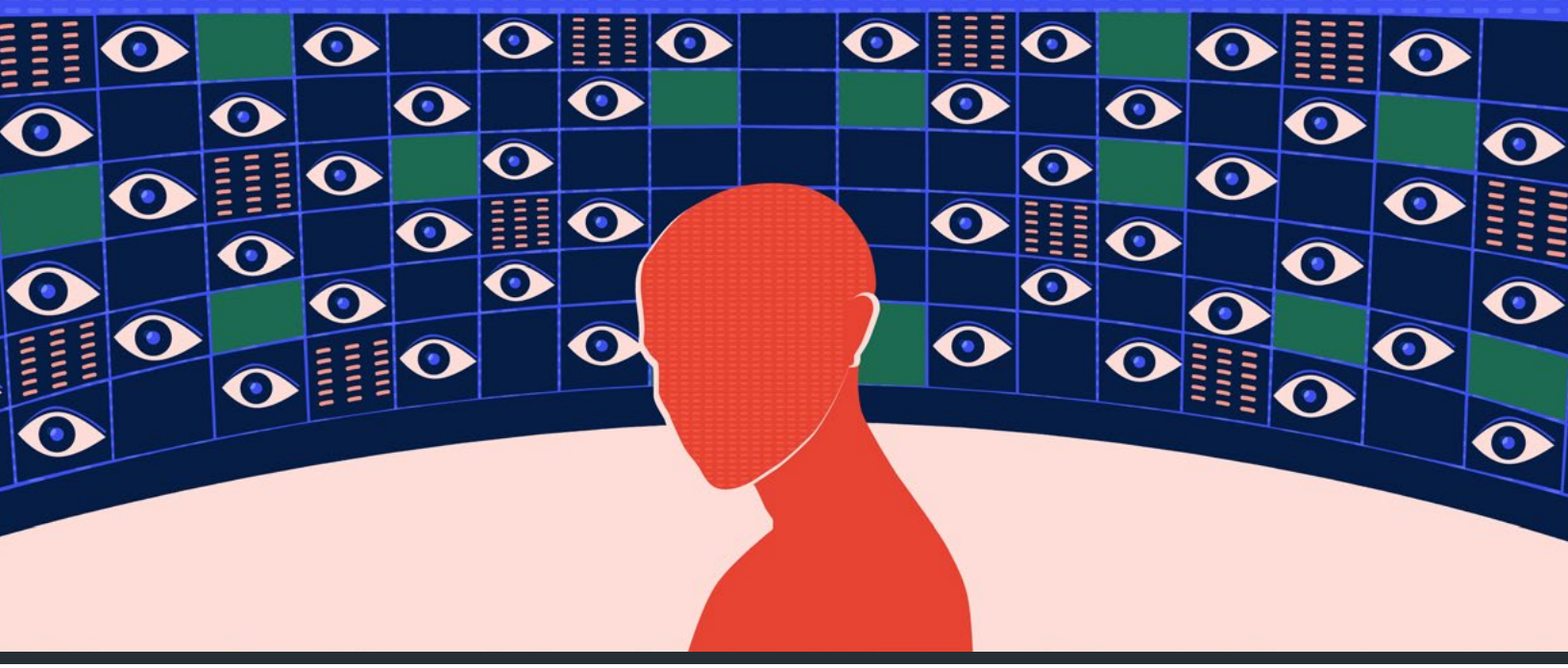
NOVEMBER 2021



The Future of the Digital Order

Jeff Cirillo, Lisa Curtis, Joshua Fitt, Kara Frederick, Coby Goldberg, Ilan Goldenberg, Andrea Kendall-Taylor, Megan Lamberth, Martijn Rasser, and Dania Torres

CNAS

About the Authors

Jeff Cirillo | Former Joseph S. Nye, Jr. Intern in the Transatlantic Security Program.

Lisa Curtis | Senior Fellow and Director of the Indo-Pacific Security Program.

Joshua Fitt | Associate Fellow in the Indo-Pacific Security Program.

Kara Frederick | Research Fellow in the Center for Technology Policy at the Heritage Foundation. Former Fellow in the Technology and National Security Program at CNAS.

Coby Goldberg | Former Joseph S. Nye, Jr. Intern in the Indo-Pacific Security Program.

Ilan Goldenberg | Senior Fellow and Director of the Middle East Security Program.

Dr. Andrea Kendall-Taylor | Senior Fellow and Director of the Transatlantic Security Program.

Megan Lamberth | Associate Fellow in the Technology and National Security Program.

Martijn Rasser | Senior Fellow and Director of the Technology and National Security Program.

Dania Torres | Former Joseph S. Nye, Jr. Intern in the Middle East Security Program and Communications Consulatant.

Acknowledgments

We want to thank members of CNAS' Digital Freedom Forum, including Alexandra Givens, Aynne Kokas, Alina Polyakova, and Kori Schake, whose insights helped shape the scope and analysis of this report. The Digital Freedom Forum is a bipartisan effort that brings together a diverse set of stakeholders to determine how the United States should respond to the illiberal use of technology abroad, while advancing the values of freedom and openness in the digital domain. The views expressed in this report are those of the authors alone and do not represent those of the forum or its members. The authors also thank CNAS Adjunct Senior Fellows Margarita Konaev and Samuel Bendett for their valuable input and feedback on parts of the report draft.

We thank our CNAS colleagues Maura McCarthy, Paul Scharre, Melody Cook, Rin Rothback, Emma Swislow, and Anna Pederson for their roles in the review, production, and design of this report. We also wish to acknowledge and thank Kristine Lee for her invaluable contributions to the report. Finally, we are grateful to Xiaojing (JJ) Zeng and Henry Wu for their valuable research support and assistance in reviewing and finalizing this work. Any errors that remain are the responsibility of the authors alone. This report was made possible with the generous support of the Quadrivium Foundation and general support to CNAS.

Cover Art: Melody Cook/CNAS

About the CNAS Countering High-Tech Illiberalism Project

Democracies and open societies are under assault by a new breed of high-tech illiberalism. The same digital technologies that connect people and enable a free exchange of ideas are being used to polarize and pervert the politics of democratic societies. As a result, digital technologies once touted as a democratic panacea are being subverted by authoritarians to deepen their grip internally, undermine basic human rights, spread illiberal practices beyond their borders, and erode public trust in open societies. In some instances, authoritarian regimes may even be able to harness advanced technologies to outperform democracies in certain key areas, weakening the case for political freedom in the emergent ideological competition of the 21st century.

This project, supported by a grant from the Quadrivium Foundation, aims to build a broad coalition of stakeholders in the United States and in allied and partner nations—including engineers, academics, technologists, current and former policymakers, and practitioners—to develop the policy and technology innovations necessary to secure a freer and more open future.

TABLE OF CONTENTS

Executive Summary

Nations that successfully harness the vast economic, political, and societal power of emerging information and communications technologies will shape the future of the global digital order. This future is not set in stone. A digital order defined by liberal democratic values requires U.S. leadership and the cooperation of trusted like-minded partners. In the absence of democratic leadership, autocratic rivals of the United States can fill that void—exploiting the control of information, surveillance technologies, and standards for technology governance to promote a digital ecosystem that entrenches and expands their authoritarian practices.

In exploring how a closed, illiberal order is taking root in strategic regions around the world, this report offers recommendations for how to craft, promote, and preserve a more open and democratic alternative. An assessment of crosscutting trends between China, Russia, and the Middle East across three pillars—information control, surveillance, and technology governance—leads us to the following conclusions:

- China is the prime mover in shaping the evolving digital order in its favor. Beijing's use of technologies such as facial recognition software and telecommunications networks allows the Chinese Communist Party (CCP) to expand control over its citizens. The CCP's ability to promote and export this model of digital repression, in turn, gives like-minded, nondemocratic governments a roadmap for how to deploy digital technologies for control and abuse in their own countries.
- Russia's model of digital authoritarianism, while technologically less sophisticated than China's, could prove to be more readily adaptable and enduring for current and aspiring autocrats. Regional powers such as Belarus, Azerbaijan, and some Central Asian states have already incorporated elements of this model.
- In the Middle East, authoritarian leaders use digital tools to control internal populations by sabotaging and spying on citizens, and this contributes to the construction of an illiberal digital order that is beneficial to America's peer competitors—China and Russia.

These conclusions reveal four key trends with implications for the future of the digital order:

- Growing China-Russia alignment will generate dangerous digital synergies, such as (1) making digital autocracy accessible for a broader swath of states; (2) accelerating China's and Russia's digital innovation; (3) eroding liberal norms in international institutions; and (4) raising the prospects of a "splinternet," a fragmenting of the internet along nationalistic, political, technological, religious, or ethnic lines.
- Countries around the world, particularly autocratic regimes and those flirting with illiberalism, will seek to regulate online communications platforms through (1) social media; (2) data localization laws; and (3) instigating company self-censorship, which restricts free speech and increases online control.
- Illiberal regimes will seek out Chinese technology to help them control social movements and civil protests. U.S. nondemocratic partners, adversaries, and even some democratic partners justify their pursuit of Chinese technology by underscoring ways the adopted technologies will contribute to economic growth, social stability, and efforts to fight crime and terrorism.
- The practices of illiberal regimes will reduce the efficacy of U.S. mitigation practices. Russia and China's efforts to promote an illiberal digital order complement one another and could accelerate innovation between the two nations.

The United States must craft a policy response that considers these emerging patterns and incorporates more than its usual partners in Europe and the Indo-Pacific. Shoring up the existing coalition of democratic actors to counter these illiberal trends will likely not be sufficient. This report offers recommendations that the United States can implement on three fronts: at home, while engaging with traditional U.S. democratic as well as nondemocratic partners, and when countering U.S. adversaries such as China, Russia, and Iran. The United States must take a leadership role, recognizing that the future digital order is at stake.

Summary of Recommendations

Effective policy responses must engage a range of actors to address intersecting regional trends and the implications of authoritarian attempts to reshape the digital order. This report offers recommendations to guide U.S. efforts to advance a more liberal democratic order by addressing data protection and data privacy at home, by working with the governments of other countries—both democratic and nondemocratic partners—and by challenging competitors. To implement these recommendations, coordination between legislative bodies, federal agencies, and White House officials will be instrumental.

At Home

The United States needs to put its own digital house in order to effectively shape and promote a liberal digital order around the world. A shortfall in regulatory oversight and a lack of national policies on digital matters is inhibiting America's ability to lead.

The United States should enact a national data protection and privacy law. Congress should:

- Establish a data protection framework that clearly articulates the U.S. approach to data privacy at home.

Relevant U.S. government entities should hold regular formal consultations with U.S. tech companies on the risks of doing business in countries with nondemocratic governments. The National Security Council, in conjunction with the Departments of State and Commerce, should:

- Initiate an ongoing dialogue between government officials and tech company executives on matters of digital freedom.

The U.S. government needs to prioritize research and development of privacy-preserving technology solutions. To this end, Congress and the White House would be well served to:

- Create incentives for novel research in technologies that preserve privacy of data, while also maintaining the use of techniques to extract value from datasets.

With Democratic Partners

The United States must work with like-minded democratic partners to ensure a digital order that preserves and promotes open societies, and to combat the illiberal use of emerging digital technologies.

The U.S. government needs to recruit and convene democratic allies—both bilaterally and multilaterally—to craft and execute a comprehensive framework to shape the future digital order. The White House should:

- Formalize the tech alliance concept of a global governing body of techno-democracies to coordinate policy with a broader pool of allies.
- Pursue bilateral and minilateral working groups with techno-democracies to coordinate policies and strategies pertaining to technology.
- Expand cooperation on digital initiatives in the Indo-Pacific with like-minded democratic partners, starting with the Quad countries.
- Work through the U.S.-EU Trade and Technology Council to develop a shared vision and approach to managing the human rights implications of technology.

The U.S. government must work in tandem with industry leadership in international standard-setting bodies to promote better alignment and coordination with like-minded countries within these bodies. To effect this, the White House and Congress ought to:

- Engage key partners to counter China's influence within international bodies that set standards for fundamental technologies.
- Provide financial support or incentives for U.S. firms to increase their representation on international bodies that depend on industry stakeholders.

The U.S. government should counsel key partners on best practices for investment screening and export controls. The White House and the Departments of State, Commerce, and Treasury should:

- Design and strengthen systems for screening technologies that are susceptible to abuse by authoritarians.
- Establish interagency processes to coordinate technology policy partnerships.
- Use the U.S.-EU Trade and Technology Council to share insights on specific companies and cases that need to be protected.

The United States should work with its democratic partners to incentivize and encourage middle income and developing countries to invest in trusted and secure technologies and technology infrastructure. To this end, we recommend that Congress and the White House:

- Provide financial support or incentives so that democratically aligned digital firms from allied and partner countries will provide trusted alternatives to Chinese digital investments.
- Establish a Digital Development Fund through the United States Agency for International Development (USAID) to collaborate with the International Development Finance Corporation (DFC).
- Develop assessment frameworks and standards to vet digital development projects with the State Department, USAID, and the DFC.
- Support democratic innovation bases that give incentives to diverse vendors and focus on developing secure and modular alternatives to China's Safe City and surveillance technology solutions.

The United States needs to boost multilateral engagement on governance and technical norms and standards as they pertain to emerging digital ecosystems. To effect this, the White House Office of Science and Technology Policy is advised to:

- Launch initiatives with allies in the Indo-Pacific to build out a shared set of norms on safe practices for the use of cutting-edge technologies, which can then undergird future proposals at international standards bodies.

U.S. government agencies should build local resilience among civil society and watchdog groups to combat foreign influence operations or other forms of illiberal technology use. The State Department should:

- Establish a standalone Digital Rights Fund to support civil society groups playing a watchdog role.
- Provide best-practices training to local media in countries such as Thailand, Myanmar, and Cambodia on how to counter Chinese and other disinformation campaigns, and empower civil society organizations in countries that are particularly vulnerable to digital influence operations.
- Develop an expanded Fulbright Scholars program for journalists from countries on the front line of Chinese influence campaigns.

With Nondemocratic Partners

The United States does not have the luxury of working only with like-minded, democratic allies. To provide a formidable counterweight to such antidemocratic competitors as China, Russia, and Iran, it must emphasize digital freedom concerns in bilateral relations with other nondemocratic partners.

U.S. agencies should regulate U.S. entities or persons' participation in and support of the illiberal use of technology in overseas markets. The Commerce and State Departments must:

- Provide explicit guidance to U.S. companies operating in the markets of nondemocratic partners, and take measures to prohibit U.S. companies from entering joint ventures with Chinese companies in areas that could have negative implications for digital freedom, such as smart cities.
- Take measures to establish a noncompete regulation to prevent former cybersecurity experts and officials trained or previously employed by the U.S. government from working for foreign governments.

Countering U.S. Competitors

The United States must leverage its powerful economic tools to counter competitors' illiberal technology use. Together with its allies and partners, the United States should work to effectively combat tech-enabled human rights abuses and other repressive policies.

The United States is advised to harness sanctions, advisories, and export control measures to impose costs on the repressive practices of illiberal governments. The White House should:

- Consider additional Magnitsky Act sanctions and Leahy law restrictions—in concert with the Commerce Department's Entity List—if companies are found to be complicit in tech-enabled human rights abuses.
- Coordinate with the Commerce and Treasury Departments to sanction illiberal governments' digital economies, including cybersecurity firms, in cases of their use of technology for repressive or disruptive purposes. This will signal that regimes must be responsible actors to participate in the global ecosystem.

Relevant U.S. agencies must focus on protecting areas of comparative strength vis-à-vis nation-state adversaries. To this end, the U.S. Commerce Department is advised to:

- Assess relative costs and benefits of export controls on artificial intelligence (AI) chips, which can encourage import substitution, versus targeted end-use/end-user controls on chips and on the semiconductor manufacturing equipment that is used to make the chips.[1]

Introduction: Pillars of the Digital Order

Challengers to liberal democracy seek to shape the digital order in ways that conform with their objectives and interests. This represents a direct challenge to the values, ideals, and priorities of the United States and its democratic allies. Autocratic regimes have exploited the digital environment to foster internal control and expand their external influence—both of which are integral to maintaining their hold on power. Illiberal actors use tactics in three pillars to shape the digital order in their favor: information control, surveillance, and technology governance. In practice, a government's weaponization of the digital order includes manipulating the availability and messaging of information; digital monitoring; and setting and exporting rules, norms, and policies that advance closed systems. The intent behind this weaponization is to enhance internal stability by muffling resistance, disrupting opponents, and advancing national interests globally.

The case for an open digital order rests on the fundamental principles of free societies—commitments to liberal democratic values, the rule of law, and respect for and promotion of human rights. An open digital order is the only way to ensure the trust and integrity of technological ecosystems, inclusive growth and shared prosperity, and innovation imbued with universal rights. Authoritarian uses of technology threaten the strength and resilience of democratic values and institutions.

Information Control

The shaping, storing, manipulation, and distribution of digital information is a foundational application of power in modern society. Repressive regimes exploit that power with tactics such as state-linked influence operations that disseminate targeted content; national, centralized databases; and internet and data sovereignty. States including China, Russia, and Iran, as well as several U.S. partners such as Saudi Arabia and the United Arab Emirates, conduct censorship on media platforms to restrict access to information that potentially is unfavorable to them. The creation of official, national data architectures and centralized databases is another method to entrench government control over and access to personal data. The push for internet and data sovereignty in Russia, China, and Iran in particular offers examples of how user data, access, and information can be controlled with bifurcated internet initiatives and intermittent internet shutdowns that are designed to restrict information access at political inflection points such as elections and protests.

Repressive governments can employ these tactics in combination with behavior-shaping technologies that embed less visible methods of control, including algorithms that dispense favorable information about the regime, while filtering out derogatory commentary. Access to information is much less restricted in democratic nations, but governments still seek to control their information environments, albeit to a lesser extent than in autocracies.[2] Information control in democratic contexts can be seen in "content moderation" strategies—social media companies' policies toward regulating speech on their platforms, for example—which elicit a range of support and criticism from policymakers and the public. Information control can also be exhibited in government-held databases owned by large federal agencies, with varying degrees of interoperability between systems.

Surveillance

Democracies and repressive regimes alike use surveillance technologies to counter crime, monitor crowds, and streamline traffic. Illiberal regimes often go further, employing their surveillance nets to monitor and control entire populations and to collect data on citizens and visitors alike. Such surveillance is possible with widespread deployments of cameras and video systems. China leads the world in the number of surveillance cameras in use, followed closely by the United States, India, and Brazil.[3] Building on basic surveillance techniques, new technologies such as facial recognition systems and biometric data collection platforms (e.g., voice or gait recognition technology) enable authorities to keep track of citizens and to collect, organize, and analyze information on their life patterns. New processing capabilities to parse the data and generate assessments enable predictive analytics that can be used to preemptively detain people. Smart city initiatives may eventually combine all these developments into regional panopticons that monitor citizens at scale.

Technology Governance

Authoritarian regimes wield governance as a weapon in their fight to exert influence over the digital order. Norms, values, and principles are critical to preserving the democratic use of technology. However, several authoritarian governments are pushing technology standards—which influence the way technology is used across the globe—that are infused with values that reject democratic imperatives of openness and transparency. Closed societies are increasingly implementing practices that favor their material and ideological interests in these

interactions. Furthermore, the collection, storage, and sharing of data, concerns over data privacy and illicit transfer (e.g., forced data transfer between private companies), and new modes of data exploitation will influence the digital order in fundamental ways. Data vulnerabilities stand to determine winners and losers in armed conflict, the integrity of intelligence tradecraft, the efficacy of military and intelligence operations, and other national security imperatives. Finally, export controls can also affect the transmission of technologies between states by slowing or preventing the adoption of specific tools.

This report examines these pillars and trends in three regions relevant to U.S. national security interests: China, Russia, and the Middle East. It then provides recommendations for how the U.S. government should address the challenges that digital authoritarianism poses across the world.

China

China is a prime mover in exploiting the evolving digital order. Using key digital technologies, Beijing has made repression and social control mechanisms more scalable and effective. Pervasive online censorship, ubiquitous cameras coupled with facial recognition software, and social credit systems designed to shape citizens' behavior have enhanced the Chinese Communist Party's (CCP) ability to control information and conduct surveillance of the population.

As Beijing enhances its capacity for surveillance at home, it is also marketing digital technologies abroad. Digital infrastructure projects, under the guise of China's Digital Silk Road, offer relatively low-cost alternatives to splashy and expensive physical infrastructure development.[4] In Pakistan, for example, where traditional infrastructure projects have experienced massive delays, Huawei built an 820-kilometer fiber-optic cable over two years for only $44 million—as much as it would cost to build four kilometers of railway.[5] Chinese technology companies, meanwhile, see massive profit opportunities in foreign markets, in addition to sources of more diverse data pools that can enable them to further improve their technological offerings.

China's export of digital infrastructure is integral to the expansion of the CCP's influence over norms, governance, and public security models globally as it seeks to make the world safe for autocracy.[6] The Chinese government has helped train police departments in dozens of countries on how to harness Chinese technologies toward illiberal ends, and it has provided foreign governments across the Indo-Pacific region the tools to codify illiberal digital norms in domestic law.[7] China is also exporting the notion that an open internet is not a prerequisite for accruing the economic benefits of connectivity, and indeed could even serve as a hindrance to growth.

Pushing these illiberal norms abroad bolsters Beijing's efforts to subvert international standard-setting bodies. These bodies, such as the International Telecommunication Union (ITU), exist to promote standards that protect freedom of communication and access to information, in addition to other democratic norms around the use of technology. China has been leading a campaign within multilateral fora to block resolutions that do not align with Beijing's vision of technology as a tool to expand authoritarian control.

Beijing is not exporting these technologies and associated norms into a vacuum. As autocratic governments and leaders in fragile democracies look to exert greater control over their populations and pursue inexpensive pathways toward digital development, they find Beijing's high-tech illiberalism an attractive model. They thus deliberately seek China's technology, funding, and know-how. Considering these trends, the Indo-Pacific has registered a democratic decline during the past decade, as some governments have moved toward a more statist vision of the internet predicated on government censorship and content curation.[8]

China's export of digital infrastructure is integral to the expansion of the CCP's influence over norms, governance, and public security models globally as it seeks to make the world safe for autocracy.

Although Beijing's activities are only one factor contributing to this outcome, China is well positioned to set a large portion of the region on a less free and open trajectory. The following sections examine three primary vectors by which Beijing seeks to bend the region toward a more illiberal digital future: information control, surveillance, and technology governance and standards.

Information Control

Over the past two decades, the CCP has not only sought to preclude the use of technology as a conduit of freedom and open information, but has gained an unprecedented ability to apply cutting-edge technologies toward illiberal ends. These capabilities first manifested in the CCP's control of the web, but its levers have grown far more sophisticated and far-reaching.

With the introduction of the Great Firewall in the early 2000s, China asserted sovereign control over cyberspace, a domain previously assumed to be beyond the grasp of 20th-century authoritarian governance.[9] Chinese internet users could no longer access many parts of cyberspace that were open to the rest of the world, and companies refusing to comply with Chinese content restrictions were penalized. In its early days, the Great Firewall enabled censors to take down only a few blatantly anti-CCP websites and posts, and internet users circumvented tightening control with clever homonyms and coded language. Gradually, however, sanitized yet attractive alternatives to foreign websites proliferated—to the point where many internet users stopped trying to "jump the Great Firewall," even as censors grew more sophisticated in using emerging artificial intelligence (AI) tools to scrub websites clean of any offending posts.[10] For those who continued to post content deemed problematic, the CCP in 2015 created an internet police force with the power to question and arrest people for online speech violations. Some provinces aim to establish one internet police officer for every 10,000 citizens.[11]

The CCP's content controls have also migrated to communications conducted over popular social media platforms and applications.[12] During the protracted 2019 democracy struggle in Hong Kong, the CCP's censorship machinery operated at full throttle as Tencent—WeChat's parent company—suspended the accounts of users who criticized Beijing, including those located in the United States.[13] There are similar censorship concerns regarding TikTok, which has gained broad reach in the United States.[14] As Chinese platforms proliferate beyond the nation's borders, the CCP is positioned to quietly export its model of censorship and content suppression across the region.

