G|M|F alliance for securing democracy

A Future Internet For Democracies

Contesting China’s Dominance in 5G, 6G, and the Internet-of-Everything

Lindsay P. Gorman

G | M | F The German Marshall Fund
of the United States

Please direct inquiries to
The Alliance for Securing Democracy at
The German Marshall Fund of the United States
1700 18th Street, NW Washington, DC 20009
T 1 202 683 2650
E info@securingdemocracy.org

This publication can be downloaded for free at https://securingdemocracy.gmfus.org/future-internet/.

The views expressed in GMF publications and commentary are the views of the authors alone.

Cover and vignette graphics designed by Kenny Nguyen.
Other graphics designed by Marcos da Rocha Carvalho.

Alliance for Securing Democracy

The Alliance for Securing Democracy (ASD), a bipartisan initiative housed at the German Marshall Fund of the United States, develops comprehensive strategies to deter, defend against, and raise the costs on authoritarian efforts to undermine and interfere in democratic institutions. ASD brings together experts on disinformation, malign finance, emerging technologies, elections integrity, economic coercion, and cybersecurity, as well as regional experts, to collaborate across traditional stovepipes and develop cross-cutting frameworks.

About the Author

Lindsay Gorman is the Emerging Technologies Fellow at the German Marshall Fund's Alliance for Securing Democracy and a consultant for Schmidt Futures. As an expert on technology and national security, she has spent over a decade in government and industry, including in the Office of U.S. Senator Mark Warner, the White House Office of Science and Technology Policy, and the National Academy of Sciences. A physicist and computer scientist by training, Lindsay previously ran a technology consulting firm, Politech Advisory, advising start-ups and venture capital and has developed cybersecurity tools in Silicon Valley. Her technical expertise lies in artificial intelligence, statistical machine learning, and quantum materials. She is also an awardee of the U.S. State Department Speaker Program, a member of the Truman National Security Project, and has been an expert contributor to U.S. Cyberspace Solarium Commission and an adjunct fellow at the Center for Strategic and International Studies. Lindsay's commentary and analysis regularly appears in outlets including The Washington Post, NPR, The Atlantic, Financial Times, Los Angeles Times, Bloomberg, Foreign Policy, and Lawfare. She has also published academic works in The Washington Quarterly and in leading physics journal Nature Physics on topological insulators, and programmed computer vision AI systems for a self-driving car as part of the DARPA Urban Challenge. She holds an A.B. in physics from Princeton University, where she graduated magna cum laude, and a M.S. in applied physics from Stanford University. Lindsay can be followed on Twitter at @LindsayPGorman.

Contents

Executive Summary

Democracies and Authoritarian Regimes in Competition for the Future Internet

The United States and its democratic allies are engaged in a contest for the soul of the Future Internet. Conceived as a beacon of free expression with the power to tear down communication barriers across free and unfree societies alike, the Internet today faces significant challenges to its status as the world's ultimate connector.[1] In creating connectivity and space for democratic speech, it has also enabled new means of authoritarian control and the suppression of human rights through censorship and surveillance. As tensions between democracies and the People's Republic of China (PRC) heat up over Internet technologies, the prospect of a dichotomous Internet comes more sharply into focus: a democratic Internet where information flows freely and an authoritarian Internet where it is tightly controlled—separated not by an Iron Curtain, but a Silicon one. The Future Internet is deeply enmeshed in the dawning information contest between autocracies and democracies.[2] It is the base layer—the foundation—on which communication takes place and the entry point into narrative and societal influence. How the next generation of Internet technologies are created, defined, governed, and ultimately used will have an outsized impact on this information contest—and the larger geopolitical contest—between democracy and authoritarianism.

Future Internet [ˈfyu tʃər ˈɪn tərˌnɛt] *noun.* The suite of technologies and the standards for how they operate that will define and shape digital connectivity over the next 30 years, including: infrastructure technologies and internet protocols; application layer technologies that run atop this infrastructure, harnessing data often with artificial intelligence; and the governance frameworks this technology stack imputes.

