?mtime=20190515171307.

[315] Recon Analytics, *How America's Leading Position in 4G Propelled the Economy*, at 6 (Apr. 16, 2018), https://api.ctia.org/wp-content/uploads/2018/04/Recon-Analytics_How-Americas-4G-Leadership-Propelled-US-Economy_2018.pdf.

[316] Milo Medin & Gilman Louie, *The 5G Ecosystem: Risks and Opportunities for DoD*, Defense Innovation Board, at 6 (Apr. 2019).

[317] Statement of Peter Harrell, Center for a New American Security, *5G: National Security Concerns, Intellectual Property Issues, and the Impact on Competition and Innovation*, Hearing before the United States Senate Committee on the Judiciary, May 14, 2019, at 2, https://s3.amazonaws.com/files.cnas.org/documents/Harrell-Judiciary-Testimony-May-14-2019.pdf?mtime=20190515171307.

[318] Milo Medin & Gilman Louie, *The 5G Ecosystem: Risks and Opportunities for DoD*, Defense Innovation Board, at 7 (Apr. 2019); Recon Analytics, *How America's Leading Position in 4G Propelled the Economy*, at 6 (Apr. 16, 2018).

[319] Milo Medin & Gilman Louie, *The 5G Ecosystem: Risks and Opportunities for DoD*, Defense Innovation Board, at 7 (Apr. 2019).

[320] *Id.* at 8-11.

[321] Dave Andersen, "5G FAQ series: What's the difference between mmWave and sub-6 GHz spectrum?," *RootMetrics by IHS Markit*, Oct. 28, 2019, https://rootmetrics.com/en-GB/content/5g-faq-series-whats-the-difference-between-mmwave-and-sub-6-ghz-spectrum; Gabriel Brown, *White Paper: Exploring the Potential of mmWave for 5G Mobile Access,* Heavy Reading, at 3, 8, 10 (June 2016), https://www.qualcomm.com/media/documents/files/heavy-reading-whitepaper-exploring-the-potential-of-mmwave-for-5g-mobile-access.pdf.

[322] Milo Medin & Gilman Louie, *The 5G Ecosystem: Risks and Opportunities for DoD*, Defense Innovation Board, at 8, 10 (Apr. 2019).

near-term outcome for propagating a 5G ecosystem.[323] However, in the United States, portions of the sub-6 bands are owned by the government, somewhat limiting civilian and commercial use of that spectrum.[324]

The limits on spectrum have posed a number of problems to US near-term competitiveness in the 5G global ecosystem, not least of which is that Chinese companies have managed to outpace the U.S. in development and export of its 5G infrastructure. China has pursued infrastructure buildout based on the sub-6 spectrum band, and with its head start in the global deployment of its 5G infrastructure, has been able to attract a growing share of the global market with its promises of a high quality and low cost network.[325] Given the current higher costs and lower density of the mmWave spectrum range, many global players—including key U.S. allies and partners—have chosen to follow China's lead.[326] The consequences of China leading the buildout of the global 5G ecosystem are severe, and could include creating overseas security risks for Department of Defense operations and eroding competitive supply chains for the United States.[327] **It is critically important to note, however, that the United States could find a future advantage by leading on mmWave technologies, since 1) this band is the spectrum where ultra-fast innovations may arise and 2) a fully actualized 5G network will see devices seamlessly utilize and transition between both the sub-6 and mmWave bands.[328]**

Another reason the United States finds itself in greater competition with China on 5G deployment is that China has spent more on 5G development, implementing 198,000 5G-operable base stations domestically, with 500,000 more planned, and rapidly deploying 5G equipment and infrastructure around the world.[329] In Europe in particular, Huawei and ZTE have partnered with many countries to build their 5G networks despite US protests over security concerns, and Chinese-built network infrastructure continues to spread across the continent.[330] Within Congress and the Administration there is a bipartisan understanding of the threats posed by Chinese firms building the base layers of radio equipment and other telecommunications infrastructure upon which 5G operates. Unfortunately, there is a major gap in the United States government between rhetorical complaints