Beijing leverages access to China's lucrative domestic market to influence the actions of Western technology companies in order to shape the global online information environment. China has also used the threat of blacklisting to make U.S. companies complicit in censorship. In June 2020, for example, the American video conferencing platform Zoom admitted that, at the request of the Chinese government, it had taken down user accounts based outside of China that had engaged in planning for June 4 Tiananmen Square massacre commemorations.[15] In 2019, Apple Inc. also buckled under pressure from the Chinese government. After a Chinese state-owned newspaper criticized the U.S. technology giant for allowing HKmap.live on its platform—which helped Hong Kong protesters track police movements—Apple removed the app from its online store.[16] During the same period, it also removed the Taiwanese flag emoji from iPhones in Hong Kong and Macau.[17]

Beijing has long viewed control over ideas as a core tenet of China's national power. While keeping a tight lid on its domestic cyberspace, Beijing's concerted effort to expand state media capacity, increase the market share of Chinese social media platforms, and cultivate opaque partnerships with local media companies has enabled the CCP to amplify state propaganda beyond its borders.[18]

Dating back to the late 2000s under Hu Jintao, the CCP's Central Propaganda Department sharpened its focus on the global "competition for news and public opinion" and "the contest over discourse power" through the "innovation of news propaganda."[19] Shortly after becoming the General Secretary of the CCP, Xi Jinping reiterated at the August 2013 National Meeting on Propaganda and Ideology that China needed to "strengthen media coverage . . . use innovative outreach methods . . . tell a good Chinese story, and promote China's views internationally."[20] A 2013 meeting of the Central Propaganda Department reiterated that shaping online public opinion was an area of "highest priority" for the party.[21]

Beijing has harnessed its global technology internet companies, including Alibaba, Tencent, Baidu, and Huawei, to mold public opinion and peddle its desired narratives.[22] Those at China's periphery have absorbed the brunt of the CCP's tech-enabled propaganda. For example, its "50-cent army" of government-paid commentators and bots flooded Taiwan's social media sphere in the lead-up to its 2018 local election, and operated at full throttle during the 2019 pro-democracy protests in Hong Kong to advance narratives that favored China and undermine the credibility of dissidents.[23]

In addition to eliminating dissident voices and promoting nationalistic content on domestic social media platforms such as WeChat and Douyin, Beijing has also strong-armed overseas diaspora news outlets. If these small ventures report on stories that run counter to the CCP's narrative, it has threatened to cut off ad revenue.[24] Through this tactic, Beijing can still exert control over non-state media in countries that enjoy freedom of the press.[25]

Surveillance

The CCP's techno-authoritarian controls not only govern China's internet but have taken hold in the offline world. China has a vast system of an estimated 415 million surveillance cameras across its provinces.[26] Of the 20 cities in the world with the highest ratio of surveillance cameras to people, 18 are in China.[27] The proliferation of surveillance cameras has yielded vast quantities of information about citizens' lives offline—where they go, what they say, and whom they see—that previously stood beyond the reach of authoritarian control.

New advances in AI-enabled facial recognition, voice recognition, and predictive policing technologies are necessary to turn into an effective means of control the massive amount of information produced by China's vast surveillance web. This is precisely the aim of China's new smart city technologies.

China's smart city systems and AI development are not merely tools of surveillance. They often bring material gains to governments, companies, and people. Notably, the Chinese company with the most AI-based patents is a state-owned electric utility monopoly, the State Grid Corporation of China, which uses AI to optimize grid management.[28] China's New Generation AI Development Plan, the central government policy that aims to ensure China becomes the global leader in AI research by 2030, encourages local governments to use smart city technologies for solving a range of problems—from bureaucratic accountability to transportation efficiency—and to support local companies that make use of AI in new technologies.[29]

A plurality of China's top 100 AI firms specialize in security. These companies harness technology to make repression and social control mechanisms more scalable and effective.[30] Since 2005, the Ministry of Public Security has rolled out two massive surveillance projects across the country: Skynet and Sharp Eyes. (Skynet, which references a Chinese idiom about the Net of Heaven that catches all wrongdoing, is not to be confused with the dystopian artificial intelligence from the movie *The Terminator*.)[31] Xinjiang has emerged as a testbed for Chinese companies' latest surveillance technology. In essence, Beijing has coupled 21st-century innovation with 20th century–style mass detention camps to repress the region's Uyghur population.[32]

As private companies have sprouted up to meet widespread government demand for surveillance systems, they have used the profits from their contracts and the

SenseTime, the world's highest-valued artificial intelligence company, is working closely with the Chinese government to build AI technologies that support China's facial recognition ambitions. Here, SenseTime executive Leo Gang Liu (left) speaks at the CNBC East Tech West conference in 2018. (Dave Zhong/Getty Images for CNBC International)

data collected through these systems to further hone their technologies. Two surveillance camera makers, Hikvision and Dahua, control more than 50 percent of the Chinese market for surveillance hardware.[33] Four unicorn startups, known as the AI four little dragons, specialize in facial recognition technology: SenseTime (or Shangtang, with a valuation of $12 billion in 2021, the world's most valuable AI startup), Megvii, Cloudwalk (or Yuncong), and Yitu.[34] China's most successful provider of voice recognition technology, iFLYTEK, makes 60 percent of its profits from government contracts.[35] Ultimately, China hopes to develop AI-driven predictive policing to the point where criminal patterns can be detected before crimes are committed, a lofty ambition dubbed by German scholar Sebastian Heilmann as "digital Leninism."[36]

As China introduces smart city technology to countries around the world, it has proposed health technology to scan body temperature. Following the outbreak of COVID-19, China implemented health technology, as shown in this photo, to scan body temperatures to identify possible COVID-19 cases. (Getty Images)

Technology Governance

China is exporting its digital norms and practices to governments that seek to suppress social movements and civil protest. The CCP's goal is to make the world safer for authoritarianism and create information environments that facilitate the market penetration of its technology companies. It is also increasingly using international bodies to legitimize these digital norms and standards.

China trains officials from countries around the world in methods of illiberal digital governance. In 2018, the Chinese government organized training sessions with representatives from more than 30 countries on media and information management.[37] Private companies help, too. Meiya Pico, the digital forensics company that was named in a data privacy scandal by the former Trump administration, has provided training courses for police forces across 30 countries.[38]

The Chinese government has sought to build new regulatory systems in its own image in countries that have deep economic interdependencies with China, particularly in Southeast Asia. The China Academy for Information and Communications Technology (CAICT), a state-sponsored think tank, argued in a 2019 report on cybersecurity policy in Southeast Asia that "China should leverage its influence in [Association of Southeast Asian Nations] member states to integrate ASEAN's cybersecurity action plans with its own development strategy."[39] Chinese companies have also, in some cases, helped governments write laws and development plans that directly benefit the companies. For example, Huawei drafted the Lao National ICT (information and communications technologies) Development Plan white paper for that country's Ministry of Post and Telecommunications.[40] Elsewhere, China has provided a model for illiberal digital governance without directly writing the rules. Vietnam introduced Chinese-style data localization rules in 2018; Cambodia, the Philippines, Singapore, and Thailand have all implemented laws that bring a heavy hand to regulating online speech.[41]

China has endeavored to strategically take control of standard-setting bodies. In the Chinese government's first-ever white paper on international cyberspace cooperation, jointly published by the Ministry of Foreign Affairs and the Ministry of Public Security in March 2017, the CCP committed to leading the "institutional reform of the U.N. Internet Governance Forum" by positioning China to play a larger role in shaping the global future of internet governance.[42] China is mobilizing illiberal actors in multilateral forums to control, modify, and dilute resolutions coming out of international organizations and standard-setting bodies, which are supposed to be protecting freedom of expression and other liberal democratic norms around the use of technology.

This has played out most notably in the ITU, the United Nations' ICT standard-setting body, led by former Chinese Ministry of Posts and Telecommunications official Zhao Houlin.[43] Since Zhao's ascension as secretary-general in 2014, the ITU has increasingly cooperated with and promoted the Chinese companies and technical standards that undergird Beijing's oppressive surveillance state. Notably, the ITU has spoken positively about China's attempts to monopolize future communications infrastructure in countries under the umbrella of the Digital Silk Road, which could threaten the freedom and openness of the internet. More recently, Huawei has tried to advance its new internet protocol initiative at the ITU, a framework that would give governments an easy means of shutting down websites.[44] To control the standard-setting process more effectively in international bodies, including the 3rd Generation Partnership Project (3GPP), which is responsible for setting global mobile data standards, China pressures its companies to vote in unison. In 2018, the chairman of Lenovo was forced to offer a public apology for being "unpatriotic" after it was discovered his company had backed a technologically superior American 3GPP proposal over one made by Huawei in 2016.[45]

Chinese companies have also, in some cases, helped governments write laws and development plans that directly benefit the companies.

China's politicization of the standard-setting process is most dangerous when it comes to surveillance technologies. At the ITU, companies such as ZTE and Dahua submit standards modeled on their own in-house technologies for facial recognition and urban video monitoring devices, cementing commercial advantages for models that lack privacy protections. These standards are often directly adopted as domestic law by countries that do not have the capacity to develop regulations independently of international bodies.[46] In the field of AI, China has seized the advantage; for example, in Subcommittee 42, the body of the International Organization for Standardization and the International Electrotechnical Commission that is tasked with drafting AI standards, China succeeded in electing Huawei employee Wael Diab as chairman. The committee held its inaugural meeting in Beijing in 2018.[47]

Finally, China has directed its coalition-building efforts beyond the confines of long-established international standards bodies and sought to construct alternative institutions. Leveraging support and assuming legitimacy from other illiberal regimes that share its policy preferences, Beijing has strategically positioned itself as a champion of developing states and geared its actions toward rectifying the imbalances of Western-dominated international bodies.[48] In particular, Beijing has sought to enhance standards cooperation and digital integration with members of its signature Belt and Road Initiative.

In 2019, the Standardization Administration of China (SAC) created a "national standards information platform" among the Belt and Road partner countries "to strengthen the exchange and sharing of standards information."[49] In 2020, the SAC announced 85 standardization agreements with 49 countries and regions.[50] As China increasingly pursues standard-setting work outside of the United Nations, the SAC has officially dropped its former stated goal of integrating technology standards with the European Union and United States.[51] The annual World Internet Conference (WIC) in Zhejiang, which excludes the United States and Europe, has emerged as a platform for furthering this agenda. At the WIC, China brings together representatives from a range of Belt and Road countries to discuss cyber sovereignty and the dominance of large U.S. tech platforms.[52]

Beijing is poised to advance its vast surveillance apparatus abroad under the guise of its Digital Silk Road, leveraging the political and economic inroads it has made through its Belt and Road Initiative to build China-centric coalitions through its digital infrastructure. An authoritative party journal article in 2017 discussed the centrality of the "global influence of internet companies" to China's strategy for emerging as a "cyber superpower."[53] As Chinese technology companies are encouraged to chuhai (take to the sea) and penetrate foreign markets, they have emerged as major players across the Indo-Pacific region in fields including telecommunications equipment, data centers, and urban public security networks.

Beijing is not exporting these technologies into a vacuum. Autocratic governments and leaders in fragile democracies seek to emulate China's high-tech illiberalism as they exert greater control over their populations and pursue inexpensive pathways toward digital development. For example, during Xi Jinping's state visit to the Philippines in November 2018, President Rodrigo Duterte signed 29 agreements, including a Safe Philippines Project that contracted with Huawei and the China International Telecommunication and Construction Corporation

TECHNOLOGIES UNDER THE DIGITAL SILK ROAD UMBRELLA[54]

Safe Cities. One of China's most successful exporters of surveillance infrastructure has been Huawei, the telecommunications giant with ties to the Chinese government. Huawei is partnering with local authorities on what it has branded as Safe Cities—a platform of comprehensive urban management and surveillance.[55] In some Chinese cities, the platform has become fully integrated with local police databases that enable authorities to track residents' travel and social patterns, using information gathered by the technology to identify whether individuals are predisposed to commit crimes.[56]

As of 2018, 230 cities across 90 countries had contracted with Huawei for Safe City projects.[57] The Export-Import Bank of China subsidizes these projects, making them cost-efficient for third-party governments.[58] "Joint construction of smart cities is a good opportunity for expanding international markets and promoting the importance of the cybersecurity industry," CAICT argued in a 2019 report.[59] Achieving the vision for smart cities is a work in progress. As one Thai technology expert said, "The idea of a smart city is a joke. … [A] smart city in Phuket turns out to be providing free Wi-Fi and internet to tourists!"[60] But even if the exported version of this technology does not immediately reach the level of sophistication and effectiveness found in planning documents, privacy and freedom will pay a toll along the "New Digital Silk Road."

Facial recognition software. At least three of China's AI four little dragons are helping foreign governments adopt facial recognition technology. As these companies go abroad, they send valuable data back to China to hone their algorithms, while helping foreign autocrats build out their surveillance infrastructure. Cloudwalk signed a deal with Zimbabwe's government to provide facial recognition technology.[61] Yitu provides the technology for cameras used by the Malaysian police, and it bid for a project to embed facial recognition technology in all of Singapore's lampposts.[62] Megvii has supplied upward of 500 such systems across at least 11 countries in Southeast Asia, South Asia, and the Middle East. Yitu, Megvii, and the fourth AI dragon, SenseTime, were added to the U.S. Department of Commerce's Entity List in 2019 for their role in enabling Beijing's repression of ethnic minorities in Xinjiang.[63] Cloudwalk was subsequently added in 2020.[64]

Networks and 5G infrastructure. China seeks to dominate the Indo-Pacific's 5G infrastructure. It is also making an aggressive push to gain greater control of global data flows through the construction of terrestrial and undersea fiber-optic cables that will undergird future 5G networks.[65] Undersea cables across the world carry 99 percent of global data flows.[66] Huawei Marine Systems alone has worked on nearly 100 such projects.[67] If Huawei, or another Chinese company, builds an undersea cable, it can easily build back doors through which to monitor data flows through the cable.[68]

Health care technology. Chinese companies are racing to meet pandemic-specific health care needs that cast China in the savior role. Five Chinese companies—Hikvision, Dahua, Sunell, TVT, and YCX—have emerged alongside one U.S. competitor—Teledyne FLIR—as the largest suppliers of the global market for thermal imaging, which is used for monitoring human temperatures at a distance.[69] Alibaba is trying to market its cloud services for pandemic modeling and telehealth systems.[70] Not only does the export of health-care technology provide Chinese companies access to large pools of foreign data, it also can serve as a surveillance Trojan horse for China. Hikvision and Dahua, for example, have secured contracts for their thermal vision cameras, thermal detection–enabled metal detectors, and even thermal-screening mobile apps, including in U.S. states and cities, despite the fact that these companies are on U.S. federal sanctions lists because of their roles in Xinjiang. Turning the crisis into an opportunity, the CCP seeks to further embed its companies in markets that, in less panicked times, might forgo relying on sanctioned companies.

to construct a 12,000-camera surveillance system across metropolitan Manila and other cities.[71] In 2017, Malaysia partnered with Alibaba to launch a Digital Free Trade Zone, despite concerns that the Belt and Road–sponsored project would allow Chinese companies to monopolize the Malaysian markets.[72] Two years later and under new political leadership, Malaysia deepened the digital relationship, signing five memorandums of understanding on technology cooperation.[73]

As China's national technology champions go abroad to construct the Digital Silk Road, Beijing's bid to set international technology standards and establish new platforms for online connectivity has gained momentum far beyond the Indo-Pacific region. Perhaps nowhere has it been more successful than in Africa.

China's digital governance work in Africa began in Tanzania, where, in 2015, Beijing was selected to pilot a China-Africa capacity-building program.[74] With technical assistance from the Chinese government, Tanzania enacted a cyber-crime law and a content creation–licensing system forcing bloggers and Facebook users to pay $900 for a three-year license.[75] Uganda and Zambia mimicked Tanzania's tax on online content creators and users of such platforms as WhatsApp, Skype, and Viber.[76] "Our Chinese friends have managed to block such media in their country and replaced them with their homegrown sites that are safe, constructive, and popular," Tanzania's deputy minister for transport and communications admiringly told counterparts at a Chinese-organized roundtable in Dar es Salaam.[77]

Without direct guidance from such capacity-building programs and roundtables, countries that lack the domestic capacity to build regulatory frameworks often adopt as domestic law the international standards set by Chinese companies at U.N. bodies such as the ITU. "African states tend to go along with what is being put forward by China and the ITU as they don't have the resources to develop standards themselves," observed legal department head Richard Wingfield of Global Partners Digital in an interview with *The Financial Times*.[78]

This amounts to a broad shift in emerging markets, making the internet in those places more closely resemble

China's. As one African politician told researchers from the University of Witwatersrand in South Africa, "If China could become a world power without a free internet, why do African countries need a free internet?"[79] A 2019 report by the Collaboration on International ICT Policy for East and Southern Africa warns:

> The autocratic Chinese model appears to be gaining acceptance in the continent. It comprises widespread and sophisticated automated surveillance, online content manipulation, arrests of critics, content removal, data collection, repressive laws to censor online media, violence against digital activists, technical attacks against dissidents, the great firewall blocking foreign social media, websites and messaging apps, revocation of mobile and internet connectivity.[80]

Given the Chinese regime's focus on security and stability, the CCP is likely to continue evolving its model of digital repression—exploiting and harnessing the power of digital technologies to further its control over the population. The government's use of surveillance tools and information control mechanisms serves as an illustrative example to other like-minded, aspiring digital authoritarians, charting the course for how to exploit and abuse these technologies for power and repression.

Russia

Although China is leading the charge, it is not the only country offering a vision and endorsement of digital autocracy. Whereas Beijing's pervasive system of surveillance integrates vast amounts of data to aid in citizen control, Russia's model of digital authoritarianism, albeit less technologically sophisticated, could prove to be more readily adaptable and enduring.[81] Many autocracies more closely resemble Russia than China in that they did not build censorship into their systems from the start and lack the resources and, often, the capacity to filter data and block content, as does Beijing. Likewise, many regimes prefer to uphold at least a veneer of democracy and prefer less overtly repressive approaches to digital control, potentially increasing the appeal of the Kremlin's model. Although much attention has been devoted to Russia's use of disinformation, there is less understanding of the actions Moscow is taking to support digital authoritarianism more broadly.

Moscow is focused on establishing Russia as a leader in technology and the digital economy.[82] In 2017, President Vladimir Putin famously stated, "Artificial intelligence is the future, not only for Russia, but for all humankind. . . . Whoever becomes the leader in this sphere will become the ruler of the world."[83] In recent years, the Kremlin has launched a growing number of government-sponsored projects intended to facilitate technological innovation and the development of Russia's digital economy. Putin likely views such efforts as critical for generating investment, economic growth, and global prestige in a rapidly digitalizing world. While there are constraints on Russia's ability to fulfill its technological ambitions—brain drain and a business environment that still struggles to attract and develop private investment in the technology sector, for example—the Kremlin will remain a relevant actor with the potential to influence the trajectory of the future digital order.

As the Kremlin pursues its technological development, it is also aware of the risks that digital technologies pose to regime stability and is taking steps to mitigate those risks. As Putin noted in the same 2017 speech, "[AI] comes with colossal opportunities, but also threats that are difficult to predict."[84] Putin's statement and broader actions suggest that he sees emerging technologies as posing at least three key challenges to Russian sovereignty and the regime's hold on power. First, one of the Kremlin's biggest concerns is that Russia's current dependence on Western ICT creates a vulnerability that NATO and the United States in particular could exploit in a time of conflict.[85] Moscow has explained its moves to create a sovereign Russian internet, for example, as a defensive action allowing for the uninterrupted functioning of the internet in Russia in the event of a major foreign policy crisis (typically defined as a U.S. effort to disconnect Russia from the global internet).[86] Indeed, Russian military doctrine identifies information as playing an increasingly central role in modern conflict—a vector that outside actors could use to threaten Russian sovereignty and national interests.

Second, Moscow sees ICT as a conduit for external enemies to spread "alien" values inside Russia to destabilize the country. Putin has gone to considerable lengths to establish a narrative of Russia as a "separate civilization."[87] These efforts stem from Russian discontent over U.S. efforts to promote the universality of its values in the aftermath of the Cold War. Instead, Putin and those around him have sought to establish a culturally distinct system of Russian values defined by "an authentic concept of spiritual freedom inspired by Eastern Christianity and the idea of a strong, socially protective state capable of defending its own subjects from abuses at home and threats from abroad."[88] Putin has called the

internet a "CIA project,"[89] and his brand of digital autocracy is in part designed to protect, from external threats, his notion of Russia as a separate civilization—including the influence of what the Kremlin portrays as the "decadence" of Western values.

Finally, the Kremlin is acutely aware of the way that citizens across the globe have used digital technologies to aid their efforts to challenge and in some cases overthrow governments. Kremlin fears of technology-fueled revolutions, combined with mounting domestic challenges, have led the government to increase repression. The trend toward greater reliance on control began after Putin returned to the presidency in 2012, and it has accelerated in recent years with a rash of new oppressive legislation that the regime weaponizes to silence regime critics and weaken civil society. Many of the longtime drivers of Putin's support—economic growth, patronage, and more recently public support for returning Russia to the global stage—have run their course. The Russian economy has slowed, COVID-19 remains a challenge, corruption is prevalent, and public euphoria over the annexation of Crimea in 2014 has long faded. The

After the detention of Russian opposition leader Alexei Navalny, people gathered in January 2021 in Pushkin in Moscow, to protest against Vladimir Putin's government. After images and posts in support of Navalny were shared on social media, the Russian government attempted to throttle access to Twitter. (Getty Images)

protests that accompanied Russian opposition leader Alexei Navalny's arrest in January 2021—protests the Kremlin saw as being fueled by TikTok and Twitter—solidified views of social media as a threat. The Kremlin's domestic challenges, which will likely persist in the aftermath of COVID-19, will accelerate its efforts to restrict the internet and social media and weaponize digital technologies to upgrade and enhance control tactics and better ensure the survivability of the regime.

Moreover, the Kremlin is no longer content to simply counter perceived threats within Russia's borders. Instead, Moscow views the information environment as a critical battlespace in its competition with the West. Since 2014 Moscow has gone on the offensive, taking the fight to liberal democracies, especially the United States and Europe. The Kremlin uses digital tools to undermine liberal democratic institutions and weaken the cohesion among liberal Western democracies—cohesion that it recognizes as increasing the challenge to his regime. To this end, the Kremlin has deployed paid human trolls, AI-powered social media bots, and networks of individuals to interfere in public discussions at scale. The Kremlin's goal is to sow discord and uncertainty, divert critical discourse, erode trust in democratic societies, and undermine confidence in democratic institutions.[90] While the effect of these efforts is difficult to measure, they are designed to amplify differences in societies to further divide targeted populations and distract from anti-Kremlin narratives. The Kremlin's brand of digital autocracy, in other words, is not only about controlling citizens within Russia. It is also intended to make the world safer for Putin's regime.

Moving forward, the Kremlin will likely seek to balance Russia's digital development with increasing government oversight, both legal and digital. As Russia's model develops, the Kremlin will likely hold some sway over the trajectory of the future digital order, in large part by creating a model that autocrats—current and aspiring—can adopt or emulate. The countries closest to Russia, including Belarus, Azerbaijan, and some Central Asian states, have already adopted parts of the Russian model. The spread of parts of Russia's brand of digital dictatorship will create headwinds against U.S. efforts to maintain a free and open internet and ensure the democratic use of digital technology.

Russia's model of digital control differs considerably from that of China. Although Moscow is likely to borrow from Beijing's toolkit and the two countries will continue to share best practices, Russia's model will remain distinct. Russia's brand of digital autocracy combines legal and technological measures to control citizens'

access to information from the internet, suppress domestic opposition, and undermine democratic institutions around the world to ensure the regime's survival and advance Russia's foreign policy goals. The following sections examine the three pillars of the digital order—information control, surveillance, and technology governance—in the Russian context.