China's growing presence in the global telecommunications market—and the threat that reality poses to the United States and its allies—has catalyzed both national security and economic policy interest in fifth-generation cellular network infrastructure (5G). Like 2G, 3G, and 4G before it, the next generation of mobile connectivity promises a step-change in Internet capability and a societal transformation—through the explosion of connected devices across cities, vehicles, factories, and homes.[3] The nascent data-fueled economy 5G Internet will spawn represents a new playing field for nation-state competition in both commercial innovation and systems of governance alike. In this new economy, United States leadership is not assured.

China has made a targeted push to lead the world in the emerging technologies of the future—built on future networks and extending to the applications their data will enable: from artificial intelligence (AI) and autonomous cars to smart grids and advanced manufacturing.[4] Chinese telecommunications giant Huawei has by some measures provided the most technical contributions to the 5G standard and last year filed more patents in Europe than any other company.[5] Heavy state subsidies provided by the Chinese Communist Party (CCP) have increased the competitiveness of Chinese firms in critical technology industries abroad. As the Pentagon's Innovation Board bluntly put it: "The country that owns 5G will own many of these innovations and set the standards for the rest of the world … That country is currently not likely to be the United States."[6]

A Threat Beyond Espionage

The severity of threat that Chinese leadership poses to the Future Internet has been hotly contested in the United States, across the Atlantic, and around the world. In most cases, the United States has driven this debate through a narrow, albeit important lens: using diplomatic efforts, unsealed indictments, and the sharing of U.S. intelligence, it has attempted to persuade allies that the inclusion of equipment made by Chinese telecommunications giant Huawei into national 5G networks would represent an unacceptable security risk.[7] According to the U.S. intelligence community and an increasing number of allied intelligence services, this risk is increasingly objectionable.[8] Many U.S. allies in Europe and around the globe will make decisions about Huawei's participation in their national 5G networks in the coming months. The consequences may last decades.

But the concerns around a growing authoritarian Internet go beyond espionage alone and even beyond Internet and telecommunications infrastructure itself. This report argues that competing in and securing the Future Internet—in 5G, 6G, and the generations and especially the applications to follow—is a crucial U.S. and allied national security interest. It also demonstrates how the current U.S. and allied approach suffers from strategic myopia on both sides of the Atlantic by over-focusing on traditional espionage without due consideration for the ways in which infrastructure dominance will create industry and application dominance—and permeate governance.

As such, the report provides a roadmap for contesting China's growing dominance in this critical information arena across infrastructure, application, and governance dimensions—one that doubles down on geostrategic interests and allied cooperation. An allied approach that is rooted firmly in shared values and resists an authoritarian divide-and-conquer strategy is vital for the success of democracies in commercial, military, and governance domains.

Across the infrastructure, application, and governance dimensions, the report uses open source reporting, corporation records, case studies, vignettes, and original research to detail China's use of infrastructural dependence for geopolitical manipulation; its history of intellectual property theft as well as the U.S. and European understanding of this activity and the loopholes in their attempts to counter it; the connection between personal data and the CCP Propaganda Department as "new oil"; China's increasing role in international standards bodies and how it uses that presence to advance both technology and authoritarian governance norms; and the emerging synergistic relationship between one international technical organization and the Belt and Road Initiative (BRI). In some areas, the report draws on transatlantic consultations to hone in on the approach of the United States and its European allies, recognizing that while many democratic nations face similar challenges, a one-size-fits-all approach is rarely an accurate depiction of reality. Finally, it includes 47 concrete recommendations for the United States and democratic governments to strengthen their hand in Future Internet industries. Engaging in authoritarian mimicry will not secure the Future Internet for open economies and open communications. Democracies need to capitalize on their own strengths to respond effectively.

Key Findings

The report identifies ten key findings on China's efforts across the infrastructure, application, and governance dimensions of the Future Internet. These findings provide a picture of where democracies should focus—across technology development and standards-setting—to compete and defend their values in the Internet-of-Everything era.

- **The CCP has a history of creating infrastructure dependence and using it for geopolitical leverage.** As such, China's global market dominance in Future Internet infrastructure carries unacceptable risks for democracie**s.**
- **The contest to shape 6G standards is already underway, with China leading the charge internationally.** As the United States ponders how it ended up on the back foot on 5G, China is moving ahead with new proposals that would increase authoritarian control and undermine fundamental freedoms.
- **The battle over the Future Internet is playing out in the Global South.** As more developed nations eschew Chinese network equipment, democracies' response has largely ignored this global build-out of networks and applications in the proving ground of the developing world that threaten both technological competitiveness and universal rights.
- **China is exporting "technology to anticipate crime"—a dystopian future police state.** "Minority

report"-style pre-criminal arrests decimate the practice of the rule of law centered in the presumption of innocence.