---

[323] *Id.*, at 10; Dave Andersen, "5G FAQ series: What's the difference between mmWave and sub-6 GHz spectrum?," *RootMetrics by IHS Markit*, Oct. 28, 2019, https://rootmetrics.com/en-GB/content/5g-faq-series-whats-the-difference-between-mmwave-and-sub-6-ghz-spectrum

[324] Milo Medin & Gilman Louie, *The 5G Ecosystem: Risks and Opportunities for DoD*, Defense Innovation Board, at 10 (Apr. 2019). It is important to note that while the government holds large portions of the sub-6GHz spectrum, there have been certain initiatives aimed at freeing up some of this spectrum, such as S. 19, the MOBILE Now Act introduced by Senators John Thune (R-ND) and Bill Nelson (D-FL) during the 115th Congress in 2018. *Id.*

[325] *Id.*, at 12, 21; Press Release, U.S. Department of Justice, "Attorney General William P. Barr Delivers the Keynote Address at the Department of Justice's China Initiative Conference," February 6, 2020.

[326] Milo Medin & Gilman Louie, *The 5G Ecosystem: Risks and Opportunities for DoD*, Defense Innovation Board, at 15 (Apr. 2019).

[327] *Id.* at 4.

[328] Monica Alleven, "SK Telecom, Ericsson demonstrate 5G connected BMW at 28 GHz," *Fierce Wireless*, Nov. 15, 2016, https://www.fiercewireless.com/tech/sk-telecom-ericsson-demonstrate-5g-connected-bmw-at-28-ghz; Bevin Fletcher, "New Samsung 5G phones can tap both sub-6 GHz and millimeter wave spectrum," *Fierce Wireless*, Feb. 12, 2020, https://www.fiercewireless.com/devices/new-samsung-5g-phones-can-tap-both-sub-6-ghz-and-millimeter-wave-spectrum.

[329] Jason Murdock, "China Planning 500,000 New 5G Base Stations as State Officials Say Construction Has 'Entered the Fast Lane'," *Newsweek*, Feb. 24, 2020; Milo Medin & Gilman Louie, *The 5G Ecosystem: Risks and Opportunities for DoD*, Defense Innovation Board, at 13 (Apr. 2019).

[330] Milo Medin & Gilman Louie, *The 5G Ecosystem: Risks and Opportunities for DoD*, Defense Innovation Board, at 13 (Apr. 2019).

about Chinese efforts to dominate the 5G domain and actual, tangible steps to counter China's government and industry on the issue.

Finally, the United States currently does not have a domestic 5G supplier for the equipment that makes up the Radio Access Network (RAN) for 5G.[331] Instead, countries seeking viable alternatives to Chinese 5G RAN infrastructure rely on companies such as Swedish company Ericsson, South Korea-based Samsung, or Finnish firm Nokia to build out core components of their layer of the 5G infrastructure.[332] While these companies do provide alternatives to Huawei, Chinese government subsidies to Huawei allow the company to sell products at far lower prices and offer low-cost financing, undercutting the competitiveness of other firms.[333] This combination of a lack of a U.S. domestic 5G alternative and China's monetary subsidies is leading to a 5G environment that lacks stable, secure U.S. infrastructure and products, and is increasingly problematic for U.S. security. To maintain U.S. security, it is therefore imperative that the United States find, develop, and pursue policies that open up pathways for United States industry to become a leading player in all facets of the 5G domain in the future.

[331] Tom Wheeler, "5G in Five (not so) Easy Pieces," *The Brookings Institution*, July 9, 2019; "What are Radio Access Networks and 5G RAN?," Verizon, Feb. 2, 2020, https://www.verizon.com/about/our-company/5g/5g-radio-access-networks (last accessed July 10, 2020).
[332] Tom Wheeler, "5G in Five (not so) Easy Pieces," *The Brookings Institution*, July 9, 2019.
[333] *Id.*