Information Control

Russian leaders have long viewed the media as instruments of political propaganda, and information as a commodity that needs to be controlled. For Putin, the first Chechen war and especially Russia's invasion of Georgia in 2008 underscored the importance of controlling information and the impact that public opinion could have on the regime's ability to advance its objectives. The Arab Spring and Russia's own large-scale protests in 2011 and 2012 further crystallized Russian leaders' belief that an uncontrolled internet threatens state stability. As the Kremlin has grown increasingly attuned to the challenges that digital technologies pose to authoritarian regimes, the Putin government has taken steps to increase control of the information environment. But rather than resorting to overt forms of censorship, the Kremlin has developed a system of legal mechanisms, discrete online surveillance, and growing internet sovereignty, while manipulating online discourse at home and abroad. This approach has enabled the Russian government to build a brand of digital authoritarianism that is distinct from China's model.

Legal framework. Russia's model of digital control is in part defined by a robust but often vague set of laws that allow for the blocking of a wide variety of content and systematic collection of user data. Russia's legal framework places a heavy burden of liability on content intermediaries, creating strong incentives for self-censorship—a key pillar supporting the stability of the Putin regime.[91] All Russian media, including the internet, are regulated by Roskomnadzor, or the Federal Service for Supervision of Communications, Information Technology, and Mass Media. Roskomnadzor and several other government agencies are charged with monitoring and blocking websites and social media posts that include "offending content," including calls for mass protest, crime, or extremist activity.[92]

While the authority to censor rests with the state, the responsibility to implement censorship falls on the internet service providers (ISPs), which are held legally responsible for forbidden content that is accessible to their users. Amid the January 2021 protests in

Protesters hold flags and banners aloft as they march in Bolotnaya Square on December 10, 2011, in Moscow. Protests took place in Moscow and St. Petersburg amid allegations from both domestic critics and international observers that the recent Duma elections had been rigged. Russia's ruling party, United Russia, lost its parliamentary majority but still won close to 49.5 percent of the vote. (Harry Engels/ Getty Images)

support of Navalny, for example, Roskomnadzor quickly moved to pressure social media platforms including TikTok, YouTube, and Instagram to remove videos that it said called for minors to participate in protests.[93] Roskomnadzor also maintains a list of banned websites that ISPs must broadly interpret to avoid liability for under-censoring, which can result in heavy fines and even the loss of their state licenses.

Since 2012, the number of laws underpinning Russia's digital control has grown. Russian authorities apply these laws indiscriminately, creating a chilling effect on the country's media environment. For example, the 2014 Blogger's Law requires all online outlets (including blogs and personal pages within social networking sites) with more than 3,000 daily page views to register with the government and be held legally liable for any content on their website that authorities deem inaccurate.[94] Likewise, the Law Against Retweets punishes with up to five years in prison the dissemination or re-dissemination of "extremist content"—which is defined vaguely so that it can be interpreted to include a broad swath of content. For example, Russian authorities have repeatedly brought charges against Crimean Tatars for online posts criticizing the invasion of Ukraine. Russian courts have also convicted at least six people of sharing pro-LGBT information over a four-year period under a 2013 anti-LGBT "propaganda" law.[95] In effect, this complex legal system empowers the government to surveil internet communications with few limitations, censor objectionable content, intimidate civil society

groups and media, and prosecute individual Russians for expressing dissenting political views.[96] Online media outlets and social media platforms also face the threat of potential financial takeovers and pressures to change editors, CEOs, or other key personnel if they fail to uphold content restrictions.

Internet surveillance. In addition to the legal framework, intimidation, and social norms around self-censorship, Russia's brand of digital control is based on a robust system of technical surveillance of internet traffic. The Kremlin has long used its System of Operative Search Measures (SORM) to monitor and filter content on the internet. SORM is a nationwide system of automated and remote legal interception adapted from the Soviet period. It covers all Russian telecommunications, including phone calls, email traffic, and internet browsing activity.[97] ISPs and telecom providers are required by law to install SORM equipment. Telecommunications intercepted by SORM equipment are stored in a national database for access by the Federal Security Service (FSB), which can monitor the data with little oversight and few constraints. Russian laws that effectively criminalize criticism of the government further empower the FSB to censor internet communications.[98] These capabilities allow the government to enforce its complex web of laws that effectively ban different forms of dissent. Civil society groups and media organizations are frequently targeted for surveillance.[99] Between April 2019 and June 2020, authorities brought 200 criminal prosecutions against Russians who disseminated information online that contradicted official statements—including against journalists, politicians, and activists.[100]

In effect, this complex legal system empowers the government to surveil internet communications with few limitations, censor objectionable content, intimidate civil society groups and media, and prosecute individual Russians for expressing dissenting political views.

Technological developments, including in data analytics, will enable the Kremlin to become more effective with its online surveillance. AI technologies, for example, will eventually enable the regime to sift through a greater volume of images and text, more effectively filtering and blocking online content that is unfavorable to the government. Much of Russia's recent publicly available AI research is focused on technologies with surveillance applications, including linguistics and natural-language processing for internet content monitoring, as well as computer vision, pattern recognition, and machine learning for facial recognition.[101] And even if censorship fails and dissent escalates, the Kremlin has an added line of defense: the government can block citizens' access to the internet (or large parts of it) to prevent members of the opposition from communicating, organizing, or broadcasting their messages. The Russian government reportedly used targeted mobile internet shutdowns during anti-government protests related to local elections in Moscow in August 2019, and there were some reports of disruption to mobile phone and internet coverage during the pro-Navalny protests in January 2021.[102]

Internet sovereignty and data localization. Beyond surveillance, the government has taken several further steps to increase control over the internet, despite the potential for backlash from a public grown accustomed to a relatively free and open internet. Since 2014, the Russian state has moved to establish a "sovereign internet" more like the Chinese model, which can potentially be severed from the global internet, allowing the government to control cross-border data flows.[103] Internet sovereignty laws allow for compulsory installation of state-controlled technical equipment and centralized control of cross-border connection lines, as well as the development of a Russian national domain name system. These sovereign internet measures will potentially allow the government to censor content more easily, stop the flow of internet traffic across Russian borders, determine the flow of information within them, and expand surveillance.[104]

The Russian government's efforts to assert control over the internet have also included a push for data localization through laws requiring all personal data on Russian persons to be stored domestically. As of July 1, 2018, anti-terror legislation, known as Yarovoya's Law, has required ISPs, cell phone operators, search engines, and other web services to store all Russian traffic, including private chat rooms, emails, and social network posts, for as long as six months at their own expense.[105] Metadata are to be stored for three years. Russia blocked access to LinkedIn in 2016 and has fined other large companies for failing to store all data on Russian territory.[106] In July 2021, Putin signed into law

legislation requiring foreign social media companies to open offices in Russia.[107] Such legislation represents yet another effort by the Kremlin to exert greater control over Big Tech. Moscow has also stepped up efforts to fine firms such as Google for failing to delete content it defines as being illegal.[108]

Government regulators block virtual private networks (VPNs)—a common means for bypassing internet controls—that allow access to content that the government has blocked.[109] Encryption has also increasingly become a target of internet regulation. In October 2020, the Ministry of Digital Development, Communications, and Mass Media published a draft law that will ban websites from using common internet encryption protocols that protect user privacy, potentially eliminating a barrier that currently makes it harder for the government to block banned content and track the websites that users visit.[110]

Propaganda and misinformation. Propaganda and misinformation operations are a defining feature of Russia's brand of digital control. The Kremlin seeks to manipulate the information environment at home and beyond Russia's borders to increase regime security and advance its own objectives. In both arenas, the government's tactics are designed not to limit the supply of information, but rather to flood the environment with pro-government information and misinformation; deflect and drown out negative press; distract, obfuscate, and confuse; and persuade through pro-Kremlin narratives.[111] Automated accounts (or bots) on social media amplify useful narratives inside Russia and in other countries and produce a flurry of distracting or misleading posts that crowd out opponents' messaging. The Kremlin floods the internet with pro-regime stories, distracting online users from negative news and creating confusion and uncertainty through the spread of alternative narratives.[112] Russia's misinformation and disinformation efforts abroad have been extensively covered, and the Kremlin uses many of the same tactics domestically as it does beyond its borders.[113] In both cases, the Russian government manipulates information with the goal of enhancing regime security.

Looking forward, maturing technologies such as microtargeting and deepfakes—realistic digital forgeries of audio, video, or images—are likely to further boost the capacity of the Kremlin to manipulate perceptions of its citizens and foreign targets. Microtargeting will eventually allow the government to tailor content for specific individuals or segments of society, just as the commercial world uses demographic and behavioral characteristics to customize advertisements. AI-powered algorithms, for example, will allow the government to microtarget individuals with information that either reinforces their support for the regime or seeks to counteract specific sources of discontent. Likewise, the production of deepfakes will make it easier to spread false information even more convincingly, potentially making it more difficult for individuals to know what is real and enhancing the Kremlin's ability to sow doubt, confusion, and apathy.[114]

Surveillance

Because the Russian state is the dominant funder of high-tech research in the nation, AI development there is likely to focus on applications of interest to government: surveillance and domestic security.[115] The Kremlin uses AI technologies to expand its physical surveillance of citizens, although its capabilities remain more limited than China's. Russian authorities have not published data on the number of cameras in cities, but reports suggest that in 2019, there were 193,000 in Moscow and 55,000 in St. Petersburg.[116] One Russian survey estimates there are more than 13 million video cameras across public places in all of Russia. This figure is far fewer than the 200 million in China and 50 million in the United States; but in per capita terms, Russia ranks third in the world behind these two countries.[117] Facial recognition cameras are also planned for Russia's schools. By June 2020, the surveillance systems had reportedly been delivered to 1,608 schools, and authorities plan to surveil the country's more than 43,000 schools in coming years.[118]

Russian authorities have used AI-powered facial recognition cameras to scan crowds for criminal suspects and monitor civic activity such as protests.[119] For example, Russian sources report that officials used the growing network of video cameras in public places and improvements in facial recognition technology to identify participants in the Navalny protests of January 2021 so that they could arrest them.[120] Doing so allows the regime to avoid high-profile arrests being captured on the streets by social media users, thereby reducing the risk of public backlash during vulnerable periods for the regime. Russian officials also posit that augmented-reality glasses will soon allow police to identify and track suspects in real time, although there are reasons to be skeptical of such claims, especially given the regime's interest in inflating public perceptions of its capabilities.[121]

The COVID-19 pandemic has raised questions about the strength of Russia's surveillance capabilities. The nation's network is likely less sophisticated than

China's and thus less able to effectively enforce public health rules. Nonetheless, the pandemic has allowed the Russian government to expand surveillance and experiment with new tools with its facial recognition camera network and surveillance of mobile devices.[122] In Moscow, authorities have enforced quarantines and punished alleged violators with the help of a network of facial recognition cameras, and the public has been required to download a mobile app that tracks residents' movements.[123] However, it remains unclear how effective these systems are, and researchers have expressed skepticism that the technology is as accurate as Russian authorities and manufacturers claim.[124]

Russian surveillance has taken other forms, including extended employee monitoring. Since October 2020, employees of Moscow companies that switch to remote work must provide employers with their personal data, including phone numbers, travel documents, and vehicle registration numbers.[125] Failure to comply with this requirement could cost employers a fine of up to 300,000 rubles (almost $4,000).[126] Local and regional governments, under a mandate from the Kremlin that took effect in December 2020, now operate "regional management centers" for data that combine citizens' personal information with other data such as traffic patterns, economic indicators, and shopping trends. The ostensible purpose of these data centers is to improve local and regional government functions. In effect, however, they act as management centers not for local governing but to tie Russians' personal data into central government oversight.

Though the Russian tech sector lags behind those of the United States and China, the Russian state has accelerated efforts to boost research and development of AI technologies. In October 2019, Putin approved a national strategy for AI. Its goals are primarily economic, including accelerating research and development of AI technologies and assuring national "self-sufficiency" in AI, including the "predominant use" of domestic technologies.[127] Several Russian companies have achieved market success in AI technologies, including facial recognition tech producer NtechLab.[128] Putin in 2019 promised to dramatically increase funding for the national AI effort, to $6.1 billion over six years, and called for additional legal changes that would be friendlier to high-tech research and experimentation.[129] In 2018, Russia announced a new company that seeks to exploit military developments in AI for civilian use, aiming to accelerate domestic applications for AI and reduce dependence on foreign suppliers.[130] Russia's focus on AI, even if it has not kept up with the United States and China, will increase its capacity to field digital tools.

Technology Governance

Russia promotes elements of its model of digital authoritarianism through diplomacy, particularly working with China in multilateral organizations to advance norms that legitimize state control of information under the pretense of cybersecurity.[131] In the West, cybersecurity is narrowly understood to protect data and internet infrastructure from damage or theft. U.S. officials have long argued that the open internet serves U.S. political, economic, and diplomatic interests. The internet freedom agenda advocated by the United States during the administrations of Bill Clinton, George W. Bush, and Barack Obama comprised ideas that would allow for the free flow of information on the internet in the interest of personal freedoms, economic growth, and innovation.[132]

However, Russia and China are advancing notions of cybersecurity, or, in their terms, "information security," that emphasize control over content and communications methods to eliminate threats to regime legitimacy and social stability.[133] The Russian government views the internet and the global media environment more broadly as working to advance U.S. and liberal democratic influence and values that threaten the Putin regime's hold on power. Putin has likened the American notion of internet freedom to "internet imperialism," an arm of Western influence within Russia's borders and a threat to domestic stability.[134] This perception underpins Russia's efforts in international arenas to legitimize its pursuit of surveillance and censorship capabilities and to encourage other countries to follow its lead. It is therefore a primary objective of the Russian state to not only assert sovereignty over the network within its borders, but also "make other countries, especially the United States, accept" this right.[135] Moreover, the Russian military considers itself the target of persistent U.S. cyber activity, using this stated belief to justify what it describes as "defensive" information and cyber actions inside Russia.

Russia sees international organizations as forums where it can reshape norms and advance new ones around cyber and internet sovereignty to create conditions more conducive to its vision of digital control and sovereignty. It frequently does so in tandem with China and other partner countries in the Shanghai Cooperation Organization, and especially in U.N. bodies. These forums tend to favor the interests of governments, many of which want greater internet control than do the civil society groups and tech companies that advocate for a free, open, and secure internet.[136] In 2011 and 2015, Russia proposed an International Code of Conduct for Information Security—presented at the U.N. alongside representatives of China, Tajikistan, and Uzbekistan—which calls on

states to crack down on "dissemination of information" that "undermines other countries' political, economic or social stability," as well as information that incites terrorism or extremism.[137] Largely rhetorical, the proposal illustrated these nations' approach to cybersecurity and seemed aimed at persuading developing countries of its merit.[138] In 2012, Russia introduced a proposal at the ITU that would allow national governments to usurp control of internet regulation functions currently managed by the U.S. nonprofit Internet Corporation for Assigned Names and Numbers (ICANN).

The U.N. has been a critical venue for Russian efforts to reshape global governance. Much of this work, which is done in lockstep with China, has taken place within the Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security (now known as the Group of Governmental Experts on Advancing Responsible State Behavior in Cyberspace in the Context of International Security, or more commonly just GGE). In 2013, Moscow worked with Beijing in the GGE to include language in the group's consensus report that "state sovereignty" and the international norms and principles that flow from sovereignty apply to state conduct in cyberspace. They expanded this norm in the 2015 report, which stated that sovereignty applies to states' "ICT-related activities and to their jurisdiction over ICT-related infrastructure within their territory."[139]

After failing to reach a consensus with the United States in the GGE in 2017, Russia and China have sought to build on their past progress with an Open-Ended Working Group (OEWG) open to all U.N. member states. Though the large and open-ended nature of this group naturally makes it slower to reach any meaningful consensus, it has served as another platform for Russian and Chinese representatives to promote norms of sovereignty in cyberspace over norms of internet openness and freedom.[140] In December 2019, Russia backed a resolution to establish a committee to consider a new U.N. cybercrime treaty. Several large democracies, including Nigeria and India, were persuaded by Russian arguments that a new treaty was needed to fight cybercrime and terrorism, even as the United States warned that the treaty could be a veiled effort to legitimize internet surveillance and crackdowns on online dissent.[141] In October, the United States and Russia agreed to seek a common set of "rules of the road" to prevent malicious cyberattacks. The U.N. joint resolution embraces Washington's favored Group of Governmental Experts report and Russian-backed recommendations from the Open-ended Working Group. The joint resolution underscores the two countries' commitment to and focus on cybersecurity and growing risks emanating from this domain.

Russian President Vladimir Putin addresses the United Nations General Assembly in 2015. Since then, Russia has attempted to shape global norms and standards on digital governance, promoting a model that gives sovereign states greater ability to regulate, censor, and undermine access to information. (John Moore/Getty Images)

Russia has also focused on building support for internet sovereignty. It hopes to create a precedent with its own effort to create sovereignty over the internet and monitor communications, and to persuade other countries to accept this sovereignty and adopt a similar model.[142] Moscow also sought international partnerships to develop technological alternatives to the current unrestricted global internet. Russia has pushed for undersea cable projects that would allow BRICS countries—Brazil Russia, India, China, and South Africa—to link their networks without routing traffic through the United States.[143] Additionally, Russia is pursuing greater ICT activity with other BRICS member states.[144] Putin has also worked bilaterally with Xi Jinping, signing a 2015 agreement on cybersecurity that further articulated and affirmed cyber sovereignty norms. The two countries continue to work in the framework of that agreement, primarily by jointly developing technology and processes for internet control.[145]

The Exportability of the Russian Model of Digital Control

The CCP will retain far more influence over the trajectory of the future digital order than the Kremlin. Nonetheless, Russia's experimental approach to information manipulation and control—one that combines legal and technological measures to limit citizens' access to information over the internet, suppress

domestic opposition, and undermine democratic institutions around the world—will continue to play a role in shaping future trends. Moreover, the Kremlin is likely to be forward leaning, taking on risk in its development and application of new digital technologies, which in turn will influence the future digital order. The Putin regime is likely to accept more risk in this domain because the Russian president is acutely aware that his country lags behind the United States and China in AI development. In particular, he seeks to avoid losing another key contested space to the United States.

For the time being, Russia's brand of digital authoritarianism will have the most influence in the countries along its periphery. Belarus, Ukraine, and several Central Asian countries have adopted SORM-like systems, making them natural customers for Russian-sourced surveillance technology. Moreover, many of these former Soviet nations have adopted parts of Russia's legal framework, which they similarly use to stifle the information environment.[146] Farther afield, Russian influence will likely be more limited, in part because the country is unlikely to compete with China as a primary exporter of digital control through its sales of surveillance technology, software, and applications. Nonetheless, the Kremlin will wield some influence in less direct ways, including diplomacy and norm-setting. Going forward, Russia's influence over the future digital order will likely depend on the ease of emulating the Russian digital control model, the efficacy and scope of digital authoritarianism inside Russia, the response of the international community, and Russia's ability to overcome barriers to technological innovation.

The Putin regime is likely to accept more risk in this domain because the Russian president is acutely aware that his country lags behind the United States and China in AI development.

The ease of emulating the Russian model. Many countries lack the capacity to emulate China's comprehensive model of censorship and social control. This requires a large state apparatus, expensive and advanced technology, and a domestic internet built for censorship from the get-go. In addition, China's model is more overtly repressive and therefore a risky choice for governments that still claim legitimacy by upholding the trappings of democracy. Russia's model, in other words, may be more appealing to a broader swath of countries. Russia's laws and other nontechnical forms of digital control do not necessitate significant resources or know-how, and the less overtly repressive approach may be more palatable than Beijing's model for countries that sit closer to the democracy end of the political spectrum.

Russia's primary edge on China in the surveillance technology market in some countries is that its solutions are, for now, cheaper and easier to install. But they may not remain that way for long. As more countries adopt other Chinese digital technologies, such as 5G equipment from Huawei, Chinese surveillance technology will become less expensive and easier to integrate, leaving less opportunity for Russia to grow its share of the surveillance technology market.[147]

The efficacy and scope of digital authoritarianism inside Russia. The Kremlin likely views digital tools as an opportunity to upgrade and enhance its repressive tactics. Putin appears intent on more effectively harnessing technology to solve Russia's domestic challenges, including the increasing public discontent with his regime. The appointment of Prime Minister Mikhail Mishustin, for example, likely reflects this focus. Mishustin had success as chief of the Russian Federal Taxation Service by using technological solutions to cut tax fraud and evasion while boosting government receipts. His success in those areas probably influenced the Kremlin's decision to appoint him prime minister. If the Kremlin can harness digital technologies to strengthen control over an increasingly restive population, other autocrats may take note and seek to emulate those tactics. Likewise, if Russia can prove a concept for nationalizing the internet, other leaders may follow suit.

The Kremlin's drive for greater control over the digital space, however, risks domestic backlash that could limit the scope of its control. Unlike China, Moscow did not build a controlled internet from the ground up, and the Russian internet has long been relatively free and open.[148] The government appears attuned to the risk of backlash and is taking incremental actions that over time could effectively limit the digital sphere without triggering a strong public reaction. However, Russians have grown accustomed to their relative freedoms online and could mount resistance to Kremlin efforts to restrict the space. Russian citizens protested against the internet sovereignty law, for example, and could continue to push back against future efforts, especially if they appear brazen.[149] Such domestic opposition could constrain the scope of what the Kremlin is able to do, limiting the comprehensiveness of the digital model that other leaders look to emulate. Likewise, wide-scale

protests and/or other forms of instability in Russia would also make the Kremlin's model less attractive for leaders watching from other countries.

The international response. Russia's influence operations have destabilized politics around the world, particularly in the United States and Europe. Intentionally or not, the Kremlin's aggressive posture has demonstrated the vulnerability of open societies to Russian tactics. Moreover, Russia has faced few consequences for its interference in the United States and in European democracies, signaling to other countries the limited costs associated with these efforts. U.S. adversaries such as China and Iran have followed Russia's lead and increased their initiatives to interfere in the U.S. domestic political system.[150] The ability of liberal democracies to mount a strong and cohesive response to Russia's tactics—by both raising the costs and increasing resilience—will significantly shape the extent to which other countries seek to adopt or emulate elements of the Russian model.

Limits on Russian technological competitiveness and innovation. Ultimately, Russian influence on the future digital order will be contingent on Moscow's ability to compete in this domain. There are, however, real constraints on the Kremlin's ability to meet its technological ambitions, and this will limit its future influence, at least on a global stage. First, implementation of some Russian initiatives has been plagued by delays. The Russian sovereign internet, for example, currently exists only on paper. Federal law now includes the frameworks for a centrally controlled internet, but implementing it has been challenging. A key test of the underlying technology was delayed in late 2020, and other tests had already been delayed because of the COVID-19 pandemic.[151] The pandemic has also thrown a wrench in data localization plans: Russian ICT providers are struggling to comply with new data storage requirements while also handling a huge surge in traffic caused by pandemic-induced restrictions.[152]

Likewise, Russia may be delayed in the development and therefore the export of its digital surveillance technology while it waits for its own domestic solutions. The country is determined to use primarily domestic technology for AI development, but still cannot produce key digital products with the same quality and efficiency as can China and the United States.[153] Brain drain and the lack of an innovative start-up culture have affected Russia's drive for domestic high-tech developments. Much of the country also lacks the infrastructure to support this high-tech development, although government programs are now trying to reverse the trend.[154] New government investment has helped address some of these flaws, but centralized funding also creates opportunities for bureaucratic waste and graft that could constrain advancement.[155] Moreover, because Russia's research and development is so heavily state funded, it is also overwhelmingly defense- and security-focused. Meanwhile, the pandemic has forced the national government to plan to scale back its financial support for civilian AI development.[156]

The Middle East

The Middle East region presents a different type of challenge for the United States than either China or Russia in the context of the global digital order. With the exception of Iran and Syria, the states in this region that use technology to strengthen authoritarian governance are U.S. partners. Egypt's government regularly uses information control and censorship online to stifle political discourse. The United Arab Emirates has one of the most pervasive surveillance systems in the world. Saudi Arabia used digital surveillance to track the movements of the dissident Jamal Khashoggi, who was ultimately murdered by operatives reporting to Saudi Crown Prince Mohammad bin Salman. Even Israel—one of the few democracies in the Middle East—has been associated with problematic behavior, with Israeli firms selling cutting-edge surveillance applications to repressive governments that have used the technology to spy on journalists and opponents.