- **Personal Data Exfiltration: CCP entities see "Alternative Data" as "New Oil" for AI-driven applications in the Internet-of-Everything.** These applications provide new and expanded avenues for mass data collection, as much as they depend on this data to succeed--giving China the means and the motivation to vacuum up the world's data.
- **Data in, propaganda out: Future Internet technology presents opportunities to influence the information environment, including the development of information applications that simultaneously perform big data collection.** Chinese companies are building information platforms into application technologies, reimagining both the public square and private locales as tools for propaganda.
- **Already victims of intellectual property theft by China, the United States and its democratic partners are ill-prepared to secure sensitive information as the Future Internet ecosystem explodes access points.** This insecurity will continue to undermine technological competitiveness and national security and compound these effects in new ways.
- **China outnumbers the United States nearly two-to-one on participation in and leadership of critical international Future Internet standards-setting efforts.** Technocratic standards bodies are becoming unlikely loci of great power technical competition, as Beijing uses leadership posts to shape the narrative and set the course for the next generation of Internet technologies to support China's own technological leadership, governance norms, and market access.
- **The world's oldest UN agency is being leveraged as a propaganda mouthpiece for the CCP's AI and Future Internet agenda, whitewashing human rights abuses under a banner of "AI for Good."** The upshot is an effort to shape the UN Sustainable Development agenda to put economic development with authoritarian technology--not individual liberty—at their center.
- **A symbiotic relationship has developed between China's Belt and Road Initiative and UN agencies involved in Future Internet and digital development.** In this way, China leverages the United Nations enterprise to capture market dominance in next generation technologies.

Recommendations

The report includes 47 concrete strategic and tactical policy recommendations democracies should adopt to succeed in the Internet-of-Everything era while advancing the democratic values of human rights, transparency, and freedom from tyranny. When practicable, these recommendations embrace a multilateral frame that envisions democracies as strategic partners in the defense and promotion of these values, along five key dimensions:

Counter China's Structural Advantages in Future Internet Development and Deployment

Offsetting China's cross-societal play requires adequate coordination in government. In the United States, the White House should create a Technology Directorate at the National Security Council and appoint a Future Internet Director with a joint appointment at the White House Office of Science and Technology Policy to coordinate an interagency task force on U.S. and democratic global competitiveness to build out and implement a cross-cutting Future Internet strategy.

The director should also establish a private sector working group of industry representatives; plan for 6G now by leading a public-private coalition on 6G experimentation, standards, and spectrum, in coordination with democratic partners; develop an interagency digital development agenda including a focus on the application and governance dimensions of the Future Internet, and provide national security input to economic and trade policy. European partners should tailor analogous structures to national environments, with an emphasis on bridging communication and decision-making between economics ministries and ministries of foreign affairs on matters of technology and national security.

Construct Allied Solutions for the Developed and Developing Worlds

The United States cannot compete on its own: unilateral tech policy is vulnerable to claims of protectionism, and in many areas U.S. allies are out front. A transnational alliance of democracies such as Britain's "D10" should fuse expertise and build collective political will to ensure the Future Internet is an open and democratic one. The D10 should create a multilateral "Trusted Internet" or "Trusted Cyber" standard based on the Prague Proposals for 5G and 6G infrastructure systems, hold a summit with the goal of drafting democratic principles for the application layer of the Future Internet, and stablish three joint Future Internet Research and Development (R&D) Centers of Excellence (CoE) on infrastructure, applications, and governance in North America, Europe, and the Asia-Pacific. The standard should include the development of sustainable off-ramp plans and be used as input into new Organization for Economic Cooperation and Development (OECD) member accession decisions, and the output of the application layer summit should include a rubric for evaluating information apps in democracies.