This situation is not surprising given the broader context in the region and the history of U.S. policy. The Middle East is the least free region in the world, with 83 percent of the population living under repressive governments—regimes that Freedom House classifies as "not free."[157] Moreover, the United States has a long track record of maintaining good relations with these authoritarian states, because of evolving motivations that have ranged from countering the Soviet Union during the Cold War to relying on Middle Eastern oil to partnering with these states on counterterrorism after 9/11.

However, an increasingly authoritarian digital order in the Middle East works against U.S. interests in several ways. First, the low levels of freedom and opportunity for the region's populations, particularly young adults, have been major factors in instability and conflict during the past 20 years. This atmosphere has resulted in widespread repercussions, such as the development of terrorist safe havens and mass migration movements, which harm U.S. interests and destabilize allied and partner nations not only in the Middle East but also in

Europe. These problems will persist into the future if regional governments use technology to repress their populations more effectively.

Moreover, the pattern of using technology for illiberal aims contributes to growing levels of influence for America's peer competitors. China in particular can benefit from Middle Eastern states' demand for these types of technological tools, by exporting them and thus further strengthening Chinese influence.

Middle Eastern states, however, are less interested than Russia or China in exporting governance structures that support an authoritarian digital order. While Chinese and Russian efforts are at least partially inspired by their desire to bend international norms to their interests and thus counter the United States, Middle Eastern states have no such motivation. As U.S. partners, they are content to support the current international order provided that their violations of democratic norms are overlooked.

As a whole, this situation leads to tough questions for U.S. policymakers as they try to maintain good relations with many of the states in the region, while also convincing them to take steps to maintain a freer digital environment. The following sections again examine the three pillars of the digital order: information control, surveillance, and technology governance. Following this analysis, the paper then makes recommendations for how to address the policy challenges posed by nondemocratic partners in the context of the evolving global digital order.

In February 2011, thousands of people protesting former Egyptian President Hosni Mubarak used social media platforms, including Facebook, to amplify their message and organize protests in Tahrir Square in Cairo. Since then, Egyptian authorities have blocked internet activity by banning websites and online platforms, and have even jailed citizens for social media activity. (Chris Hondros/Getty Images)

Information Control

Across the Middle East, information control online has taken two central forms. The first is censorship, which is used as a tool by governments to suppress challenges to their authority. The second is the use of disinformation as a method of suppression and targeting other states. These developments are not new, but their speed and wide reach have intensified.

Censorship. Governments in the region actively curtail freedom of expression through institutionalized mass blocking, targeted attacks, and blanket bans on websites and online platforms. Egypt's growing digital authoritarianism serves as a dark example.[158] Over the past few years, Egypt's High Council for Cybersecurity has taken steps to block internet activity by acquiring high-tech equipment from Western countries, including the United States and Germany.[159] Egyptian courts have increased their crackdown on social media, jailing female TikTok influencers on charges of indecency and violating public morals.[160] In 2018, Egyptian President Abdel Fattah al-Sisi ratified the Anti-Cyber and Information Technology Crimes Law—ostensibly a counterterrorism measure allowing authorities to block websites considered "a threat to national security" or to the "national economy."[161] The Egyptian government also instituted a law that considers social media accounts with more than 5,000 followers to be publishing outlets, and therefore liable to more stringent restrictions and accusations of spreading fake news.[162] In June 2020, Egypt's Supreme Council for Media Regulation went a step further, announcing a ban on media covering "sensitive issues," which include the Grand Ethiopian Renaissance Dam, the coronavirus, and conflicts in Libya and the Sinai Peninsula.[163]

However, Egypt is far from the only example of a U.S. partner in the Middle East that uses online censorship to control political discourse. Before Bahrain's 2018 elections, the Ministry of the Interior announced plans to crack down on activists who criticized the government online; many have since been imprisoned and tortured.[164] In the case of Saudi Arabia, there was a significant increase in the number of censored websites after the murder of Jamal Khashoggi.[165]

Government censorship exists even when countries take positive steps toward peace and security in the region. For example, in the aftermath of the United Arab Emirates–Israel normalization agreement announced in August 2020, Twitter accounts linked to the Emirati government ordered security forces to monitor the tweets of residents opposing the deal; one account urged agencies to "expel them from this country because they will be a threat to the security of our nation."[166] In Egypt, the government warned its country's media outlets against publishing news and statements that criticized the Emirati-Israeli normalization agreement.[167]

Many regional governments also rely on blanket internet shutdowns to control the spread of information. For example, in response to anti-government protests in 2019, Iraq—a U.S. partner whose population has greater freedoms compared to those in many other countries in the region—deliberately interrupted internet connectivity for 263 hours, affecting 19 million users and costing the country an estimated $2.3 billion in lost economic activity.[168] In a more extreme case, the Iranian government imposed days-long internet blackouts in November and December 2019, as it pursued a bloody crackdown on protestors.[169] Indeed, Iran's Islamic Revolutionary Guard Corps works in concert with the Islamic Republic of Iran Broadcasting to develop cyber battalions that prioritize information control and content production to achieve their national security aims.[170]

In some cases, restricted internet access is also motivated by economic interests rather than information control. Oman, Qatar, and the United Arab Emirates have long blocked free internet calling apps, including WhatsApp, Skype, and FaceTime, to protect the commercial interests of their state-owned telecommunications companies.[171] During the COVID-19 pandemic, human rights activists have urged governments to lift restrictions on such applications, on which millions of low-paid migrant workers rely to communicate with their families at home.[172]

Disinformation. In addition to censorship, Middle Eastern governments often engage in disinformation campaigns, sometimes to downplay domestic challenges but more often as a foreign policy tool. These campaigns are occasionally the product of intense state-on-state competition, as was evident during the recent blockade of Qatar by Saudi Arabia, the United Arab Emirates, Egypt, and Bahrain. In cases involving American adversaries—most notably Iran—this disinformation is targeted at trying to counter U.S. priorities in the Middle East.

At the start of the blockade against Qatar in 2017, there were reports of the United Arab Emirates hacking Qatari state websites and posting comments that were falsely attributed to the Qatari emir.[173] Saudi Arabia and the United Arab Emirates deployed hundreds of thousands of bots to launch attacks on Qatar, criticizing the Muslim Brotherhood and Qatar's hosting of the 2022 World Cup.[174] In 2019, Twitter took down 4,525 accounts linked to Saudi Arabia, Egypt, and the United Arab Emirates for spreading propaganda that voiced support for the war in Yemen and opposed the Houthis, Qatar, and Iran.[175] The conflict in Libya, in which a number of regional actors have been engaged, has also become a ripe battleground for cyberwarfare, with Saudi, Emirati, Egyptian, Qatari, and Turkish accounts each elevating their own proxies. Last year, Facebook removed multiple pages, groups, and accounts for "coordinated inauthentic behavior" against Libya.[176] Meanwhile in Iraq, Iranian-backed Hezbollah have reportedly been training "electronic armies" to spread false information and incite violence against political opponents.[177]

Iran also conducts these types of political warfare operations against the United States. Between April 2018 and March 2019, threat intelligence analysts traced a number of social media accounts to an Iranian influence operation.[178] These accounts, many on Twitter, appropriated existing profile pictures, including those of U.S. political candidates, to create fake accounts and then spread doctored audio and video interviews, along with false American political commentary voicing anti-Saudi, anti-Israeli, and pro-Palestinian sentiment.[179] This material penetrated legitimate print and online media outlets in the United States and Israel via the publication of letters, guest columns, and blog posts.[180] Perhaps most worrisome, the U.S. intelligence community has concluded that in the run-up to the 2020 U.S. presidential election, Iran used a multipronged covert and overt influence campaign based on online tools to harm Donald Trump's prospects for reelection and undermine confidence in U.S. institutions.[181]

Surveillance

Across the Middle East, states deploy surveillance technology, mainly imported from such countries as China, Israel, Russia, and the United States, in the name of national security. States have long used digital infrastructure, such as closed-circuit television (CCTV) cameras and license plate detection, to surveil their populations, but have progressively enhanced their systems by adopting the latest AI and machine learning tools, such as biometrics solutions and spyware.[182] These

advances have allowed autocrats in the Middle East to monitor more people, collect more data, and use the information toward illiberal ends. Advanced technologies are weaponized to target political dissidents, journalists, and activists deemed threats to their regimes, spurring a chain of human rights abuses. The remainder of this section first describes how Middle Eastern governments use surveillance technologies. It then discusses the problems associated with exports of these types of technologies to the Middle East from democratic states such as the United States and Israel. Finally, it examines how the smart city model that the Chinese are exporting to the region has contributed to a more authoritarian digital order.

Use of surveillance technology. Governments throughout the Middle East use spyware to gain access to private data, primarily on cellphones. Through measures such as hacking, regimes are able to intimidate dissidents at home and conduct espionage operations outside their borders. U.S. partners such as the United Arab Emirates and Saudi Arabia have spent millions of dollars reinforcing their coercive ecosystems of "preventative surveillance."[183] The most famous example is Saudi Arabia's use of electronic surveillance tools to track Khashoggi to the Saudi Consulate in Istanbul, where he was murdered.[184] Saudi Arabia even went so far as to allegedly hire two Twitter employees to spy on users and hack dissidents' accounts.[185] In another example, the United Arab Emirates for years targeted Ahmed Mansoor, a prominent human rights activist, with spyware on his devices. In 2017, he was fined and jailed for his posts on Facebook and Twitter that allegedly "publish[ed] false information, rumors and lies about the U.A.E.," which "would damage the U.A.E.'s social harmony and unity."[186]

Surveillance technology is being used not only in the Gulf but also the Levant. The Egyptian government has supported sophisticated methods to target and track its own citizens. In one operation, software installed on the phones of Egyptian journalists, academics, activists, and opposition politicians allowed Egypt's General Intelligence Service to read victims' files and emails, track their locations, and identify whom they contacted and when.[187] In 2019, during a worsening economic and political crisis, Lebanese government agents infiltrated WhatsApp chat groups to track down anti-government protest leaders.

American and Israeli sales of surveillance technology. American companies and individuals have also been complicit in surveillance operations across the Middle East. Spyware equipment used in the region was traced to IBM and Google, though public criticisms and domestic regulatory constraints have caused some companies to distance themselves from projects of concern.[188] In an operation known as Project Raven, the United Arab Emirates hired U.S. contractors and former National Security Agency officials to help Emirati intelligence hack into the phones and computers of suspected terrorists, political rivals, dissidents, and activists using a sophisticated hacking tool called Karma. These operatives helped the United Arab Emirates collect evidence against Mansoor and his wife, including emails in which he discussed an upcoming demonstration in front of the Emirati Federal Supreme Court with family members of imprisoned dissidents. Ultimately, some American cyber professionals withdrew from the project and disclosed their concerns to the FBI.[189] This incident, however, points to the need for greater regulation to prevent former U.S. government officials who have these types of expertise from providing their services to nondemocratic states—including those aligned with the United States.

Israel, a key U.S. partner, has come under fire for exporting spyware to authoritarian states in the region and across the globe. In 2019, WhatsApp alleged that the Israeli surveillance company NSO Group had assisted governments with hacking into the mobile devices of dozens of people around the world, including journalists and human rights activists.[190] Further details emerged in 2021, including the release of a list of 50,000 phone numbers allegedly targeted by clients of NSO that counted opposition politicians and heads of state.[191] By delivering malicious software through seemingly innocuous WhatsApp video calls, the malware initiated various forms of spying, such as intercepting communications, stealing photos and other forms of data, activating microphones and cameras, and tracking the locations of targets.[192] Furthermore, Pegasus, a "lawful intercept" surveillance tool developed by NSO Group, was used to spy on Mansoor and Khashoggi.[193] NSO Group executives argue that they ultimately cannot control how their product is used, and that its primary purpose is as a counterterrorism tool. Importantly, in November 2021 the U.S. Commerce Department placed NSO Group on a blacklist stating that its behavior was "contrary to the foreign policy and national security interests of the United States," and sending a powerful signal that even companies associated with close U.S. allies will suffer consequences for this type of behavior.

To divert the illiberal trajectory of these high-tech applications, private companies must be held to higher standards. David Kaye, a former U.N. special rapporteur on freedom of expression, advocated for increased standards in the surveillance industry, highlighting the need for closer scrutiny of companies' client bases, as well as potential safeguards to prevent abuse.[194]

Smart cities and Chinese sales of surveillance technology. Gulf States have also looked to establish smart cities, which integrate a variety of surveillance efforts, including the use of sensors and cameras to gather information in real time. This information can be used for all kinds of purposes—ostensibly to consolidate the management of cities and raise productivity, but also to surveil and track dissidents. China has become an important investor in this arena, helping to establish smart cities in Iraq and Saudi Arabia.

In 2019, following the liberation of areas previously under ISIS occupation, Huawei launched the first phase of the Iraq Safe City Solution project, which aims to improve security measures. The initiative's objective is to reduce existing security checkpoints by incorporating smart surveillance cameras that track individuals more efficiently.[195] Since 2014, Huawei has also collaborated with authorities in Yanbu, a major Red Sea port city in western Saudi Arabia, to construct a connected city. The project involves installing broadband and cloud-computing infrastructure to build a sensor-enabled city, including security and public services. Huawei provided a comprehensive portfolio of network and information technology solutions, as well as devices such as surveillance cameras; the eSight + Network Management System platform, which uniformly manages network-wide devices; and software produced by Huawei partners.[196] The resulting operations collect a range of data on residents, including electricity consumption, vehicle parking, and crowd density, for simultaneous management and analysis.

In 2019, Yanbu installed an "e-police" system, which comprises 256 high-definition cameras at 16 major intersections, providing high-quality images and videos that allow authorities to trace vehicles or impose different controlling measures by automatically identifying traffic violations. Since its introduction, this system has reduced monthly violations from 5,000 to 2,000.[197] Similarly, police in Dubai have launched a system called Oyoon—"eyes" in Arabic—intended to reduce crime and traffic accidents by using AI to analyze images and behaviors that point to crime, with little regulatory oversight.[198]

China has been a significant player on this front in the Middle East. Multiple countries have signed memorandums of understanding with Chinese companies, and regional telecom groups have partnered with Huawei and ZTE to foster cooperation on 5G telecommunications.[199] While these advanced technologies can improve a country's safety, they can also facilitate nefarious aims if left unchecked. U.S. policymakers are rightly alarmed that companies such as Huawei, which has faced tighter restrictions from the United States, and Hikvision, the surveillance company whose equipment has been used to monitor Uyghurs in Xinjiang, have developed closer economic and technological ties with Middle East countries with a history of suppression.[200] Additionally, these developments provide the Chinese regime access to and control over critical infrastructure in the region. The expansion of China's Digital Silk Road threatens the civil liberties of people in these countries, exacerbates U.S. concerns regarding stability and the use of these technologies, and is a component of the strategic competition between the United States and China.

Technology Governance

Investment in emerging technologies carries the promise of a digital transformation for the Middle East—a path to economic growth and decreased dependence on oil. Indeed, many states in the region are keen to embrace this opportunity. The reality is, however, that given the highly repressive nature of these states, they are also content to use the technology for illiberal ends and are certainly not keen to establish the type of norms that can protect the rights of their populations. The result is that technology standards and regulations in the Middle East are moving more slowly than adoption and aspirational visions.

Adoption of AI serves as an emblematic case. According to a 2020 survey, 82 percent of large companies across the Middle East and North Africa had launched AI programs by the end of 2019, though the speed of adoption has trailed behind other parts of the world.[201] When it comes to regulatory frameworks, however, the region is characterized by a general lack of AI regulation, standards, and ethics.[202]

Regulations on management, transfer, storage, sharing, and use of data are also deficient—despite the central role such protocols would play in any potential digital transformation. Even among Middle East–based companies that adopt AI, executives identify additional regulatory clarity and agreed-upon industry standards as prerequisites for willingly engaging in the data sharing that would bring benefits such as faster supply chains and more innovative product development.[203]

Beyond business-to-business data sharing, there are also no regulations or clear guidelines for cross-border data flows. No Middle Eastern countries currently participate in plurilateral or bilateral agreements, either binding or non-binding, that would provide a framework for data transfer across borders.[204]

Data protection laws are on the books in the free zones of Abu Dhabi Global Markets and the Dubai International Financial Centre, but not the United Arab Emirates comprehensively. In Dubai, the laws cover the regulation of data collection, transfer, and sharing.[205] Egypt's data protection law went into effect in October 2020 but will likely not be enforced until 2022.[206] Since 2018, Bahrain, Qatar, and Turkey have all made efforts to pass legislation that addresses certain aspects of data privacy. Given that most legislation in the region is nascent, the effectiveness of the laws as well as enforcement precedents and patterns have yet to be evaluated. Regulations are still to come in Saudi Arabia.[207]

Given the authoritarian nature of most of the governments in the region, they are unlikely to develop effective technology governance because such standards are ultimately not in their interest. Instead, the models supported by China, which entail economic growth combined with using technology as a mechanism to reinforce an autocratic system, are far more appealing.

The only good news is that most of these countries do align themselves with the United States and, unlike China or Russia, have little interest in fundamentally reshaping the international order. Thus, while they may be receptive to China's version of the future digital order, they will not go out of their way to promote it. Indeed, there may be opportunities for the United States to move these states in a more positive direction over time.

Implications of Regional Trends for the Digital Order

Efforts by authoritarians to shape the digital order have implications that must be addressed by initiatives to safeguard liberal democratic norms and values. This section outlines four dynamics that are especially concerning. First, the increasingly close alignment between China and Russia will generate dangerous digital synergies. Second, authoritarian regimes will inevitably seek to expand censorship of free information exchange and political speech. Third, illiberal governments throughout Asia, the Middle East, and parts of Eurasia will continue to seek technology, funding, and technical expertise from China to control social movements and civil society protests. Together these trends will impair U.S. efforts to mitigate risk to the global digital order. The emerging patterns stem from the interplay between different actors across multiple regions. To ensure a more liberal digital order, it is necessary to understand how attempts to expand digital authoritarianism could mutually reinforce and accelerate illiberal behavior.

Growing China-Russia alignment will generate dangerous digital synergies.

Russian and Chinese views on emerging technologies and digital control are increasingly aligned. Both governments view a free and open internet and the spread of social media and other digital tools as threats to their national sovereignty and their hold on power. These governments view the internet and digital technologies as conduits for the United States to destabilize their regimes and as tools for citizens to overthrow oppressive and unresponsive administrations. They are therefore taking steps and aligning efforts in the digital realm to solidify control over their populations internally. While China will retain a leading role in the digital domain, the countries' alignment and increasing coordination are likely to amplify the effects of their individual actions in several ways:

Making digital autocracy accessible for a broader swath of states. Chinese and Russian leaders have concluded that digital tools, if properly managed, can be leveraged to increase their control over their citizens. But the two countries have approached digital authoritarianism differently, in large part because they started from different places domestically. China built repression and control into its model from the start, whereas Russia is now working to roll back a previously open space. Nonetheless, the two countries will continue to share best practices as they refine their approaches to digital dictatorship. Just as important, the differences in the Chinese and Russian toolkits offer aspiring autocrats a grab bag of options for tailoring approaches to digital control that are best suited to their own domestic contexts. In some cases—most likely in full autocracies—China's model will dominate. In hybrid regimes where leaders want to maintain the veneer of democracy or cannot get away with such blatant repression, leaders will likely mix and match elements of the Russian and Chinese models. In this way, the alignment of the two countries' objectives—even when they pursue them differently—is likely to amplify the effect of their individual actions by making digital authoritarianism accessible for more states.

Accelerating their digital innovation. Russia and China view the technology domain as a critical battle space in their competition with the United States, and in some instances view collaboration in the digital sphere as offering the potential for accelerated innovation. Their technology-focused dialogues and exchanges indicate that collaboration in areas such as AI is a priority that should be expected to expand. In some cases, their collaboration will have the potential to accelerate the development of illiberal technologies. For example, Russia's NtechLab (one of the country's leading developers in AI and facial recognition) and China's Dahua Technology (a manufacturer of video surveillance solutions) jointly produced a wearable camera with a face recognition function. Complementarity between the two nations in AI development may allow them both to more quickly develop surveillance and predictive policing models that other governments will follow.

Eroding liberal norms in international institutions. China and Russia view the structure of governance of the internet as a source of U.S. power and influence. They therefore seek to undermine this system and shape norms around the internet and emerging technologies such as AI in ways that advance their own illiberal interests. They have made progress on this front and are likely to continue to push a large cadre of states to back their visions for internet sovereignty and domestic surveillance. China, for example, has joined with Russia and a coalition of other countries to build support at the United Nations for their concepts of digital sovereignty. This coalition is composed entirely of nations ranked by the Freedom House's "Freedom in the World" index as not free. Its strength was clear in December 2019, when the U.N. adopted a cybercrime resolution titled "Countering the Use of Information and Communications Technologies for Criminal Purposes" that was jointly backed by China, Russia, and a consortium of illiberal actors including North Korea, Iran, Syria, and Venezuela.[208] The resolution stands in stark contrast to the norms that the United States and its allies have championed, including maximal access to the global internet, and instead seeks to equip authoritarian governments with broad-based means to punish, repress, and censor dissidents online.[209] While the Sino-Russian view on internet governance does not currently enjoy majority support in most international institutions, it is plausible that a plurality of states could join the cause in the future. They are also likely to amplify one another's efforts to create alternative cyber, AI, and digital economy domains that will not be constrained by democratic norms, civil liberties, and privacy standards.

Raising the prospects of "splinternet." Russia and China are pursuing independent root server systems, pushing hosts to remove root servers from the United States to limit America's ability to cut off internet access.[210] As noted, Russia is following China's lead in its effort to create a sovereign internet, RuNet—an initiative that analysts have compared with China's Great Firewall.[211] Although Russia's capacity to implement the law is untested, RuNet's existence underscores the way Russia and China are sharing best practices and legitimizing each other's actions. Working together, these two nations pose a more potent force advancing a trend toward fragmentation. If other countries follow suit, the splintering of the internet will create high barriers for global trade, cause U.S. tech companies to lose access to global markets, limit citizens' access to free and open information, and empower authoritarians around the world to tighten control over their countries—potentially resulting in fewer countries aligned with U.S. values and interests.

It is inevitable that countries around the world will seek to regulate online communications platforms.

Online communications platforms have reshaped the global political information landscape. For years, the spread of U.S. platforms across Southeast Asia, South Asia, and the Middle East was viewed as a vector of free speech and political liberties. The Arab Spring was launched on Facebook in 2011; WhatsApp helped topple 50 years of one-party rule in Malaysia in 2018; and even Tinder, the dating app, played a vital role in the 2020 Thai protest movement.[212] But these unregulated information ecosystems have become pathways for legitimate and spurious news alike. They have imperiled elections in Indonesia and the Philippines, and they have been abused to stoke ethnic and religious violence in India and Myanmar.[213]

Social media. Governments across the world have exploited the issue of fake news and disinformation on unregulated platforms to assert heavy-handed censorship over online information spaces. From Egypt to Singapore, regimes have used concerns about false news to crack down on activists and opposition parties.[214] Even India—the world's largest democracy—has started to institute regulations on social media. In February 2021, India announced the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules. The new regulations require Facebook, Twitter, and YouTube to appoint India-based compliance officers, who will

provide a report every month that details complaints received and what actions the companies have taken to address them. The companies will be required to remove content within 36 hours of receiving a legal order from Indian authorities, and to reveal the originators of such content. Although these new regulations may have merit, the hurried way they were announced, with little warning to the affected companies, raises questions. Many observers view the rushed new orders as a response to a recent dispute between the Indian government and Twitter regarding hashtags tied to farmer protests that rocked the government in late 2020.

Data localization laws. Data localization laws pioneered in China and Russia have been adopted by India, Pakistan, Turkey, Indonesia, and Vietnam, where governments share a desire to enjoy the economic benefits of digitization within the safety of highly controlled online spaces.[215] More recently, however, governments in India, Indonesia, and Vietnam have relaxed data localization policies, following heavy lobbying by U.S. industry.[216]

Company self-censorship. Technology companies—including U.S. ones—have compounded the issue of states exerting greater control over online platforms. Chinese apps such as the video-sharing platforms TikTok and Kuaishou have gained significant ground on American competitors in fast-growing online markets including Brazil and Southeast Asia.[217] The Chinese companies have admitted to self-censoring content about such subjects as repression in Xinjiang and protests in Hong Kong.[218] Non-Chinese companies also are turning to self-censorship as a means of ensuring they retain a foothold in markets governed by authoritarian governments. U.S. companies including Disney, Yahoo, and Zoom have attempted to toe the CCP line on sensitive issues to avoid losing market access.[219]

Illiberal regimes will seek out Chinese technology to help them control social movements and civil protests.

As autocratic governments and leaders in fragile democracies look to exert greater control over their populations and pursue cheap pathways toward digital development, they find Beijing's high-tech illiberalism an attractive model. They actively seek China's technology, funding, and know-how. These countries justify their pursuit of Chinese technology by underscoring ways it will contribute to economic growth, social stability, and efforts to fight crime and terrorism. Across the Middle East and Indo-Pacific, countries such as the Philippines, the United Arab Emirates, Egypt, and Iran have readily welcomed the adoption of technologies that can be employed for illiberal ends. Chinese technologies and associated norms offer these countries appealing tools for pursuing their interests—population control, state-on-state competition, shifts in regional alignment, and market incentives.[220] However, the autocratic leaders' true aims are to keep a lid on criticism of the government, and to easily identify and punish individuals who dissent from their policies or inspire others to do so.

The demand for Chinese technology. Beijing has exported surveillance technology worldwide, often to countries that seek more effective and cost-efficient ways of repressing opposition. For example, in the United Arab Emirates, Huawei, which has close linkages to the Chinese government, is partnering with local authorities on Safe Cities platforms that provide comprehensive surveillance.[221] And in 2012, ZTE, one of China's largest telecommunications companies, sold surveillance systems to the Telecommunication Corporation of Iran, a state-owned company.[222] In 2018, the Filipino government contracted with Huawei and the China International Telecommunication and Construction Corporation to construct a 12,000-camera surveillance system across metropolitan Manila and other cities. These systems allow the government to monitor landlines and all communications across phones and the internet, mimicking China's own use of authoritarian controls.

Copying Chinese regulations and standards. Not only have these countries imported Chinese technologies, they have also looked to Beijing as a model for designing a regulatory environment that benefits government interests. Chinese companies have helped produce other countries' government plans, as was the case with Huawei and the "Lao National ICT Development Plan 2016–2020 White Paper."[223] In the Middle East, Huawei partnered with the U.S. firm Deloitte to develop its own vision of "Government 4.0" in the region, applying the latest technologies to modernize the delivery of government services.[224] China has hosted numerous sessions on censorship in Egypt, Jordan, Saudi Arabia, and the United Arab Emirates.[225] Egypt's latest moves in broadening its censorship efforts unequivocally mirror China's internet governance strategy.[226] Similarly, in the United Arab Emirates, Iraq, and Saudi Arabia, firms including

Huawei and ZTE are partnering with local authorities on Safe Cities platforms to provide comprehensive city surveillance.[227]

The dilemma for the United States. U.S. partner interest in using technology for illiberal purposes poses a dilemma for the United States, which must decide if it will push back on the contentious behaviors and transactions of its allies around the world. If it chooses to do so, it must decide how, to what extent, and potentially at what cost. The dynamics in the Middle East underscore the challenges facing U.S. policymakers. The notion that the United States can export its own high-tech equipment to displace Chinese investment may be valid with a democratic partner such as Israel, but not with a non-democratic partner such as Saudi Arabia, which will deploy these technologies, regardless of their origin, toward the same authoritarian ends as does China. High-tech illiberalism in part is a function of where the technology is employed, and not necessarily its country of origin, whether that is the United States or China. Yet in some cases, the United States should be prepared to amplify democratic values and principles as a means of providing an alternative to China, and as the basis for future economic cooperation with these countries. Furthermore, the United States can facilitate and encourage investment and cooperation between its like-minded allies and countries susceptible to the Chinese model, especially in projects where the United States itself cannot directly assist.

The practices of illiberal regimes will reduce the efficacy of U.S. mitigation efforts.

Current U.S. efforts to mitigate digital authoritarianism are insufficient. The United States uses sanctions, export controls, cost imposition measures, and censure through international institutions to counter the multipronged efforts of its adversaries in the digital space. However, this playbook will prove outdated in the new digital order. This expanding, permissive environment has allowed bad actors to pull from a grab bag of digital tools to exert control. Russia's and China's complementary efforts to accelerate illiberal innovation will diminish the efficacy of U.S. mitigation practices. This factor, coupled with the creation of technical redundancies and coalition-building moves to counteract U.S. pressure, necessitates an agile, comprehensive policy response from the United States.

Authoritarian governments can embolden other states and lower the barrier to entry for other bad actors to propagate high-tech illiberalism. For instance, Russian forays into U.S. election interference in 2016 broke open the path for China to try its own, distinct tactics in the digital sphere during the 2020 U.S. presidential race.[228] Iran, long practiced at hard cybersecurity operations, crafted similar attempts to take aim at Americans' trust in their electoral system in the run-up to the 2020 U.S. presidential election.[229] In addition, the newly permissive environment expanded the playing field to non-state actors and chaos agents leveraged by adversary governments. Russian use of fringe media outlets and China's co-opting of "patriotic netizens" to harass Democratic Progressive Party supporters in Taiwan provided operational experience for these new players while obfuscating links to the governments that sponsored them.[230] A growing number of bad actors who work in a complementary fashion accelerate and broaden the challenges, making mitigation more difficult.

The marriage of convenience between authoritarian governments can also counter U.S. pressure through coalition building. Countries can cultivate ad hoc alliances that both legitimize them to outside states and offer an attractive, alternative bloc characterized by subsidized technology and quick tech rollouts. In this way, Russia confers legitimacy on China, and vice versa, when attempting to appeal to nation-states on the fence about adopting Western technologies. This veneer of legitimacy, coupled with material considerations, can be compelling to national leaders with autocratic sympathies. On the U.S. side, this factor makes it more difficult to encourage such leaders to pursue democratic digital behavior.

Recommendations

The United States and its allies and partners are engaged in a contest over the future digital order. To effectively shape this order and ensure that democratic rules and norms in the digital domain prevail, the United States must pursue a multipronged approach, tailoring its engagement to different actors and contexts. U.S. efforts to advance a more liberal digital order must include actions that are customized according to whether they are applied at home or for democratic partners, nondemocratic partners, or competitors.

At Home

The United States needs to put its own digital house in order to effectively shape and promote a liberal digital order around the world. A shortfall in regulatory oversight and a lack of national policies on digital matters is inhibiting America's ability to lead.

The United States should enact a national data protection and privacy law. Congress should:

- *Establish a data protection framework that clearly articulates the U.S. approach to data privacy at home.*[231] Such measures are necessary to address national security risks, streamline regulations, mitigate barriers to innovation, and create a better environment for global influence on data protection and privacy issues.[232]

Relevant U.S. government entities should hold regular formal consultations with U.S. tech companies on the risks of doing business in countries with nondemocratic governments. The National Security Council, in conjunction with the Departments of State and Commerce, should:

- *Initiate an ongoing dialogue between government officials and tech company executives on matters of digital freedom*. These should be two-way exchanges, with government officials and industry representatives sharing ideas on best practices, creating information-sharing mechanisms, identifying risk indicators, and anticipating challenges.[233]

The U.S. government needs to prioritize research and development of privacy-preserving technology solutions. To this end, Congress and the White House would be well served to:

- *Create incentives for novel research in technologies that preserve privacy of data, while also maintaining the use of techniques to extract value from datasets.* These technologies include homomorphic encryption, secure multiparty computation, differential privacy, and distributed learning.[234]

With Democratic Partners

The United States must work with like-minded democratic partners to ensure a digital order that preserves and promotes open societies, and to combat the illiberal use of emerging digital technologies.

The U.S. government needs to recruit and convene democratic allies—both bilaterally and multilaterally—to craft and execute a comprehensive framework to shape the future digital order. The White House should:

- *Formalize the tech alliance concept of a global governing body of techno-democracies to coordinate policy with a broader pool of allies.* The United States should push for the creation of a multilateral forum comprising the world's leading techno-democracies to serve as the mechanism by which members reach a coordinated approach. Such an organization will be valuable at the very least for the purposes of better information sharing, and for addressing the priority agenda items mentioned previously. Members, in addition to the United States, should include Australia, Canada, Finland, France, Germany, India, Israel, Italy, Japan, Netherlands, South Korea, Sweden, and the United Kingdom.
- *Pursue bilateral and minilateral working groups with techno-democracies to coordinate policies and strategies pertaining to technology.* The United States should also introduce bilateral working groups with key partners, or in some cases small subgroups of partners (e.g., several key European states together), to address this issue. The working groups should involve subgroups to discuss: (1) reconciling U.S. and partnership strategic perspectives on China, led by the U.S. State Department; (2) developing and sharing best practices in investment screening and export controls, led by the U.S. Treasury Department; and (3) deepening economic and technology cooperation to enhance the United States' and its partners' technological edge, led by the U.S. Office of Science and Technology Policy.
- *Expand cooperation on digital initiatives in the Indo-Pacific with like-minded democratic partners, starting with the Quad countries.* The National Security Council should continue to guide U.S. interagency efforts to operationalize the Quad working group on emerging and critical technologies. The working group should

identify which areas of technological development are most central to maintaining a free and open political order, and then develop a common understanding of the challenge. The four countries should decide on a coordinated policy approach, and then consider how to expand multilateral action within a wider group of democratic nations.[235]

- *Work through the U.S.-EU Trade and Technology Council to develop a shared vision and approach to managing the human rights implications of technology.*[236] The transatlantic partners need to outline a shared understanding of how to ensure human rights protections in the application and development of technologies, as well as how to effectively compete with China's technology offerings in developing countries. Such a shared understanding will provide a strong foundation to take into discussions with a broader set of democratic nations, including the Quad countries as described above.

The U.S. government must work in tandem with industry leadership in international standard-setting bodies to promote better alignment and coordination with like-minded countries within these bodies. To effect this, the White House and Congress ought to:

- *Engage key partners to counter China's influence within international bodies that set standards for fundamental technologies.* On critical technologies such as 5G, the United States should work with the European Union, Japan, India, and South Korea to increase transparency and representation at the ITU and 3GPP.[237] Collaboration with existing agencies, including the National Institute of Standards and Technology, will allow the United States to develop and promote technical standards that are in line with U.S. interests.[238]
- *Provide financial support or incentives for U.S. firms to increase their representation on international bodies that depend on industry stakeholders.* Some international forums, including the International Organization for Standardization, are heavily dependent on industry stakeholders. However, smaller firms often cannot afford to work on proposals for standards.[239] Targeted grants will allow smaller U.S.-based vendors to participate in standard-setting bodies.[240]

The U.S. government should counsel key partners on best practices for investment screening and export controls. The White House and the Departments of State, Commerce, and Treasury should:

- *Design and strengthen systems for screening technologies that are susceptible to abuse by authoritarians.* Washington should help partner governments on the front lines of digital illiberalism to design and strengthen their screening systems. These include India's addition of a government-approval requirement for investments from its bordering countries,[241] the European Union's Investment Screening Regulation,[242] and Israel's advisory committee on foreign investment in October 2019.
- *Establish interagency processes to coordinate technology policy partnerships.* The Departments of State, Commerce, and the Treasury should coordinate export controls, technology controls and standards, and acquisition efforts.[243]
- *Use the U.S.-EU Trade and Technology Council to share insights on specific companies and cases that need to be protected.* Investment screening will be a central theme for the Trade and Technology Council, featured in one of the effort's ten working groups. Policymakers should ensure that they move past political statements about working together to align investment screening and start sharing insights on specific cases.

The United States should work with its democratic partners to incentivize and encourage middle income and developing countries to invest in trusted and secure technologies and technology infrastructure. To this end, we recommend Congress and the White House:

- *Provide financial support or incentives so that democratically aligned digital firms from allied and partner countries will provide trusted alternatives to Chinese digital investments.* Washington should leverage the expanded authorities granted by Congress to the DFC to selectively back ally and partner firms that are well positioned to offer alternatives to China's digital infrastructure. The United States should also facilitate the growth of sustainable start-up ecosystems abroad, through publicly funded incubators and government support for private American incubators abroad.
- *Establish a Digital Development Fund through USAID to collaborate with the DFC.*[244] USAID and the DFC should collaborate to set up a Digital Development Fund to support information connectivity projects in the Indo-Pacific and beyond. With Beijing offering financial and political support to its national technology champions, companies from the United States compete at a disadvantage in third markets. A new U.S. Digital Development Fund will help to rectify this imbalance by providing lines of credit and concessional grant capital to U.S. companies building information

connectivity projects overseas, including those in the Indo-Pacific. One digital infrastructure development effort that the DFC could seek to replicate is its successful support for an undersea fiber-optic cable connecting the United States, Singapore, and Indonesia.[245]

- *Develop assessment frameworks and standards to vet digital development projects with the State Department, USAID, and the DFC.* The Blue Dot Network, a concept developed by the Trump administration, certifies transparent, sustainable, and inclusive infrastructure projects. Along these lines, the State Department, USAID, and the DFC should collaborate to develop standards specific to digital infrastructure projects that can be coordinated with allies and partners. After the standards are developed, the State Department should spearhead an effort to encourage fragile democracies to sign on to the framework. This can be accomplished by emphasizing the benefits of cultivating open digital ecosystems for economic growth, job creation, innovation, and capacity building.
- *Support democratic innovation bases that give incentives to diverse vendors and focus on developing secure and modular alternatives to China's Safe City and surveillance technology solutions.* The U.S. government should fund the development of privacy-protecting alternatives to Chinese surveillance technology. For instance, by funding research into technological solutions to combating online disinformation, the United States will encourage industry to develop tools that avoid intrusive solutions such as those employed by the Chinese.

The United States needs to boost multilateral engagement on governance and technical norms and standards as they pertain to emerging digital ecosystems. To effect this, the White House Office of Science and Technology Policy is advised to:

- *Launch initiatives with allies in the Indo-Pacific to build a shared set of norms on safe practices for the use of cutting-edge technologies, which can then undergird future proposals at international standards bodies.* The United States should start these discussions with Japan, and then bring in other like-minded democratic partners from Asia and Europe. The goal should be to develop consistent standards and guidelines that protect individual privacy, promote government transparency, and allow for broad and inclusive access to technologies.

U.S. government agencies should build local resilience among civil society and watchdog groups to combat foreign influence operations or other forms of illiberal technology use. The State Department should:

- *Establish a standalone Digital Rights Fund to support civil society groups playing a watchdog role.* A Digital Rights Fund will provide project accountability whenever the U.S. government helps partner nations with weak governing institutions develop their digital ecosystems. The United States could also invest in initiatives modeled on the Open Technology Fund to shape the digital development trajectories of nations with illiberal digital regulatory systems.
- *Provide best-practices training to local media in countries such as Thailand, Myanmar, and Cambodia on how to counter Chinese and other disinformation campaigns, and empower civil society organizations in countries that are particularly vulnerable to digital influence operations.* Several parts of the U.S. State Department are well positioned to support such initiatives. The Bureau of Democracy, Human Rights, and Labor should expand funding for technologies—such as VPNs—to empower activists and journalists living under oppressive regimes. The Bureau of International Information Programs should support exchanges about digital norms between governments and civil society groups. The Global Engagement Center is also advised to form strategic partnerships with local media.
- *Develop an expanded Fulbright Scholars program for journalists from countries on the front line of Chinese influence campaigns.* In this initiative, scholars would be awarded sponsorship funds to receive media training at U.S. universities. Additionally, the program could sponsor American journalists doing stints in these countries, thereby supporting local media in their efforts to cover the rise of high-tech illiberalism.[246]

With Nondemocratic Partners

The United States does not have the luxury of working only with like-minded, democratic allies. To provide a formidable counterweight to such anti-democratic competitors as China, Russia, and Iran, it must emphasize digital freedom concerns in bilateral relations with other nondemocratic partners.

U.S. agencies should regulate U.S. entities or persons' participation in and support of the illiberal use of technology in overseas markets. The Commerce and State Departments must:

- *Provide explicit guidance to U.S. companies operating in the markets of nondemocratic partners, and take measures to prohibit U.S. companies from entering joint ventures with Chinese companies in areas that could have negative implications for digital freedom, such as smart cities.* The U.S. government should support continued economic engagement with nondemocratic partners—but establish clear redlines around areas where U.S. and democratically allied companies may not invest or enter. This process should include restrictions on U.S. companies' sharing, for example through joint ventures, of certain types of technology that can be used for surveillance and censorship.
- *Take measures to establish a noncompete regulation to prevent former cybersecurity experts and officials trained or previously employed by the U.S. government from working for foreign governments.* The United States should put restrictions on former U.S. government officials, especially in the intelligence and technology sectors, working for nondemocratic allies. It is not uncommon for former analysts in the intelligence community to leave government and use their cybersecurity skills in the private sector or abroad. Currently there are few, if any, restrictions preventing government employees from later leveraging their extensive cyber experience in opportunities with foreign governments. The United States must instead rely on the goodwill or conscience of former employees to recognize the serious national security dangers associated with working with foreign, nondemocratic partners in particular. Washington should codify provisions that prevent these government-trained cybersecurity experts from potentially exploiting U.S. systems through employment by foreign governments. In addition, the intelligence community must find ways to lower attrition rates and increase the number and range of competitive opportunities for employment within the U.S. government that are available to these cyber experts.

Countering U.S. Competitors

The United States must leverage its powerful economic tools to counter competitors' illiberal technology use. Together with its allies and partners, the United States should work to effectively combat tech-enabled human rights abuses and other repressive policies.

The United States is advised to harness sanctions, advisories, and export control measures to impose costs on the repressive practices of illiberal governments. The White House should:

- *Consider additional Magnitsky Act sanctions and Leahy law restrictions—in concert with the Commerce Department's Entity List—if companies are found to be complicit in tech-enabled human rights abuses.* Measures to be deployed in such cases should include International Emergency Economic Powers Act suspensions (for example, importation or distribution of Chinese-controlled social media services and apps should be banned) and divestment via the Committee on Foreign Investment in the United States. Pursuant to the Uyghur Human Rights Policy Act of 2020, the U.S. president and the FBI should bring closer scrutiny to technology companies involved in repression in Xinjiang, and work with Customs and Border Protection to block the import of associated goods.[247] The executive branch and relevant government agencies could also explore the creation of a sanctions list for any company that provides technologies for mass surveillance systems without accompanying safeguards.[248]
- *Coordinate with the Commerce and Treasury Departments to sanction illiberal governments' digital economies, including cybersecurity firms, in cases of their use of technology for repressive or disruptive purposes. This will signal that regimes must be responsible actors to participate in the global ecosystem.* Such actions will likely attract the attention of illiberal governments, given that many of these regimes have prioritized the development of their digital economies.

Relevant U.S. agencies must focus on protecting areas of comparative strength vis-à-vis nation-state adversaries. To this end, the U.S. Commerce Department is advised to:

- *Assess relative costs and benefits of export controls on AI chips, which can encourage import substitution, versus targeted end-use/end-user controls on chips and on the semiconductor manufacturing equipment that is used to make the chips.*[249] Just as the United States has moved aggressively to choke Huawei's supply of semiconductor chips, it should seek to cut off China's means of stealing the intellectual property for and importing supplies of the chips upon which AI companies rely. Graphics processing units (GPUs) are a particular supply chain vulnerability for China's AI firms. GPUs are a central component of AI training, and the global

market share is split between three U.S. companies: NVIDIA, AMD, and Intel.[250] None of China's 10 leading chip makers specialize in making GPUs, and though some Chinese startups have declared their intention to enter the field, they are currently unable to compete on any significant level.[251] Chinese chip makers are also entirely dependent on foreign sources for semiconductor manufacturing equipment, making these devices a key chokepoint.

Conclusion

Critical trends around information control, surveillance, and technology governance are shaping the use of technology across the globe. An effective policy response to authoritarian attempts to reshape the digital order will necessitate dealing with a diverse set of actors, including key democratic partners, nondemocratic actors, and competitors. Policy solutions must account for emerging digital synergies between China and Russia. Dangerous digital synergies between China and Russia will make digital autocracy accessible for a broader swath of states, while accelerating their digital innovation, eroding liberal norms, and bringing the "splinternet" closer to a reality. Authoritarian regimes will continue to rigorously assert their norms, especially self-censorship, in opposition to free information ecosystems. This will result in more stringent regulation of online communications platforms. Illiberal countries will continue to respond to the demand signal from U.S. nondemocratic partners, adversaries, and even some democratic allies for inexpensive and cutting-edge technology. U.S. mitigation practices suffer diminished efficacy due to bad actors' use of a grab bag of digital tools, along with Russia and China's complementary efforts to accelerate innovation in those two nations. The United States must synthesize a policy response that addresses these emerging and troubling patterns.

At a minimum, the United States must work with like-minded democratic partners to ensure a digital order that preserves and promotes open societies. To do so, the White House should recruit and convene democratic allies—both bilaterally and multilaterally—to build a comprehensive framework that can shape the future digital order.

Whether or not autocrats' digital models prevail on the world stage will be determined in the next decade, and democracies must take an active role now in shaping that result. Reclaiming the digital order for democracy will require a synthesized, dynamic policy response. The United States and its partners should direct their resources and influence toward countries on the brink of imitating the CCP's totalitarian vision, and toward nondemocratic partners tempted by this repressive vision. To counter an ascendent China and its allies of convenience, as well as temper the permissive digital environment for these authoritarians, the United States must invest in unconventional coalitions. There are many potential spoilers in the global contest for digital freedom in the form of undecided nation-states. The courses they chart will determine whether the digital future bends toward a closed world or an open one.

APPENDIX

Countering High-Tech Illiberalism: Events, Products, and Media Engagement

The CNAS Countering High-Tech Illiberalism project is composed of several lines of effort, including Digital Dictators, Digital Freedom Initiative, and Blunting China's Authoritarian Toolkit. Select publications, media features, and public events from these lines of effort are listed here.

Digital Dictators

This initiative aims at understanding the ways autocracies are leveraging technology to their advantage and developing the strategies to respond.

PUBLICATIONS

- "China and Russia's Dangerous Convergence," Andrea Kendall-Taylor and David Shullman, *Foreign Affairs*, May 3, 2021.
- "The Digital Dictators: How Technology Strengthens Autocracy," Andrea Kendall-Taylor, Erica Frantz, and Joseph Wright, *Foreign Affairs*, March/April 2020.
- "Digital Repression in Autocracies," Erica Frantz, Andrea Kendall-Taylor, and Joseph Wright, The Varieties of Democracy Institute Working Papers, March 1, 2020.
- "Digital Authoritarianism: Finding Our Way Out of the Darkness," Naazneen Barma, Brent Durbin, and Andrea Kendall-Taylor, War on the Rocks, February 10, 2020.

MEDIA FEATURES

- "Digital Dictators," Andrea Kendall-Taylor, Center for a New American Security, August 26, 2020.
- "The Rise of Digital Dictators, with Andrea Kendall-Taylor," Andrea Kendall-Taylor on The President's Inbox, a podcast from the Council on Foreign Relations, March 6, 2020.

Digital Freedom Initiative

This effort is dedicated to identifying solutions to protect digital democracy in the United States and abroad by preserving the integrity and value of technologies for free citizens and helping defeat their abuse by malign actors.