> *"The United States and its allies are not coming together to defend their shared values or to clarify what they mean in the digital arena.*

Increase Allied Coordination and Activity in International Standards Bodies

One reason China is writing the new global rules at international standards bodies is that the United States and its allies are not coming together to defend their shared values or to clarify what they mean in the digital arena. The D10, in coordination with the private sector, should conduct ongoing monitoring and assessment of the proceedings of international standards bodies (such as the Third Generation Partnership Project (3GPP), the UN International Telecommunications Union (ITU), and International Organization for Standardization (ISO). This effort should provide an allied coordination function in advance of key meetings on standards that implicate democratic governance, as well as ongoing assessment of PRC bloc action to advance specific features that advantage Chinese companies or promote authoritarian Internet governance norms in infrastructure or application standards. The D10 should also build a minimum common understanding of governance norms that should shape a democratic Future Internet and work to install democratic leadership in key positions and focus groups.

Secure the Future Internet

Information security and data privacy must be pillars of a Future Internet for democracies – across both the infrastructure and application layers. Nationally in the United States, Congress should pass comprehensive federal data protection legislation including cybersecurity standards for IoT devices and applications and transparency around data brokers. The U.S. and allied intelligence communities should conduct comprehensive, end-to-end 5G cyber risk assessments across the entire Future Internet technology stack. At the international level, NATO should update its cost-sharing structure to count a portion of excess nation spending on secure 5G and 6G infrastructure towards its two percent defense spending goals; update its telecommunications security requirements to align with the Prague Proposals; and conduct a forward-looking security assessment of future NATO communications infrastructure into 5G and 6G that includes an assessment of quantum information progress.

Contest Unfair Business Practices and Build Resiliency to Intellectual Property Theft

In the cyber domain, the United States suffers from a tragedy-of-the-commons problem in which companies are not incentivized to come forward to report cyber intellectual property (IP) theft, especially from China, due to fear of business repercussions. How and by whom data is stored, handled, accessed, and shared are central to the distinction between democracy and autocracy. Democracies should extend and amplify that distinction. Congress should pass comprehensive federal data protection legislation that includes a breach notification requirement as a matter of corporate governance. The European Union should form a Commission on the Theft of European Intellectual Property to study the costs of economic espionage and IP theft in Europe.

The Future Internet and the New Data Economy

Key Findings

- **Market dominance in the Future Internet will create economic opportunity across infrastructure, application, and governance domains.** Democratic strategy on the Future Internet should promote an affirmative vision for data-based application layer technologies that champion democratic values and actively challenge authoritarian governance norms.
- **China is exporting "technology to anticipate crime"—a dystopian future police state.** 5G is only the beginning of an application ecosystem that includes healthcare, education, energy and water management, transportation, smart industries, and policing. Smart city and "safe city" infrastructure and command centers are a key Chinese surveillance export. In one case study, Brazilian authorities tout the use of Chinese technology "to anticipate crime," proclaiming "we will not wait for the crime to be committed before we act."
- **The battle over the Future Internet is playing out in the Global South.** While many developed nations pursue alternatives to Huawei, Chinese infrastructure is prevalent in Africa and Latin America, and Huawei is building out the Future Internet's application layer. The report calls for an international trusted cyber certification to be developed multilaterally and used as input to new OECD membership for nations like Brazil and Argentina. It also calls for a digital development strategy that prioritizes Future Internet application development as well as infrastructure financing in the developing world.

The Future Internet is the suite of technologies and the standards for how they operate that will define and shape digital connectivity over the next 30 years, including: infrastructure technologies and internet protocols; application layer technologies that run atop this infrastructure, harnessing data often with artificial intelligence; and the governance frameworks this technology stack imputes. Just as the current Internet of mobile applications was a step change from the world of dial-up, the Future Internet will depart from our status quo, carrying with it just as significant impacts on our information environment and our democracy. To date, U.S. efforts have largely focused on infrastructure.

The Infrastructure Layer: What Are 5G and 6G?

At its core, 5G is a set of technical rules—packaged into a global standard—that define how the next (fifth) generation of telecommunications networks operate: which radio frequencies are used to communicate information and how components like cellular devices, antennas, and base stations ferry that information. Much like generations of wireless networks before it, 5G promises to usher in a step-change in capability arising from faster speeds, lower latency, and higher bandwidths available for data-based applications.[9]

> *"In authoritarian states, an abundance of personal information presents new opportunities for repression and control.*

At least equaling 5G's promise has been the hype surrounding its advent. Major airports around the globe have been plastered with 5G-related ads, and in the United States, network providers like AT&T have billed pre-5G deployments.[10] Yet according to a Barclays survey, only 28 percent of businesses knew what 5G was and what it could do in practice.[11]

New generations of mobile networks have transformed the world population's connected lives—and with them the means of global economic and technological competition.