PUBLICATIONS

- "Cuba Needs a Free Internet," Richard Fontaine and Kara Frederick, *Foreign Policy*, July 29, 2021.
- "Democracy's Digital Defenses," Richard Fontaine and Kara Frederick, *Wall Street Journal*, May 7, 2021.
- "Democracy by Design: An Affirmative Response to the Illiberal Use of Technology for 2021," Kara Frederick, Center for a New American Security, December 15, 2020.
- "If You Play Videogames, China May Be Spying on You," Dave Aitel and Jordan Schneider, *The Wall Street Journal*, October 28, 2020.
- "The Razor's Edge: Liberalizing the Digital Surveillance Ecosystem," Kara Frederick, Center for a New American Security, September 3, 2020.
- "Beyond TikTok: Preparing for Future Digital Threats," Chris Estep, Kara Frederick and Megan Lamberth, War on the Rocks, August 20, 2020.
- "The Resilience of Sino-Russian High-Tech Cooperation," Samuel Bendett and Elsa B. Kania, War on the Rocks, August 12, 2020.
- "How to Stop China from Imposing Its Values," Anthony Vinci, *The Atlantic*, August 2, 2020.
- "Countering China's Technonationalism," Martijn Rasser, *The Diplomat*, April 24, 2020.
- "The Dangers of Manipulated Media in the Midst of a Crisis," Megan Lamberth, Council on Foreign Relations' Net Politics blog, February 12, 2020.
- "The China Challenge Strategies for Recalibrating the U.S.-China Tech Relationship," Martijn Rasser, Elizabeth Rosenberg, and Paul Scharre, Center for a New American Security, December 12, 2019.
- "Decide, Disrupt, Destroy: Information Systems in Great Power Competition with China," Ainikki Riikonen, *Strategic Studies Quarterly*, November 21, 2019.
- "The Rise of Municipal Ransomware," Kara Frederick, *City Journal*, September 3, 2019.

- "The New War of Ideas: Counterterrorism Lessons for the Digital Disinformation Fight," Kara Frederick, Center for a New American Security, June 3, 2019.
- "The Autocrat's New Tool Kit," Richard Fontaine and Kara Frederick, *The Wall Street Journal*, March 15, 2019.

MEDIA FEATURES

- "Is TikTok a Harmless App or a Threat to U.S. Security?" Kara Frederick, *60 Minutes*, November 15, 2020.
- "How TikTok Could Be Used for Disinformation and Espionage," Kara Frederick, *60 Minutes*, November 15, 2020.
- "How Corporations and Big Tech Leave Our Data Exposed to Criminals, China, and Other Bad Actors," Kara Frederick, prepared testimony before the Senate Judiciary Committee's Subcommittee on Crime and Terrorism, United States Senate, November 5, 2019.
- "The Low Road: Charting China's Digital Expansion," Kara Frederick, Dan Kliman, and Ely Ratner, Center for a New American Security, September 4, 2019.
- "Counterterrorism Lessons for the Digital Disinformation Fight," Kara Frederick, *Government Matters*, August 19, 2019.
- "Podcast: The Autocrat's New Tool Kit," Richard Fontaine, Kara Frederick, and Paul Scharre, Center for a New American Security, March 15, 2019.

Blunting China's Authoritarian Toolkit

This project focuses on developing a U.S. and allied strategy that will curb China's ability to use digital infrastructure to contravene international standards of freedom and transparency. In so doing, it also seeks to educate democratic stakeholders on the risks that an unchecked China poses.

PUBLICATIONS

- "Advancing a Liberal Digital Order in the Indo-Pacific," Lisa Curtis, Joshua Fitt, and Jake Stokes, Center for a New American Security, September 15, 2020.
- "Designing a U.S. Digital Development Strategy," Siddharth Mohandas, Kristine Lee, Joshua Fitt, and Coby Goldberg, Center for a New American Security, September 10, 2020.
- "To Counter China Online, Regulate Big Tech," Coby Goldberg, World Politics Review, August 26, 2020.
- "'Collective Resilience' Is the Way to Address China Challenge," Eric Sayers and Brad Glosserman, *The Japan Times*, August 14, 2020.
- "The U.S.-China Confrontation Is Not another Cold War. It's Something New." Richard Fontaine and Ely Ratner, *The Washington Post*, July 2, 2020.
- "Dangerous Synergies: Countering Chinese and Russian Digital Influence Operations," Daniel Kliman, Andrea Kendall-Taylor, Kristine Lee, Joshua Fitt, and Carisa Nietsche, Center for a New American Security, May 7, 2020.
- "Forging an Alliance Innovation Base," Daniel Kliman, Ben FitzGerald, Kristine Lee, and Joshua Fitt, Center for a New American Security, March 29, 2020.
- "Rising to the China Challenge: Renewing American Competitiveness in the Indo-Pacific," Ely Ratner, Daniel Kliman, Susanna V. Blume, Rush Doshi, Chris Dougherty, Richard Fontaine, Peter Harrell, Martijn Rasser, Elizabeth Rosenberg, Eric Sayers, Daleep Singh, Paul Scharre, Loren DeJonge Schulman, Neil Bhatiya, Ashley Feng, Joshua Fitt, Megan Lamberth, Kristine Lee, and Ainikki Riikonen, Center for a New American Security, January 28, 2020.
- "Challenging China's Bid for App Dominance," Kristine Lee and Karina Barbesino, Center for a New American Security, January 22, 2020.

MEDIA FEATURES

- "The Low Road: Charting China's Digital Expansion," Kara Frederick, Daniel Kliman, and Ely Ratner, Center for a New American Security, September 4, 2019.
- "China's Power Play: The Role of Congress in Addressing the Belt and Road," Daniel Kliman, prepared testimony before the United States Senate Finance Committee's Subcommittee on International Trade, Customs, and Global Competitiveness, June 12, 2019.

1. Andrew Imbrie, discussion with co-author, August 3, 2020; Saif Khan and Alexander Mann, "AI Chips: What They Are and Why They Matter" (Center for Security and Emerging Technology, April 2020), https://cset.georgetown.edu/wp-content/uploads/CSET-An-AI-Chips-Primer-What-They-Are-and-Why-They-Matter.pdf.

2. Steven Feldstein, *The Rise of Digital Repression: How Technology Is Reshaping Power, Politics, and Resistance*, (New York: Oxford University Press, 2021).

3. Liza Lin and Newley Purnell, "A World With a Billion Cameras Watching You Is Just Around the Corner," *The Wall Street Journal*, December 6, 2019, https://www.wsj.com/articles/a-billion-surveillance-cameras-forecast-to-be-watching-within-two-years-11575565402?mod=hp_listb_pos1; Oliver Philippou, "Video Surveillance Installed Base Report—2019" (Omdia, December 5, 2019), https://technology.ihs.com/607069/video-surveillance-installed-base-report-2019.

4. Paul Triolo and Robert Greene, "Will China Control the Global Internet via its Digital Silk Road?" SupChina, May 8, 2020, https://supchina.com/2020/05/08/will-china-control-the-global-internet-via-its-digital-silk-road/.

5. Jude Blanchette and Jonathan E. Hillman, "China's Digital Silk Road after the Coronavirus" (Center for Strategic and International Studies, April 13, 2020), https://www.csis.org/analysis/chinas-digital-silk-road-after-coronavirus.

6. Nadège Rolland, "China's Vision for a New World Order," NBR Special Report No. 23 (National Bureau of Asian Research, January 27, 2020), https://www.nbr.org/wp-content/uploads/pdfs/publications/sr83_chinasvision_jan2020.pdf.

7. Chris Erasmus, "Chinese Experts Train Crime-Hardened Police of South Africa's Biggest City," *South China Morning Post*, September 3, 2019, https://www.scmp.com/news/world/africa/article/3025494/chinese-experts-train-crime-hardened-police-south-africas-biggest; Deng Xiaoci and Zhang Dan, "Beijing Police Working with Foreign Counterparts and Interpol to Hunt Down Fugitives," *Global Times*, April 28, 2019, http://www.globaltimes.cn/content/1147860.shtml; and Danielle Cave, Fergus Ryan, and Vicky Xiuzhong Xu, "Mapping More of China's Tech giants: AI and Surveillance" (Australian Strategic Policy Institute, November 28, 2019), https://www.aspi.org.au/report/mapping-more-chinas-tech-giants.

8. Freedom House, "Freedom in the World 2019: Democracy in Retreat" (Freedom House, 2019), https://freedomhouse.org/sites/default/files/Feb2019_FH_FITW_2019_Report_ForWeb-compressed.pdf.

9. "Remarks by the President in Address on China and the National Interest," The White House Office of the Press Secretary, press release, October 24, 1997, https://clinton-whitehouse4.archives.gov/WH/New/html/19971024-3863.html.

10. Yaqiu Wang, "In China, the 'Great Firewall' Is Changing a Generation," *Politico*, September 1, 2020, https://www.politico.com/news/magazine/2020/09/01/china-great-firewall-generation-405385.

11. Paul Mozur, "Coronavirus Outrage Spurs China's Internet Police to Action," *The New York Times,* March 16, 2020, https://www.nytimes.com/2020/03/16/business/china-coronavirus-internet-police.html.

12. Tamara Khandaker, "The WeChat factor," Vice, February 1, 2019, https://www.vice.com/en_ca/article/zmana5/experts-say-we-should-watch-out-for-wechats-influence-in-canadas-election.

13. Isobel Asher Hamilton, "WeChat Users in the U.S. Say the App Is Censoring Their Messages about Hong Kong," Business Insider, November 26, 2019, https://www.businessinsider.com/us-wechat-users-censored-messages-hong-kong-china-2019-11.

14. Abby Ohlheiser, "Welcome to TikTok's Endless Cycle of Censorship and Mistakes," *MIT Technology Review*, July 13, 2021, https://www.technologyreview.com/2021/07/13/1028401/tiktok-censorship-mistakes-glitches-apologies-endless-cycle/.

15. Jason Slotkin, "Zoom Acknowledges It Suspended Activists' Accounts at China's Request," NPR, June 12, 2020, https://www.npr.org/2020/06/12/876351501/zoom-acknowledges-it-suspended-activists-accounts-at-china-s-request.

16. Jack Nicas, "Apple Removes App That Helps Hong Kong Protesters Track the Police," *The New York Times*, October 9, 2019, https://www.nytimes.com/2019/10/09/technology/apple-hong-kong-app.html.

17. Mark Gurman, "Apple Pulls Taiwanese Flag Emoji From iPhones in Hong Kong," Bloomberg, October 8, 2019, https://www.bloomberg.com/news/articles/2019-10-08/apple-pulls-taiwanese-flag-emoji-from-iphones-in-hong-kong.

18. Sarah Cook, "Beijing's Global Megaphone: The Expansion of Chines Communist Party Media Influence Since 2017" (Freedom House, 2020), https://freedomhouse.org/report/special-report/2020/beijings-global-megaphone.

19. Liu Yunshan, "Huigu Yu Zhanwang" [Seeking truth: review and outlook], QSTheory, June 22, 2009, https://web.archive.org/web/20110120200108/http://www.qstheory.cn/zxdk/2009/200901/200906/t20090609_1625.htm.

20. Anne-Marie Brady, "Authoritarianism Goes Global (II): China's Foreign Propaganda Machine," *Journal of Democracy*, 26 no. 4 (October 2015), 51–59.

21. "Ba Wangshang Yulun Gongzuo Zuowei Xuanchuan Sixiang Gongzuo De Zhongzhongzhizhong" [Make online public opinion work the top priority of propaganda and ideological work], CPCNews, October 31, 2013, http://theory.people.com.cn/n/2013/1031/c40537-23387807.html.

22. Elsa Kania, Samm Sacks, Paul Triolo, and Graham Webster, "China's Strategic Thinking on Building Power in Cyberspace," New America, September 25, 2017, https://www.newamerica.org/cybersecurity-initiative/blog/chinas-strategic-thinking-building-power-cyberspace/.

23. I-fan Lin, "Made-in-China Fake News Overwhelms Taiwan," Global Voices Advox, November 30, 2018, https://advox.globalvoices.org/2018/11/30/made-in-china-fake-news-overwhelms-taiwan/; Freedom House, "China Attempts to Influence Taiwan Elections through Social Media," China Media Bulletin No. 135, April 24, 2019, https://freedomhouse.org/report/china-media-bulletin/china-media-bulletin-student-indoctrination-surveillance-innovation.

24. For more on the topic of digital influence operations and how the tactics of Beijing and Moscow are converging, see Daniel Kliman, Andrea Kendall-Taylor, and Kristine Lee et al., "Dangerous Synergies: Countering Chinese and Russian Digital Influence Operations" (Center for a New American Security, May 7, 2020), https://www.cnas.org/publications/reports/dangerous-synergies.

25. Dan Levin, "Chinese-Canadians Fear China's Rising Clout Is Muzzling Them," *The New York Times*, August 27, 2016, https://www.nytimes.com/2016/08/28/world/americas/chinese-canadians-china-speech.html.

26. Paul Bischoff, "Surveillance Camera Statistics: Which Cities Have the Most CCTV Cameras?" Comparitech, July 22, 2020, https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/.

27. Holly Chik, "China Is Home to 18 of the 20 Most Surveilled Cities in the World," Inkstone, July 27, 2020, https://www.inkstonenews.com/society/china-home-18-20-most-surveilled-cities-world/article/3094805?utm_source=twitter&utm_medium=social&utm_content=article; Bischoff, "Surveillance Camera Statistics: Which Cities Have the Most CCTV Cameras?"

28. Jeffrey Ding, "ChinAI #82: State Grid—A Hidden Giant in AI?" ChinAI Newsletter, February 9, 2020, https://chinai.substack.com/p/chinai-82-state-grid-a-hidden-giant.

29. Matt Sheehan, "How China's Massive AI Plan Actually Works," MacroPolo, February 12, 2018, https://macropolo.org/analysis/how-chinas-massive-ai-plan-actually-works/; Graham Webster, Rogier Creemers, Paul Triolo, and Elsa Kania, "China's Plan to 'Lead' in AI: Purpose, Prospects, and Problems," New America, August 1, 2017, https://www.newamerica.org/cybersecurity-initiative/blog/chinas-plan-lead-ai-purpose-prospects-and-problems/.

30. Jeffrey Ding, "ChinAI #48: Year 1 of Chinai," ChinAI Newsletter, April 1, 2019, https://chinai.substack.com/p/chinai-48-year-1-of-chinai.

31. Cave, Ryan, and Xu, "Mapping More of China's Tech Giants."

32. Charles Rollet, "In China's Far West, Companies Cash in on Surveillance Program That Targets Muslims," *Foreign Policy*, June 13, 2018, https://foreignpolicy.com/2018/06/13/in-chinas-far-west-companies-cash-in-on-surveillance-program-that-targets-muslims/.

33. "IDC Releases China Video Surveillance Equipment Tracker Report: AI & 5G Bring Video Surveillance to a New Era," EMSNow, September 23, 2019, https://emsnow.com/idc-releases-china-video-surveillance-equipment-tracker-report-ai-5g-bring-video-surveillance-to-a-new-era/.

34. Bernard Marr, "Meet the World's Most Valuable AI Startup: China's SenseTime," *Forbes*, June 17, 2019, https://www.forbes.com/sites/bernardmarr/2019/06/17/meet-the-worlds-most-valuable-ai-startup-chinas-sensetime/#a078172309fc; Narayanan Somasundaram, "Chinese AI Startup SenseTime Resumes Push for $2bn Hong Kong IPO," *Nikkei Asia*, June 18, 2021, https://asia.nikkei.com/Business/China-tech/Chinese-AI-startup-SenseTime-resumes-push-for-2bn-Hong-Kong-IPO; and Parmy Olson, "SoftBank Backs Facial-Recognition Startup Despite Privacy Concerns," *The Wall Street Journal*, July 7, 2021, https://www.wsj.com/articles/softbank-backs-facial-recognition-startup-despite-privacy-concerns-11625650539.

35. Mara Hvistendahl, "How a Chinese AI Giant Made Chatting—and Surveillance—Easy," *Wired*, May 18, 2020, https://www.wired.com/story/iflytek-china-ai-giant-voice-chatting-surveillance/.

36. Jeffrey Ding, "Deciphering China's AI Dream" (University of Oxford, March 2018), https://www.fhi.ox.ac.uk/wp-content/uploads/Deciphering_Chinas_AI-Dream.pdf; Andrew Browne, "China Uses 'Digital Leninism' to Manage Economy and Monitor Citizens," *The Wall Street Journal*, October 17, 2017, https://www.wsj.com/articles/xi-jinping-leads-china-into-big-data-dictatorship-1508237820.

37. Adrian Shahbaz, "The Rise of Digital Authoritarianism: Freedom on the Net 2018" (Freedom House, October 31, 2018), https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism; Daniel Kliman, Rush Doshi, Kristine Lee, and Zach Cooper, "Grading China's Belt and Road" (Center for a New American Security, April 8, 2019), https://www.cnas.org/publications/reports/beltandroad.

38. Cave, Ryan, and Xu, "Mapping More of China's Tech Giants."

39. "Zhongguo-Dongmeng Wangluo Anquan Chanye Fazhan Xianzhuang Yanjiu Baogao," research report on current developments of China-ASEAN cybersecurity industry (China Academy for Information and Communications, December 2019), http://www.caict.ac.cn/kxyj/qwfb/bps/201912/P020191228471585415832.pdf.

40. "Broadband Forum to Develop ICT in Laos," *The Nation Thailand*, December 1, 2016, https://www.nationthailand.com/Startup_and_IT/30301275.

41. Allie Funk, "Internet Freedom in Asia Hits Unprecedented Low" (Freedom House, December 2, 2019), https://freedomhouse.org/article/internet-freedom-asia-hits-unprecedented-low.

42. International Strategy of Cooperation on Cyberspace, Chapter III: "Strategic Goals," Xinhua, March 1, 2017, http://www.xinhuanet.com/english/china/2017-03/01/c_136094371_3.htm.

43. Broadband Commission for Sustainable Development, Mr. Houlin Zhao, Secretary-General, ITU, Co-Vice Chair of Commission (bio), https://www.broadbandcommission.org/commissioners/Pages/zhao.aspx.

44. Madhumita Murgia and Anna Gross, "Inside China's Controversial Mission to Reinvent the Internet," *Financial Times*, March 27, 2020, https://www.ft.com/content/ba94c2bc-6e27-11ea-9bca-bf503995cd6f.

45. James Andrew Louis, "Can Telephones Race? 5G and the Evolution of Telecom" (Center for Strategic and International Studies, June 15, 2020), https://www.csis.org/analysis/can-telephones-race-5g-and-evolution-telecom; Frank Hersey, "Lenovo Founder in Public Backlash for 'Unpatriotic 5G Standards Vote,'" Technode, May 16, 2018, https://technode.com/2018/05/16/lenovo-huawei-5g/.

46. Anna Gross, Madhumita Murgia, and Yuan Yang, "Chinese Tech Groups Shaping UN Facial Recognition Standards," *Financial Times*, December 1, 2019, https://www.ft.com/content/c3555a3c-0d3e-11ea-b2d6-9bf4d1957a67.

47. Jeffrey Ding, Paul Triolo, and Samm Sacks, "Chinese Interests Take a Big Seat at the AI Governance Table," New America, June 20, 2018, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinese-interests-take-big-seat-ai-governance-table/.

48. John Hurley, Scott Morris, and Gailyn Portelance, "Examining the Debt Implications of the Belt and Road Initiative from a Policy Perspective," CGD Policy Paper No. 121 (Center for Global Development, March 2018), https://www.cgdev.org/sites/default/files/examining-debt-implications-belt-and-road-initiative-policy-perspective.pdf; Jonathan E. Hillman, "Corruption Flows Along China's Belt and Road" (Center for Strategic and International Studies, January 18, 2019), https://www.csis.org/analysis/corruption-flows-along-chinas-belt-and-road.

49. "Belt and Road Cooperation: Shaping a Brighter Shared Future," *China Daily*, April 28, 2019, http://124.127.52.76/a/201904/28/WS5cc4fa20a3104842260b8cf7_5.html.

50. "The Belt and Road Initiative: Progress, Contributions and Prospects," Permanent Mission of the People's Republic of China to the United Nations Office at Geneva and other International Organizations in Switzerland, http://www.china-un.ch/eng/zywjyjh/t1675564.htm.

51. Paul Triolo, Kevin Allison, and Clarise Brown, "The Digital Silk Road: Expanding China's Digital Footprint" (Eurasia Group, April 29, 2020), https://www.eurasiagroup.net/live-post/digital-silk-road-expanding-china-digital-footprint.

52. Paul Triolo and Robert Greene, "Will China Control the Global Internet via its Digital Silk Road?" SupChina, May 8, 2020, https://supchina.com/2020/05/08/will-china-control-the-global-internet-via-its-digital-silk-road/.

53. Kania, Sacks, Triolo, and Webster, "China's Strategic Thinking on Building Power in Cyberspace."

54. This framing section includes analysis and language that originated in Daniel Kliman, then–Senior Fellow and Director, Asia-Pacific Security Program, Center for a New American Security, "China's Power Play: The Role of Congress in Addressing the Belt and Road," Statement to the Subcommittee on International Trade, Customs, and Global Competitiveness, Committee on Finance, U.S. Senate, June 12, 2019, https://www.finance.senate.gov/download/06122018-kliman-testimony&download=1; Daniel Kliman, Senior Fellow and Director, Asia-Pacific Security Program, Center for a New American Security, "Addressing China's Influence in Southeast Asia: America's Approach and the Role of Congress," Statement to the Subcommittee on Asia, the Pacific, and Nonproliferation, Committee on Foreign Affairs, U.S. House of Representatives, May 8, 2019, https://s3.amazonaws.com/files.cnas.org/documents/Daniel-Kliman_Final-Testimony-for-HFAC-Subcommittee-on-Asia-the-Pacific-and-Nonproliferation-min.pdf?mtime=20190508124206.

55. "Safe cities" is sometimes translated as "smart cities," depending on the specific name of the initiative. This report remains faithful to the direct translation of each individual project. Bob Koigi, "Huawei Launches Safe City Project to Tackle Africa Customers' Security Needs," Africa Business Communities, October 19, 2016, https://africabusinesscommunities.com/news/huawei-launches-safe-city-project-to-tackle-africa-customers-security-needs.html; "Huawei Holds Safe City Africa Summit in Case Town," Huawei News, April 29, 2015, https://www.huawei.com/us/news/2015/04/hw_425413; Juan Pedro Tomás, "Huawei, Dubai Police to Develop Safe City Innovation Center," Enterprise IoT Insights, October 21, 2016, https://enterpriseiotinsights.com/20161021/channels/news/huawei-dubai-police-develop-safe-city-innovation-center; and "Inside Huawei's Bandung Safe City Project with Telkom Indonesia," Telecom Asia, April 15, 2016, https://www.telecomasia.net/content/inside-huaweis-bandung-safe-city-project-telkom-indonesia.

56. Diana Adams, "Real Life Huawei Collaborative Smart City and Safe City Solution in Action," Medium, November 15, 2017, https://medium.com/@adamsconsulting/real-life-huawei-collaborative-smart-city-and-safe-city-solution-in-action-e340657d89f0.

57. Cave, Ryan, and Xu, "Mapping More of China's Tech Giants."

58. Steven Feldstein, "The Global Expansion of AI Surveillance" (Carnegie Endowment for International Peace, September 17, 2019), https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847.

59. "Zhongguo-Dongmeng Wangluo Anquan Chanye Fazhan Xianzhuang Yanjiu Baogao," research report.

60. Feldstein, "The Global Expansion of AI Surveillance," 15.

61. Lynsey Chutel, "China Is Exporting Facial Recognition Software to Africa, Expanding Its Vast Database," Quartz, May 25, 2018, https://qz.com/africa/1287675/china-is-exporting-facial-recognition-to-africa-ensuring-ai-dominance-through-diversity/.

62. Li Tao, "Malaysian Police Wear Chinese Start-Up's AI Camera to Identify Suspected Criminals," *South China Morning Post*, April 20, 2018, https://www.scmp.com/tech/social-gadgets/article/2142497/malaysian-police-wear-chinese-start-ups-ai-camera-identify.

63. Cave, Ryan, and Xu, "Mapping More of China's Tech Giants. "Addition of Certain Entities to the Entity List," *Federal Register*, October 9, 2019, https://www.federalregister.gov/documents/2019/10/09/2019-22210/addition-of-certain-entities-to-the-entity-list.