Mobile Network Evolution

From the first handheld mobile phone call—placed in 1973—mobile network innovations have increased speed, improved data-carrying capacity, and decreased latency, yielding a host of new applications with each successive generation.

- 1G – Analog voice. Built in the late 1970s and 1980s, the retroactively named first generation automated cellular network was voice-only and analog. In this new "cellular" design, voices traveled over radio channels to and from operator-deployed base stations in specific ranges of licensed frequency spectrum. Neighboring cells operated at different frequencies to avoid interference, but the same frequency ranges could be used over and over again when separated by enough physical distance. While the design was novel, coverage was poor and sound quality low. Security was also non-existent. Voice conversations were transmitted over radio waves unencrypted, meaning anyone with an off-the-shelf radio scanner could easily eavesdrop on 1G conversations.[12] Devices were large and heavy, with poor battery life. And because different operators worked on different networks, there was no roaming support between them.[13]
- 2G – Digital voice & basic data. Where the first generation established the foundations of mobile communications, 2G replaced analog radio networks with digital signals, including text. Built in the 1990s, 2G digital networks saw mass consumer and business adoption, as digital compression and coding techniques enabled more efficient use of the radio spectrum and a greater number of users on the network. Signals were also digitally encrypted, making them more secure than the open analog calls of 1G. Over successive deployments, the 2G era saw the advent of text (SMS), email, and picture messages, with data transfer speeds comparable to dialup Internet and early DSL.[14]
- 3G – From the Blackberry to the iPhone. The International Telecommunications Union (ITU)'s IMT-2000 standard codified 3G, which increased bandwidth and gave rise to the smart phone revolution, enabling video conferencing, video streaming and voice over IP.[15] From multimedia entertainment to location-based services, smartphone apps ushered in an entirely new economy.[16] Broadband Internet found its way to the home and office, and 3G powered truly global roaming. The iPhone was introduced in 2007, and by 2010, 92 out of every 100 people worldwide held a mobile subscription—up from 39 in 2000.[17]
- 4G LTE – Mobile Broadband. The 2010s era of true mobile broadband saw large increases in data capacity supporting richer content and more connections across smartphones, tablets, and laptops. Wider channels, more antennas, and aggregated data pipes fueled faster connections, supporting Voice over IP (VoIP), Internet Protocol version 6 (IPv6), gaming, and high-quality and high-definition video conferencing and streaming capabilities. A simplified core network and lower latencies opened up these applications in real-time. LTE Advanced is evolving to attain dynamic broadcasting and continuous device-to-device proximity awareness.[18]
- 5G – The Internet-of-Things era. Like generations of advances before it, 5G promises faster speeds, higher bandwidth, and lower latency that will usher in an era of connected devices and the ability to process the data they produce. The upshot is a new generation of consumer and industrial technologies.
  - Applications: Smart cities, remote surgeries & telemedicine, automated factories, industrial sensors, driverless cars, virtual reality and augmented reality, 3D video, precision agriculture systems, cloud computing, and the Internet of Things (IoT).[19]
  - Speed. Running from 10 to 100 times the speed of 4G means downloads and data-processing fast enough for advanced processing and real-time decisions.
  - Bandwidth. 4G networks are bandwidth-limited—too many connections slow down the network. Increased bandwidth in 5G allows for more connected devices operating at the same time and the ability to act in concert—from connected toothbrushes and kitchen appliances to street lights.[20]

    - Latency. Low latency—the lag time in communications between devices and servers—allows for the near-instantaneous communication necessary for technologies such as self-driving cars. Sensors on the vehicle must perceive the driving environment, send signals over the network to a cloud processing unit, analyze the influx of environmental data, and send a signal back to the vehicle directing its next move. To do so successfully and safely, such communication must be rapid.

- 6G – The Surface Revolution. As 5G lays the groundwork for the future of connected devices, full realization of the Internet-of-Everything and many of the higher end promises of 5G may not truly be achieved until 6G in the 2030s. Heralded as the end of the smartphone era, 6G is the stuff of science fiction: multisensory augmented, virtual, or mixed reality, connected robotics and autonomous systems, drone-delivery systems, autonomous drone swarm, and vehicle platoons. The emergence of smart surfaces and environments, wireless brain-computer interactions, and blockchain and distributed ledger applications will again revolutionize the economy and modern day life.[21] Crucially, China is acting today by leading international efforts to shape the development of 6G to accord with authoritarian norms of control.

The Application Layer: IoT and the Trillion Dollar Data Economy

The new data economy that 5G and 6G network infrastructure enables will open up not only new applications, but new modes of value creation and economic power.

Deloitte defines IoT as follows:

> "The IoT is a suite of technologies and applications that equip devices and locations to generate all kinds of information—and to connect those devices and locations for instant data analysis and, ideally, "smart" action. Conceptually, the IoT implies physical objects being able to utilize the Internet backbone to communicate data about their condition, position, or other attributes."[22]

Worldwide corporate data has been increasing exponentially over the last decade, and the advent of the IoT will only continue this trend.[23] Technology research firm IDC predicts that by 2025, there will be 41.6 billion connected devices serving consumers and businesses worldwide, creating upwards of 79 zettabytes of data.[24] Harnessing, processing, analyzing, and acting on this abundance of data will be central to economic success in factories, cities, retail, medicine, and more.

The United States lacks a federal legal or regulatory framework for securing this data, while in Europe, there is an overreliance on high-risk vendors from China with a history of IP theft. In many partly free states from Thailand to Kenya to Ecuador—including some that Morgus et al, have dubbed the "digital deciders"—both problems are true.[25]

According to a seminal McKinsey report, by 2025, IoT will generate from $4 to $11 trillion of potential economic impact each year.[26] The academic international relations literature has long drawn connections between economic and geopolitical power, and China's economic rise is no exception to this trend.[27] The task of democracies will be to harness this power while advancing the principles of privacy, accountability, and data protection that may seem, at times, to be at odds with capturing this value.

The Governance Layer: New Opportunities and New Risks

This explosion of data has already given rise to business models based on the mass collection and aggregation of personal data—what Shoshanna Zuboff terms "surveillance capitalism."[28] In democracies, these business models raise questions about the responsible handling and securing of data on the grounds of personal privacy and sensitive data protection. In authoritarian states, an abundance of personal information presents new opportunities for repression and control.[29] At a time when the United States and its democratic allies and partners are struggling to construct a model for governance of the data-driven economy that accords with their most basic values, China is charging ahead to imagine the future of AI.[30]