64. "Addition of Certain Entities to the Entity List; Revision of Existing Entries on the Entity List," *Federal Register*, June 5, 2020, https://www.federalregister.gov/documents/2020/06/05/2020-10868/addition-of-certain-entities-to-the-entity-list-revision-of-existing-entries-on-the-entity-list.

65. Andrew Kitson and Kenny Liew, "China Doubles Down on Its Digital Silk Road" (Center for Strategic and International Studies, November 14, 2019) https://reconnectingasia.csis.org/analysis/entries/china-doubles-down-its-digital-silk-road/.

66. Douglas Main, "Undersea Cables Transport 99 Percent of International Data," *Newsweek*, April 2, 2015, https://www.newsweek.com/undersea-cables-transport-99-percent-international-communications-319072.

67. Jonathan Hillman, "War and PEACE on China's Digital Silk Road" (Center for Strategic and International Studies, May 16, 2019), https://www.csis.org/analysis/war-and-peace-chinas-digital-silk-road.

68. James Stavridis, "China's Next Naval Target Is the Internet's Underwater Cables," Bloomberg, April 8, 2019, https://www.bloomberg.com/opinion/articles/2019-04-09/china-spying-the-internet-s-underwater-cables-are-next.

69. Dave Gershgorn, "In Just 6 Months, 'Fever Cameras' Have Become a Full-Fledged Industry," Medium, July 20, 2020, https://onezero.medium.com/in-just-6-months-fever-cameras-have-become-a-full-fledged-industry-ab8ef4a5648c.

70. Blanchette and Hillman, "China's Digital Silk Road after the Coronavirus."

71. Sheena Chestnut Greitens, "Dealing with Demand for China's Global Surveillance Exports" (Brookings Institution, April 2020), https://www.brookings.edu/research/dealing-with-demand-for-chinas-global-surveillance-exports/.

72. Nyshka Chandran, "Alibaba's 'Digital Free Trade Zone' Has Some Worried about China Links to Malaysia," CNBC, February 12, 2018, https://www.cnbc.com/2018/02/12/concerns-over-alibaba-led-digital-free-trade-zone-in-malaysia.html.

73. Jenne Lajiun, "Five MoUs Signed during Malaysia-China Meeting," *The Borneo Post*, June 15, 2019, https://www.theborneopost.com/2019/06/15/five-mous-signed-during-malaysia-china-meeting/.

74. Samm Sacks, "Beijing Wants to Rewrite the Rules of the Internet," *The Atlantic*, June 18, 2018, https://www.theatlantic.com/international/archive/2018/06/zte-huawei-china-trump-trade-cyber/563033/.

75. George Ogola, "The Threats to Media Freedom Are Getting More Sophisticated in Africa's Digital Age," Quartz, October 4, 2018, https://qz.com/africa/1412973/african-governments-are-blocking-social-media-or-taxing-it/.

76. Ogola, "The Threats to Media Freedom Are Getting More Sophisticated in Africa's Digital Age."

77. Sacks, "Beijing Wants to Rewrite the Rules of the Internet."

78. Gross, Murgia, and Yang, "Chinese Tech Groups Shaping UN Facial Recognition Standards."

79. Emeka Umejei, "The Imitation Game: Will China's Investments Reshape Africa's Internet?" Power 3.0, December 6, 2018, https://www.power3point0.org/2018/12/06/the-imitation-game-will-chinas-investments-reshape-africas-internet/.

80. "Mapping Trends in Government Internet Controls, 1999–2019" (Collaboration on International ICT Policy for East and Southern Africa, September 2019), https://cipesa.org/?wpfb_dl=307.

81. Jaclyn Kerr, "The Russian Model of Digital Control and Its Significance," in *Artificial Intelligence, China, Russia, and the Global Order*, ed. Nicholas D. Wright (Maxwell AFB, AL: Air University Press, 2019), 70, https://www.airuniversity.af.edu/Portals/10/AUPress/Books/B_0161_WRIGHT_ARTIFICIAL_INTELLIGENCE_CHINA_RUSSIA_AND_THE_GLOBAL_ORDER.PDF; Alina Polyakova, "Russia Is Teaching the World to Spy," *The New York Times*, December 5, 2019, https://www.nytimes.com/2019/12/05/opinion/russia-hacking.html.

82. Keith Dear, "Will Russia Rule the World Through AI?" *The RUSI Journal*, 164 no. 5–6 (November 2019), 36–60.

83. Radina Gigova, Who Vladimir Putin Thinks Will Rule the World," CNN, 2 September 2017, https://www.cnn.com/2017/09/01/world/putin-artificial-intelligence-will-rule-world/index.html.

84. Gigova, Who Vladimir Putin Thinks Will Rule the World."

85. Larry Lewis, "Russian Kryptonite to Western Hi-Tech Dominance," Center for Autonomy and AI blog (CNA), July 18, 2018, https://caai.blog/2018/07/18/russian-kryptonite-to-western-hi-tech-dominance/.

86. "Russia Is 'Ready' to Disconnect from Global Internet, Medvedev Says," *The Moscow Times*, February 1, 2021, https://www.themoscowtimes.com/2021/02/01/russia-is-ready-to-disconnect-from-global-internet-medvedev-says-a72791.

87. "Russia Is a 'Distinct Civilization,' Putin Says," *The Moscow Times*, May 18, 2020, https://www.themoscowtimes.com/2021/02/01/russia-is-ready-to-disconnect-from-global-internet-medvedev-says-a72791.

88. Andrei Tsygankov, "Crafting the State-Civilization Vladimir Putin's Turn to Distinct Values," *Problems of Post-Communism*, 63 no. 3 (April 2016), 146–58, https://www.tandfonline.com/doi/abs/10.1080/10758216.2015.1113884.

89. Ewen MacAskill, "Putin Calls Internet a 'CIA Project' Renewing Fears of Web Breakup," *The Guardian*, April 24, 2014, https://www.theguardian.com/world/2014/apr/24/vladimir-putin-web-breakup-internet-cia.

90. Denis Stukal, Sergey Sanovich, Richard Bonneau, and Joshua A. Tucker, "Bots for Autocrats: How Pro-Government Bots Fight Opposition in Russia," http://www.denisstukal.com/uploads/8/4/7/0/84708866/stukal_et_al__2020__bots_for_autocrats.pdf.

91. Robert Morgus, "The Spread of Russia's Digital Authoritarianism," in *Artificial Intelligence, China, Russia, and the Global Order*, ed. Nicholas D. Wright, 89–97, Air University Press, https://www.airuniversity.af.edu/Portals/10/AUPress/Books/B_0161_WRIGHT_ARTIFICIAL_INTELLIGENCE_CHINA_RUSSIA_AND_THE_GLOBAL_ORDER.PDF.

92. "Russia: Growing Internet Isolation, Control, Censorship," Human Rights Watch, June 18, 2020, https://www.hrw.org/news/2020/06/18/russia-growing-internet-isolation-control-censorship#.

93. Kat Lonsdorf, "Social Media Fueled Russian Protests despite Government Attempts to Censor," NPR, January 24, 2021, https://www.npr.org/2021/01/24/960113653/social-media-fueled-russian-protests-despite-government-attempts-to-censor.

94. Michael Birnbaum, "Russian Blogger Law Puts New Restrictions on Internet Freedoms," *The Washington Post*, July 31, 2014, https://www.washingtonpost.com/world/russian-blogger-law-puts-new-restrictions-on-internet-freedoms/2014/07/31/42a05924-a931-459f-acd2-6d08598c375b_story.html; Neil MacFarquhar, "Russia Quietly Tightens Reins on Web with 'Bloggers Law,'" *The New York Times*, May 6, 2014, https://www.nytimes.com/2014/05/07/world/europe/russia-quietly-tightens-reins-on-web-with-bloggers-law.html.

95. "Online and on All Fronts: Russia's Assault on Freedom of Expression," Human Rights Watch, July 18, 2017, https://www.hrw.org/report/2017/07/18/online-and-all-fronts/russias-assault-freedom-expression#.

96. Alina Polyakova and Chris Meserole, "Exporting Digital Authoritarianism: The Russian and Chinese Models" (Brookings Institution, August 2019), 6, https://www.brookings.edu/research/exporting-digital-authoritarianism/.

97. Polyakova and Meserole, "Exporting Digital Authoritarianism: The Russian and Chinese Models," 8.

98. Shannon von Sant, "Russia Criminalizes the Spread of Online News Which 'Disrespects' the Government," NPR.org, March 18, 2019, https://www.npr.org/2019/03/18/704600310/russia-criminalizes-the-spread-of-online-news-which-disrespects-the-government.

99. Polyakova and Meserole, "Exporting Digital Authoritarianism: The Russian and Chinese Models," 9.

100. "The Fake News 'Infodemic': The Fight against Coronavirus As a Threat to Freedom of Speech," Agora International Human Rights Group, https://agora.legal/fs/a_delo2doc/196_file__ENG_final.pdf.

101. Margarita Konaev and James Dunham, "Russian AI Research 2010–2018" (Center for Security and Emerging Technology, October 2020), 13, https://cset.georgetown.edu/publication/russian-ai-research-2010-2018/.

102. Elizaveta Focht, "Internet during Rallies in Moscow Could Be Jammed at the Request of Security Officials" [in Russian],BBC, August 6, 2019, https://www.bbc.com/russian/features-49255791; Zak Doffman, "Russian Authorities 'Secretly' Shut Down Moscow's Mobile Internet:

Report," *Forbes*, August 8, 2019, https://www.forbes.com/sites/zakdoffman/2019/08/08/russian-security-agencies-secretly-shut-moscows-mobile-internet-to-control-protestors-report/; "Authorities Jammed Moscow's Mobile Internet during Opposition Protests," *The Moscow Times*, August 7, 2019, https://www.themoscowtimes.com/2019/08/07/authorities-jammed-moscows-mobile-internet-during-opposition-protests-ngo-a66741; and "Alexei Navalny: 'More than 3,000 Detained' in Protests across Russia," BBC News, January 23, 2021, https://www.bbc.com/news/world-europe-55778334.

103. Polyakova and Meserole, "Exporting Digital Authoritarianism: The Russian and Chinese Models," 7; Alena Epifanova, "Deciphering Russia's 'Sovereign Internet Law,'" DGAP Analysis No. 2 (German Council on Foreign Relations, January 2020), https://dgap.org/sites/default/files/article_pdfs/dgap-analyse_2-2020_epifanova_0.pdf.

104. "Russia: Growing Internet Isolation, Control, Censorship."

105 "Russia's 'Big Brother' Law Enters into Force," *The Moscow Times*, July 1, 2018, https://www.themoscowtimes.com/2018/07/01/russias-big-brother-law-enters-into-force-a62066.

106. Shaun Walker, "Russia Blocks Access to LinkedIn over Foreign-Held Data," *The Guardian*, November 17, 2016, https://www.theguardian.com/world/2016/nov/17/russia-blocks-access-to-linkedin-over-foreign-held-data.

107. "Putin Signs Law Forcing Foreign Social Media Giants to Open Russian Offices," Reuters, July 1, 2001, https://www.reuters.com/technology/putin-signs-law-forcing-foreign-it-firms-open-offices-russia-2021-07-01/.

108. "Russia Fines Google Again for Failing to Remove Banned Content," Reuters, August 19, 2021, https://www.reuters.com/technology/russia-fines-google-further-26989-failing-remove-banned-content-2021-08-19/.

109. Polyakova and Meserole, "Exporting Digital Authoritarianism: The Russian and Chinese Models," 9–10.

110. "Russia's Digital Development Ministry Wants to Ban the Latest Encryption Technology from the RuNet," Meduza, September 21, 2020, https://meduza.io/en/feature/2020/09/22/russia-s-digital-development-ministry-wants-to-ban-the-latest-encryption-technologies-from-the-runet.

111. Adrian Chen, "The Agency," *The New York Times*, June 2, 2015, https://www.nytimes.com/2015/06/07/magazine/the-agency.html; Morgus, "The Spread of Russia's Digital Authoritarianism," 85.

112. Kerr, "The Russian Model of Digital Control and Its Significance," 55.

113. See, for example, the extensive work conducted by the German Marshall Fund's Alliance for Securing Democracy and the Atlantic Council's Digital Forensic Research Lab. See also CNAS's report "Dangerous Synergies: Countering Chinese and Russian Digital Influence Operations," for more on the convergence of Russian and Chinese information operations; Daniel Kliman et al., "Dangerous Synergies: Countering Chinese and Russian Digital Influence Operations," (CNAS, May 2020), https://www.cnas.org/publications/reports/dangerous-synergies.

114. "It's Getting Harder to Spot a Deep Fake Video," Bloomberg QuickTake, September 27, 2018, YouTube video, https://www.youtube.com/watch?v=gLoI9hAX9dw.

115. Vladimir Gelman, "Brave Digital World: Alternatives for Russia," *The Moscow Times*, May 1, 2019, https://www.themoscowtimes.com/2019/05/01/brave-digital-world-alternatives-for-russia-a65452.

116. Paul Goble, "Video Facial Recognition Technology Used to Make Arrests after January 23 Navalny Protest," Window on Eurasia, January 31, 2021, https://windowoneurasia2.blogspot.com/2021/01/video-facial-recognition-technology.html.

117. Goble, "Video Facial Recognition Technology Used to Make Arrests after January 23 Navalny Protest."

118. Matthew Luxmoore, "Yes, Big Brother IS Watching: Russian Schools Getting Surveillance Systems Called 'Orwell,'" Radio Free Europe/Radio Liberty, June 17, 2020, https://www.rferl.org/a/russian-schools-getting-surveillance-systems-called-orwell-/30676184.html; "Russia to Install 'Orwell' Facial Recognition Tech in Every School—Vedomosti," *The Moscow Times*, June 16, 2020, https://www.themoscowtimes.com/2020/06/16/russia-to-install-orwell-facial-recognition-tech-in-every-school-vedomosti-a70585.

119. Felix Light, "Russia Is Building One of the World's Largest Facial Recognition Networks," *The Moscow Times*, November 12, 2019, https://www.themoscowtimes.com/2019/11/12/russia-building-one-of-worlds-largest-facial-recognition-networks-a68139; Felix Light, "Coronavirus Outbreak Is Major Test for Russia's Facial Recognition Network," *The Moscow Times*, March 25, 2020, https://www.themoscowtimes.com/2020/03/25/coronavirus-outbreak-is-major-test-for-russias-facial-recognition-network-a69736.

120. Goble, "Video Facial Recognition Technology Used to Make Arrests after January 23 Navalny Protest." Kristina Foltynova, "We See You! How Russia Is Developing a Video Surveillance System" [in Russian], Idel Reality, https://www.idelreal.org/a/31076237.html.

121. Light, "Russia Is Building One of the World's Largest Facial Recognition Networks."

122. Peter Podkopaev, "On Social Control, the Kremlin's Reach May Exceed Its Grasp" (Freedom House, July 8, 2020), https://freedomhouse.org/article/social-control-krem-

lins-reach-may-exceed-its-grasp.

123. Light, "Russia Is Building One of the World's Largest Facial Recognition Networks."

124. Patrick Reevell, "How Russia Is Using Facial Recognition to Police Its Coronavirus Lockdown," ABC News, April 30, 2020, https://abcnews.go.com/International/russia-facial-recognition-police-coronavirus-lockdown/story?id=70299736.

125. "Moscow Authorities Intend to Collect Personal Data of Employees of Moscow Companies through Employers" [in Russian], D-Russia, August 10, 2020, https://d-russia.ru/vlasti-moskvy-namereny-cherez-rabotodatelej-sobirat-personalnye-dannye-sotrudnikov-moskovskih-kompanij.html.

126. Anastasiia Zlobina, "Moscow Government Collects Employees Data without Consent," Human Rights Watch, October 13, 2020, https://www.hrw.org/news/2020/10/13/moscow-government-collects-employees-data-without-consent.

127. Office of the President of the Russian Federation, *Decree of the President of the Russian Federation on the Development of Artificial Intelligence in the Russian Federation*, October 10, 2019, https://cset.georgetown.edu/wp-content/uploads/Decree-of-the-President-of-the-Russian-Federation-on-the-Development-of-Artificial-Intelligence-in-the-Russian-Federation-.pdf.

128. Samuel Bendett, "Russia's AI Quest Is State-Driven—Even More Than China's. Can It Work?" Defense One, November 25, 2019, https://www.defenseone.com/ideas/2019/11/russias-ai-quest-state-driven-even-more-chinas-can-it-work/161519/.

129. Bendett, "Russia's AI Quest Is State-Driven—Even More Than China's. Can It Work?"; Samuel Bendett, "Putin Seeks to Plug Gaps in Russia's State-Driven Tech Efforts," Defense One, January 18, 2020, https://www.defenseone.com/technology/2020/01/putin-calls-more-hi-tech-breakthroughs/162496/.

130. Lewis, "Russian Kryptonite to Western Hi-Tech Dominance."

131. Morgus, "The Spread of Russia's Digital Authoritarianism," 88.

132. MacAskill, "Putin Calls Internet a 'CIA Project' Renewing Fears of Web Breakup." "Big Points Buried in the U.S. Cyberwar Strategy" [in Chinese], Xinhua, April 7, 2015, http://news.xinhuanet.com/zgjx/2015-04/07/c_134128303.htm.

133. Adam Segal, "Peering into the Future of Sino-Russian Cybersecurity Cooperation," War on the Rocks, August 10, 2020, https://warontherocks.com/2020/08/peering-into-the-future-of-sino-russian-cyber-security-cooperation/; U.N. General Assembly, 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, A/69/723 (July 22, 2015), https://digitallibrary.un.org/record/786846/files/A_69_723-EN.pdf.

134. MacAskill, "Putin Calls Internet a 'CIA Project' Renewing Fears of Web Breakup." "Big Points Buried in the U.S. Cyberwar Strategy."

135. Andrei Soldatov and Irina Borogan, *The Red Web: The Struggle between Russia's Digital Dictators and the New Online Revolutionaries* (New York: PublicAffairs, 2015), 223.

136. Segal, "Peering into the Future of Sino-Russian Cybersecurity Cooperation."

137. U.N. General Assembly, letter dated 9 January 2015, from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan, A/69/723.

138. Alex Grigsby, "Will China and Russia's Updated Code of Conduct Get More Traction in a Post-Snowden Era?" (Council on Foreign Relations, January 28, 2015), https://www.cfr.org/blog/will-china-and-russias-updated-code-conduct-get-more-traction-post-snowden-era.

139. U.N. General Assembly, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/70/174 (July 22, 2015), http://undocs.org/A/70/174.

140. Segal, "Peering into the Future of Sino-Russian Cybersecurity Cooperation."

141. Ellen Nakashima, "The U.S. Is Urging a No Vote on a Russian-Led U.N. Resolution Calling for a Global Cybercrime Treaty," *The Washington Post*, November 16, 2019, https://www.washingtonpost.com/national-security/the-us-is-urging-a-no-vote-on-a-russian-led-un-resolution-calling-for-a-global-cybercrime-treaty/2019/11/16/b4895e76-075e-11ea-818c-fcc65139e8c2_story.html.

142. Epifanova, "Deciphering Russia's 'Sovereign Internet Law.'"

143. Morgus, "The Spread of Russia's Digital Authoritarianism," 88.

144. "Declaration of the 5th BRICS Communications Ministers Meeting," Brasilia, August 14, 2019 (BRICS Information Centre, University of Toronto), http://www.brics.utoronto.ca/docs/190814-communications.html; "BRICS Civil Forum 2020. Mikhail Petrosyan: 'BRICS Countries Show High Digital Ambitions,'" BRICS Russia, September 28, 2020 (BRICS Summit, 17 November 2020), https://eng.brics-russia2020.ru/news/20200928/654551/BRICS-Civil-Forum-2020-Mikhail-Petrosyan-BRICS-

countries-show-high-digital-ambitions.html; and "BRICS Ministers of Communication Discuss Digital Economy Development and Prospects for BRICS Cooperation in ICTs," BRICS Russia, September 18, 2020 (BRICS Summit, 17 November 2020), https://eng.brics-russia2020.ru/news/20200918/582139/BRICS-Ministers-of-Communication-discuss-digital-economy-development-and-prospects-for-BRICS.html.

145. Andrew Roth, "Russia and China Sign Cooperation Pacts," *The New York Times*, May 8, 2015, https://www.nytimes.com/2015/05/09/world/europe/russia-and-china-sign-cooperation-pacts.html; Sean Lyngaas, "Debating the Sino-Russian Cyber Pact," *Federal Computer Week*, May 12, 2015, https://fcw.com/articles/2015/05/12/russian-chinese-cyber.aspx.

146. Polyakova, "Russia Is Teaching the World to Spy." Light, "Coronavirus Outbreak Is Major Test for Russia's Facial Recognition Network."

147. Polyakova, "Russia Is Teaching the World to Spy."

148. Polyakova and Meserole, "Exporting Digital Authoritarianism: The Russian and Chinese Models."

149. Podkopaev, "On Social Control, the Kremlin's Reach May Exceed Its Grasp."

150. "Statement by NCSC Director William Evanina: Election Threat Update for the American Public," Office of the Director of National Intelligence, press release, August 7, 2020, https://www.dni.gov/index.php/newsroom/press-releases/item/2139-statement-by-ncsc-director-william-evanina-election-threat-update-for-the-american-public.

151. "The Ministry of Telecom and Mass Communications Postponed Exercises on Runet Stability" [in Russian], *Izvestia*, September 21, 2020, https://iz.ru/1063232/2020-09-21/v-minkomsviazi-otlozhili-ucheniia-po-ustoichivosti-runeta; "Russia Postpones Sovereign Internet Test over Coronavirus," Reuters, March 20, 2020, https://www.reuters.com/article/us-health-coronavirus-russia-internet/russia-postpones-sovereign-internet-test-over-coronavirus-idUSKBN2171J6.

152. "Russia's 'Big Brother' Law Enters Into Force."

153. Light, "Coronavirus Outbreak Is Major Test for Russia's Facial Recognition Network."

154. Dear, "Will Russia Rule the World Through AI?"

155. Bendett, "Russia's AI Quest is State-Driven—Even More than China's. Can It Work?"

156. "Artificial Intelligence in Russia," Occasional Paper No. 9 (CNA Russia Studies Program, August 28, 2020), 1, https://www.cna.org/CNA_files/PDF/DOP-2020-U-027966-Final%20(002).pdf.

157. Freedom House, "Freedom in the World 2020: A Leaderless Struggle for Democracy" (Freedom House, 2020), https://freedomhouse.org/sites/default/files/2020-02/FIW_2020_REPORT_BOOKLET_Final.pdf.

158. Freedom House, "Freedom in the World 2020: A Leaderless Struggle for Democracy."

159. Samuel Woodhams, "Egypt's Arrested Digital Spaces," Middle East Report Online (Middle East Research and Information Project, July 22, 2019), https://merip.org/2019/07/egypts-arrested-digital-spaces/; Sam Kimball, "After Arab Spring, Surveillance in Egypt Intensifies," The Intercept, March 9, 2015, https://theintercept.com/2015/03/09/arab-spring-surveillance-egypt-intensifies/.

160. "Egypt Jails Female TikTok Influencers for Two Years over 'Indecent' Videos," Middle East Eye, July 27, 2020, https://www.middleeasteye.net/news/egypt-tiktok-five-female-influencers-prison-violating-public-morals.

161. "Egypt Jails Female TikTok Influencers for Two Years over 'Indecent' Videos."

162. "Egypt Jails Female TikTok Influencers for Two Years over 'Indecent' Videos."

163. Nadda Osman, "Egypt Censors Media from Reporting on Libya, Sinai, Renaissance Dam and Covid-19," Middle East Eye, June 16, 2020, https://www.middleeasteye.net/news/egypt-media-censors-libya-sinai-renaissance-dam-covid.

164. "Bahrain Vows Greater Crackdown on Online Criticism amid New Arrests," Americans for Democracy & Human Rights in Bahrain, March 30, 2018, https://www.adhrb.org/2018/03/bahrain-vows-greater-crackdown-on-online-criticism-amid-new-arrests/.

165. "Freedom on the Net 2019: Saudi Arabia" (Freedom House), https://freedomhouse.org/country/saudi-arabia/freedom-net/2019.

166. "U.A.E.-Linked Twitter Accounts Urge Crackdown on Israel Peace Deal Critics," The New Arab, August 16, 2020, https://english.alaraby.co.uk/english/news/2020/8/16/uae-linked-accounts-urge-crackdown-on-israel-peace-deal-critics.

167. "Egyptian News Media Warned Not to Criticize U.A.E.-Israel Deal," Al-Monitor, August 27, 2020, https://www.al-monitor.com/pulse/originals/2020/08/egypt-ban-media-criticism-uae-israel-peace-deal.html.

168. Chloe Taylor, "Government-Led Internet Shutdowns Cost the Global Economy $8 Billion in 2019, Research Says," CNBC, January 8, 2020, https://www.cnbc.

com/2020/01/08/government-led-internet-shutdowns-cost-8-billion-in-2019-study-says.html.

169. Farnaz Fassihi, "Iran Blocks Nearly All Internet Access," *The New York Times*, November 17, 2019 (updated December 5, 2019), https://www.nytimes.com/2019/11/17/world/middleeast/iran-protest-rouhani.html.

170. Wil Crisp and Suadad al-Salhy, "Inside Hizbollah's Fake News Training Camps Sowing Instability Across the Middle East," *The Telegraph*, August 2, 2020, https://www.telegraph.co.uk/news/2020/08/02/exclusive-inside-hezbollahs-fake-news-training-camps-sowing/; Emerson T. Brooking and Suzanne Kianpour, "Iranian Digital Influence Efforts: Guerrilla Broadcasting for the Twenty-first Century" (The Atlantic Council, 2020), https://www.atlanticcouncil.org/in-depth-research-reports/report/iranian-digital-influence-efforts-guerrilla-broadcasting-for-the-twenty-first-century/.

171. "Gulf States Urged to Unblock Internet Calls amid Coronavirus Pandemic," The New Arab, April 8, 2020, https://english.alaraby.co.uk/english/news/2020/4/8/gulf-states-urged-to-unblock-internet-calls-amid-coronavirus.

172. "Gulf States Urged to Unblock Internet Calls amid Coronavirus Pandemic."

173. Karen Young and Ellen Nakashima, "U.A.E. Orchestrated Hacking of Qatari Government Sites, Sparking Regional Upheaval, According to U.S. Intelligence Officials," *The Washington Post*, July 16, 2017, https://www.washingtonpost.com/world/national-security/uae-hacked-qatari-government-sites-sparking-regional-upheaval-according-to-us-intelligence-officials/2017/07/16/00c46e54-698f-11e7-8eb5-cbccc2e7bfbf_story.html.

174. Marc Owen Jones, "Saudi, U.A.E. Twitter Takedowns Won't Curb Rampant Disinformation on Arab Twitter," *The Washington Post*, September 25, 2019, https://www.washingtonpost.com/politics/2019/09/25/saudi-uae-twitter-takedowns-wont-curb-rampant-disinformation-arab-twitter/.

175. Jones, "Saudi, U.A.E. Twitter Takedowns Won't Curb Rampant Disinformation on Arab Twitter."

176. Nathaniel Gleicher, "Removing Coordinated Inauthentic Behavior in U.A.E., Egypt and Saudi Arabia," Facebook Newsroom, August 1, 2019, https://about.fb.com/news/2019/08/cib-uae-egypt-saudi-arabia/amp/?__twitter_impression=true.

177. Matthew Levitt, "Hezbollah's Regional Activities in Support of Iran's Proxy Networks" (The Middle East Institute, July 2021), https://www.mei.edu/publications/hezbollahs-regional-activities-support-irans-proxy-networks.

178. Alice Revelli and Lee Foster, "Network of Social Media Accounts Impersonates U.S. Political Candidates, Leverages U.S. and Israeli Media in Support of Iranian Interests," FireEye, May 28, 2019, https://www.fireeye.com/blog/threat-research/2019/05/social-media-network-impersonates-us-political-candidates-supports-iranian-interests.html.

179. Revelli and Foster, "Network of Social Media Accounts Impersonates U.S. Political Candidates, Leverages U.S. and Israeli Media in Support of Iranian Interests."

180. Revelli and Foster, "Network of Social Media Accounts Impersonates U.S. Political Candidates, Leverages U.S. and Israeli Media in Support of Iranian Interests."

181. National Intelligence Council, *Foreign Threats to the 2020 U.S. Federal Elections*, ICA 2020-00078D (March 10, 2021), https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf.

182. Laura Mackenzie, "Surveillance State: How Gulf Governments Keep Watch on Us," *Wired*, January 21, 2021, https://wired.me/technology/privacy/surveillance-gulf-states/.

183. Megha Rajagopalan, "Facial Recognition Technology Is Facing a Huge Backlash in the U.S., but Some of the World's Biggest Tech Companies Are Trying to Sell It in the Gulf," *Buzzfeed News*, May 19, 2019, https://www.buzzfeednews.com/article/meghara/dubai-facial-recognition-technology-ibm-huawei-hikvision.

184. Deborah Amos, "Lebanon's Government Is Accused of Swarming WhatsApp to Catch Protesters," NPR, March 9, 2020, https://www.npr.org/2020/03/09/809684634/lebanons-government-is-accused-of-swarming-whatsapp-to-catch-protesters.

185. Aaron Holmes, "Saudi Arabia Allegedly Recruited Twitter Employees to Spy on Users. That's Just One of Many Ways Saudi Agents Use Tech Tools to Spy on Critics," Business Insider, November 7, 2019, https://www.businessinsider.com/saudi-arabia-big-tech-spy-on-dissidents-twitter-2019-11#the-human-rights-watch-report-recommends-that-twitter-and-other-tech-companies-investigate-possible-spying-and-advocate-for-the-release-of-dissidents-detained-for-criticizing-saudi-arabia-9.

186. "U.A.E.: Prominent Activist Jailed for Ten Years for Social Media Posts," Amnesty International UK, May 31, 2018, https://www.amnesty.org.uk/press-releases/uae-prominent-activist-jailed-ten-years-social-media-posts.

187. Ronen Bergman and Declan Walsh, "Egypt Is Using Apps to Track and Target Its Citizens, Report Says," *The New York Times,* October 3, 2019, https://www.nytimes.com/2019/10/03/world/middleeast/egypt-cyber-attack-phones.html.

188. Ryan Gallagher, "Middle East Dictators Buy Spy Tech from Company Linked to IBM and Google," The Intercept, July 12, 2019, https://theintercept.com/2019/07/12/

semptian-surveillance-mena-openpower/; Thomas Brewster, "Microsoft Slammed for Investment in Israeli Facial Recognition 'Spying on Palestinians,'" *Forbes*, August 1, 2019, https://www.forbes.com/sites/thomasbrewster/2019/08/01/microsoft-slammed-for-investing-in-israeli-facial-recognition-spying-on-palestinians/#536789456cec.

189. Christopher Bing and Joel Schectman, "Inside the U.A.E.'s Secret Hacking Team of American Mercenaries," Reuters, January 30, 2019, https://www.reuters.com/investigates/special-report/usa-spying-raven/.

190. Craig Timberg and Jay Greene, "WhatsApp Accuses Israeli Firm of Helping Governments Hack Phones of Journalists, Human Rights Workers," *The Washington Post*, October 29, 2019, https://www.washingtonpost.com/technology/2019/10/29/whatsapp-accuses-israeli-firm-helping-governments-hack-phones-journalists-human-rights-workers/.

191. Daniel Estrin, "What to Know about the Spying Scandal Linked to Israeli Tech Firm NSO," NPR, August 25, 2021, https://www.npr.org/2021/08/25/1027397544/nso-group-pegasus-spyware-mobile-israel.

192. Timberg and Greene, "WhatsApp Accuses Israeli Firm of Helping Governments Hack Phones of Journalists, Human Rights Workers."

193. Bill Marczak and John Scott-Railton, "The Million Dollar Dissident: NSO Group's iPhone Zero-Days Used against a U.A.E. Human Rights Defender," Citizen Lab Research Report No. 78 (University of Toronto, August 2016), https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/; Timberg and Greene, "WhatsApp Accuses Israeli Firm of Helping Governments Hack Phones of Journalists, Human Rights Workers."

194. Timberg and Greene, "WhatsApp Accuses Israeli Firm of Helping Governments Hack Phones of Journalists, Human Rights Workers."

195. "China's Huawei Helps Promote Security in Iraq's Capital via 'Safe City Solution' Project," Xinhua, http://www.xinhuanet.com/english/2019-03/08/c_137876838.htm.

196. "Yanbu: A Smart Industrial Oil Kingdom City," Huawei, https://e.huawei.com/en/publications/global/ict_insights/201708310903/manufacturing/201712061133.

197. Thamer Anwar Noori and Royal Commission Yanbu, "With AI, Yanbu Has Become Smarter and Safer," SmartCitiesWorld, July 30, 2020, https://www.smartcitiesworld.net/opinions/opinions/with-ai-yanbu-has-become-smarter-and-safer.

198. Mackenzie, "Surveillance State: How Gulf Governments Keep Watch on Us."

199. Alexander Cornwell, "Bahrain to Use Huawei in 5G Rollout despite U.S. Warnings," Reuters, March 26, 2019, https://www.reuters.com/article/us-huawei-security-bahrain/bahrain-to-use-huawei-in-5g-rollout-despite-us-warnings-idUSKCN1R71B3; "Huawei Signs 5 MoUs with Saudi Ministries to Develop ICT Infrastructure," Telecom Review, March 20, 2019, https://www.telecomreview.com/index.php/articles/telecom-vendors/2936-huawei-signs-5-mous-with-saudi-ministries-to-develop-ict-infrastructure; and Juan Pedro Tomás, "ZTE Signs Deal with Ooredoo to Pave the Way for 5G in the Middle East," RCR Wireless News, March 2, 2018, https://www.rcrwireless.com/20180302/5g/zte-5g-ooredoo-middle-east-tag23.

200. Alexander Cornwell, "Bahrain to Use Huawei in 5G Rollout despite U.S. Warnings." "Huawei Signs 5 MoUs with Saudi Ministries to Develop ICT Infrastructure"; Juan Pedro Tomás, "ZTE Signs Deal with Ooredoo to Pave the Way for 5G in the Middle East," RCR Wireless News.

201. "The Global AI Agenda: The Middle East and Africa" (MIT Technology Review Insights, 2020), https://mittrinsights.s3.amazonaws.com/AIagenda2020/MEAAIagenda.pdf, 2.

202. "Regulation of Artificial Intelligence in Selected Jurisdictions," (Law Library of Congress, July 2019), https://irp.fas.org/eprint/lloc-ai.pdf.

203. "The Global AI Agenda: The Middle East and Africa," 7.

204. "Mapping Approaches to Data on Data Flows: Report for the G20 Digital Economy Task Force" (Organisation for Economic Co-operation and Development, 2020), http://www.oecd.org/trade/documents/mapping-approaches-to-data-and-data-flows.pdf, 34.

205. Nadim Al Jisr, "Data Protection in the U.A.E.," Thomson Reuters, Middle East and North Africa, https://mena.thomsonreuters.com/en/resources/articles/data-protection-to-automate.html.

206. Al Tamimi & Company, "Egypt Passes New Personal Data Protection Law," Lexology, July 21, 2020, https://www.lexology.com/library/detail.aspx?g=2dccd758-ff8e-47c0-a93c-55d5e1cd31ef#:~:text=Egypt's%20Personal%20Data%20Protection%20Law,expected%20by%2014%20April%202021; "Egypt Data Protection," International Trade Administration, October 14, 2020, https://www.trade.gov/market-intelligence/egypt-data-protection.

207. "Saudi Arabia: Data Privacy Landscape," PwC Middle East, November 2019, https://www.pwc.com/m1/en/services/tax/me-tax-legal-news/2019/saudi-arabia-data-privacy-landscape-ksa.html.

208. Justin Sherman and Mark Raymond, "The U.N. Passed a Russia-Backed Cybercrime Resolution. That's Not Good News for Internet Freedom," *The Washington Post*, December 4, 2019, https://www.washingtonpost.com/politics/2019/12/04/un-passed-russia-backed-cybercrime-

resolution-thats-not-good-news-internet-freedom/.

209. Joe Uchill, "Russia and China Get a Big Win on Internet 'Sovereignty,'" Axios, November 21, 2019, https://www.axios.com/russia-china-united-nations-internet-sovereignty-3b4c14d0-a875-43a2-85cf-21497723c2ab.html.

210. Dear, "Will Russia Rule the World Through AI?"

211. Zak Doffman, "Putin Now Has Russia's Internet Kill Switch to Stop U.S. Cyberattacks," *Forbes*, October 28, 2019, https://www.forbes.com/sites/zakdoffman/2019/10/28/putin-now-has-russias-internet-kills-witch-to-stop-us-cyberattacks/.

212. Jose Antonio Vargas, "Spring Awakening," *The New York Times,* February 17, 2012, https://www.nytimes.com/2012/02/19/books/review/how-an-egyptian-revolution-began-on-facebook.html; Ross Tapsell, "The Smartphone As the 'Weapon of the Weak': Assessing the Role of Communication Technologies in Malaysia's Regime Change," *Journal of Current Southeast Asian Affairs*, 37 no. 3 (March 25, 2018), https://journals.sagepub.com/doi/full/10.1177/186810341803700302; and Daria Impiombato and Tracy Beattie, "Tinder Is the Latest Social Media Battleground in Thai Protests," *Foreign Policy*, October 2, 2020, https://foreignpolicy.com/2020/10/02/tinder-is-the-latest-social-media-battleground-in-thai-protests/.

213. Soma Basu, "Manufacturing Islamophobia on WhatsApp in India," *The Diplomat*, May 10, 2019, https://thediplomat.com/2019/05/manufacturing-islamophobia-on-whatsapp-in-india/; Billy Perrigo, "Facebook's Ties to India's Ruling Party Complicate Its Fight against Hate Speech," *Time*, August 27, 2020, https://time.com/5883993/india-facebook-hate-speech-bjp/; Kate Lamb, "'I Felt Disgusted': Inside Indonesia's Fake Twitter Account Factories," *The Guardian*, July 22, 2018, https://www.theguardian.com/world/2018/jul/23/indonesias-fake-twitter-account-factories-jakarta-politic; Lauren Etter, "What Happens when the Government Uses Facebook As a Weapon?" Bloomberg Businessweek, December 7, 2017, https://www.bloomberg.com/news/features/2017-12-07/how-rodrigo-duterte-turned-facebook-into-a-weapon-with-a-little-help-from-facebook; and Paul Mozur, "A Genocide Incited on Facebook, with Posts from Myanmar's Military," *The New York Times,* October 15, 2018, https://www.nytimes.com/2018/10/15/technology/myanmar-facebook-genocide.html.

214. "Egypt to Regulate Popular Social Media Users," BBC News, July 17, 2018, https://www.bbc.com/news/world-middle-east-44858547; Ashley Westerman, "'Fake News' Law Goes into Effect in Singapore, Worrying Free Speech Advocates," NPR, October 2, 2019, https://www.npr.org/2019/10/02/766399689/fake-news-law-goes-into-effect-in-singapore-worrying-free-speech-advocates.

215. Adrian Shahbaz, Allie Funk, and Andrea Hackl, "User Privacy or Cyber Sovereignty?" (Freedom House, 2020), https://freedomhouse.org/report/special-report/2020/user-privacy-or-cyber-sovereignty.

216. Arindrajit Basu, "The Retreat of the Data Localization Brigade: India, Indonesia and Vietnam," *The Diplomat*, January 10, 2020, https://thediplomat.com/2020/01/the-retreat-of-the-data-localization-brigade-india-indonesia-and-vietnam/.

217. "Data: Top Ten Most Downloaded Apps in Six Emerging Markets," Macro Polo, https://macropolo.org/the-chinese-and-us-apps-winning-the-next-billion-users/.

218. Ben Westcott, "TikTok Exec Says She 'Misspoke' in Hearing about the App Censoring Xinjiang Content," CNN Business, November 6, 2020, https://www.cnn.com/2020/11/06/tech/tiktok-xinjiang-censorship-uk-intl-hnk/index.html.

219. James Tager, "Made in Hollywood, Censored by Beijing" (Pen America, 2020), https://pen.org/report/made-in-hollywood-censored-by-beijing/; "Race to the Bottom: Corporate Complicity in Chinese Internet Censorship," Human Rights Watch, August 9, 2006, https://www.hrw.org/report/2006/08/09/race-bottom/corporate-complicity-chinese-internet-censorship; and Naomi Xu Elegant, "Zoom's Censorship Stumble Is a Familiar Narrative for Tech Stuck between U.S. and Beijing," *Fortune*, June 12, 2020, https://fortune.com/2020/06/12/zooms-censorship-stumble-is-a-familiar-narrative-for-tech-stuck-between-u-s-and-beijing/.

220. Richard Fontaine and Kara Frederick, "The Autocrat's New Tool Kit" (Center for a New American Security, March 15, 2019), https://www.cnas.org/publications/commentary/the-autocrats-new-tool-kit.

221. Koigi, "Huawei Launches Safe City Project to Tackle Africa Customers' Security Needs." "Huawei Holds Safe City Africa Summit in Case Town"; Tomás, "Huawei, Dubai Police to Develop Safe City Innovation Center"; and "Inside Huawei's Bandung Safe City Project with Telkom Indonesia."

222. Steve Stecklow, "Special Report: Chinese Firm Helps Iran Spy on Citizens," Reuters, March 22, 2012, https://www.reuters.com/article/us-iran-telecoms/special-report-chinese-firm-helps-iran-spy-on-citizens-idUSBRE82L0B820120322.

223. "Broadband Forum to Develop ICT in Laos."

224. "National Transformation in the Middle East: A Digital Journey," Deloitte, https://www2.deloitte.com/content/dam/Deloitte/xe/Documents/technology-media-telecommunications/dtme_tmt_national-transformation-in-the-middleeast/National%20Transformation%20in%20the%20Middle%20East%20-%20A%20Digital%20Journey.pdf.

225. Sintia Radu, "China's Web Surveillance Model Expands Abroad," U.S. News, November 1, 2018, https://www.

usnews.com/news/best-countries/articles/2018-11-01/china-expands-its-surveillance-model-by-training-other-governments.

226. Sacks, "Beijing Wants to Rewrite the Rules of the Internet."

227. Feldstein, "The Global Expansion of AI Surveillance."

228. "Statement by NCSC Director William Evanina: Election Threat Update for the American Public."

229. "Statement by NCSC Director William Evanina: Election Threat Update for the American Public."

230. "New White Paper on GRU Online Operations Puts Spotlight on Pseudo–Think Tanks and Personas," Stanford Internet Observatory, November 12, 2019, https://cyber.fsi.stanford.edu/io/news/potemkin-pages-personas-blog.

231. Kara Frederick, "Democracy by Design: An Affirmative Response to the Illiberal Use of Technology for 2021" (Center for a New American Security, December 15, 2020), https://www.cnas.org/publications/reports/democracy-by-design.

232. John Costello, Martijn Rasser, and Megan Lamberth, "From Plan to Action: Operationalizing a U.S. National Technology Strategy" (Center for a New American Security, July 29, 2021), https://www.cnas.org/publications/reports/from-plan-to-action.

233. Adaptation of a recommendation from Frederick, "Democracy by Design."

234. Adaptation of a recommendation from Frederick, "Democracy by Design."

235. Martijn Rasser, "Countering China's Technonationalism," *The Diplomat*, April 24, 2020, https://thediplomat.com/2020/04/countering-chinas-technonationalism/; Amalina Anuar, "ASEAN Smart Cities: Balancing 5G And Geopolitics—Analysis," RSIS Commentary in Eurasia Review, April 30, 2020, https://www.eurasiareview.com/30042020-asean-smart-cities-balancing-5g-and-geopolitics-analysis/.

236. Wolfgang Ischinger and Joseph S. Nye Jr., "Mind the Gap: Priorities for Transatlantic China Policy—Report of the Distinguished Reflection Group on Transatlantic China Policy," Munich/Berlin/Washington, D.C.: Munich Security Conference, Mercator Institute for China Studies, Aspen Strategy Group, July 2021, https://doi.org/10.47342/GXWK1490.

237. Melanie Hart and Jordan Link, "There Is a Solution to the Huawei Challenge" (Center for American Progress, October 14, 2020), https://www.americanprogress.org/issues/security/reports/2020/10/14/491476/solution-huawei-challenge/.

238. Jeffrey Ding, "Balancing Standards: U.S. and Chinese Strategies for Developing Technical Standards in AI," The National Bureau of Asian Research, July 1, 2020, https://www.nbr.org/publication/balancing-standards-u-s-and-chinese-strategies-for-developing-technical-standards-in-ai/.

239. Jeanne Whalen, "Government Should Take Bigger Role in Promoting U.S. Technology or Risk Losing Ground to China, Commission Says," *The Washington Post*, December 1, 2020, https://www.washingtonpost.com/technology/2020/12/01/us-policy-china-technology/.

240. Hart and Link, "There Is a Solution to the Huawei Challenge."

241. Vrishti Beniwal, "India Amends Rules to Curb 'Opportunistic' Foreign Takeovers," BloombergQuint, April 18, 2020, https://www.bloombergquint.com/global-economics/india-amends-fdi-rules-to-curb-opportunistic-takeovers.

242. Andrés Ortega, "The U.S.-China Race and the Fate of Transatlantic Relations" (Center for Strategic and International Studies, January 13, 2020), https://www.csis.org/analysis/us-china-race-and-fate-transatlantic-relations.

243. Cat Zakrzewski, "The Technology 202: Bipartisan Bill Would Fund Tech Partnerships with Allies to Counter China," *The Washington Post*, March 4, 2021, https://www.washingtonpost.com/politics/2021/03/04/technology-202-bipartisan-bill-would-fund-tech-partnerships-with-allies-counter-china/.

244. Daniel Kliman, "Why the United States Needs a Digital Development Fund" (Center for a New American Security, October 10, 2019), https://www.cnas.org/publications/commentary/why-the-united-states-needs-a-digital-development-fund.

245. Blanchette and Hillman, "China's Digital Silk Road after the Coronavirus."

246. Kristine Lee and Karina Barbesino, "Challenging China's Bid for App Dominance" (Center for a New American Security, January 22, 2020), https://www.cnas.org/publications/commentary/challenging-chinas-bid-for-app-dominance.

247. James Millward and Dahlia Peterson, "China's System of Oppression in Xinjiang: How It Developed and How to Curb It" (Brookings Institution, September 2020), https://www.brookings.edu/research/chinas-system-of-oppression-in-xinjiang-how-it-developed-and-how-to-curb-it/.

248. Polyakova and Meserole, "Exporting Digital Authoritarianism: The Russian and Chinese Models."

249. Andrew Imbrie, discussion with co-author, August 3,

2020. Saif Khan and Alexander Mann, "AI Chips: What They Are and Why They Matter" (Center for Security and Emerging Technology, April 2020), https://cset.georgetown.edu/wp-content/uploads/CSET-An-AI-Chips-Primer-What-They-Are-and-Why-They-Matter.pdf.

250. Anton Shilov, "Nvidia Increases Market Share as GPU Sales Explode: JPR," Tom's Hardware, June 8, 2021, https://www.tomshardware.com/news/jpr-gpu-shipments-in-q1-2021-hit-119-million-units.

251. Greg Gao and W. M. Zhang, "Inspired by Nvidia, More Chinese Companies Foray into GPU and See Their Opportunities in Cloud Computing Based Applications," JW Insights, March 6, 2021, https://m.laoyaoba.com/n/782531.

About the Center for a New American Security

The mission of the Center for a New American Security (CNAS) is to develop strong, pragmatic and principled national security and defense policies. Building on the expertise and experience of its staff and advisors, CNAS engages policymakers, experts and the public with innovative, fact-based research, ideas and analysis to shape and elevate the national security debate. A key part of our mission is to inform and prepare the national security leaders of today and tomorrow.

CNAS is located in Washington, DC, and was established in February 2007 by co-founders Kurt M. Campbell and Michèle A. Flournoy. CNAS is a 501(c)3 tax-exempt nonprofit organization. Its research is independent and non-partisan.


Center for a
New American
Security