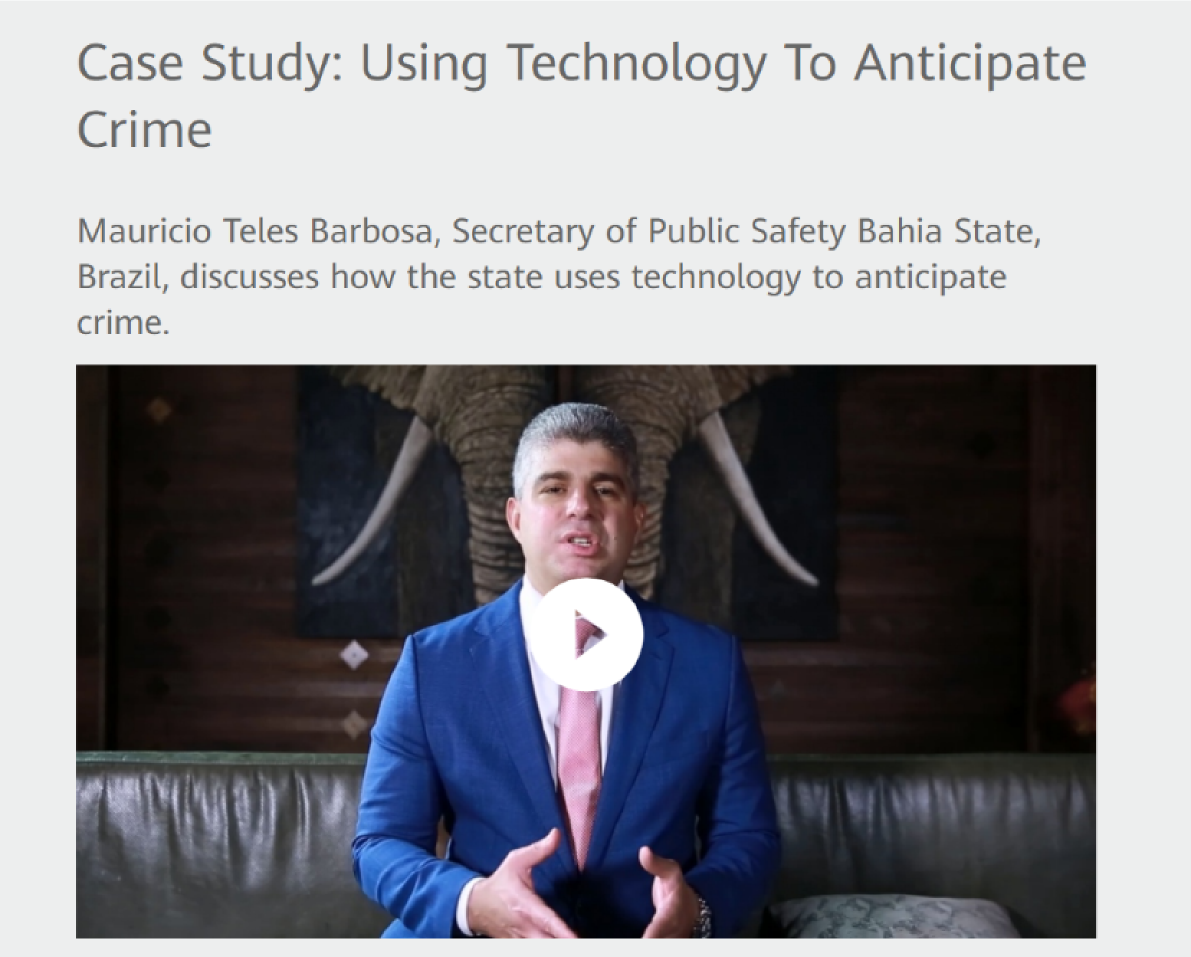
Most egregiously in Xinjiang, China, a sophisticated network of data-powered surveillance technologies is deployed to control its ethnic Uyghur population through facial recognition cameras, GPS trackers, DNA checkpoints, and online-behavior monitoring.

Outside of Xinjiang, 200 million cameras watch China's population. Some schools feature GPS and facial-recognition-enabled uniforms to enforce attendance and behavior in children. Beyond China's borders, its companies sell tracking and monitoring systems to authoritarian governments and police forces worldwide—often through similar vehicles as the placement of 5G technology.[31] Some 63 countries and counting, from Pakistan and Ghana to France and Spain, have bought AI surveillance equipment manufactured in China.[32]

Case Study: Predictive Policing ("Using Technology to Anticipate Crime" like in TV Show "Person of Interest")

"We Won't Wait for the Crime to Happen Before We Act"

In one case study highlighted by Huawei's public safety vertical, a Brazilian official describes the use of Huawei technology to "anticipate crime." In a Huawei promotional video entitled "Using Technology to Anticipate Crime," Mauricio Teles Barbosa, the Secretary of Public Safety of Brazil's Bahia State, explains that Bahia has invested in a $100 million project to build a command, control, and intelligence center for its police. "There is no point in having thousands and thousands of cameras if we don't analyze these images and use facial and license plate recognition," he says, introducing new image and video analytics tools Bahia is investing in. More suspects will be able to be arrested as "a preventive measure … We won't wait for the crime to happen before we act."[33]



Case Study: Using Technology To Anticipate Crime

Mauricio Teles Barbosa, Secretary of Public Safety Bahia State, Brazil, discusses how the state uses technology to anticipate crime.

Source: Screenshot of the Huawei video "Using Technology to Anticipate Crime."[34]

"Nowhere to Hide"—Modeling Smart and Safe Cities after CBS' Sci-Fi Show "Person of Interest"

Huawei's Safe City technology (or at least the marketing thereof) also appears to derive inspiration from American science fiction crime drama "Person of Interest"—in which an all-seeing AI collates all sources of information including surveillance cameras and electronic communications to predict human behavior and intervene in the prevention of violent crime. In one marketing document entitled “Nowhere to hide: Building safe cities with technology enablers and AI,” Huawei writes:

> “In the popular sci-fi crime drama Person of Interest, criminals are equipped with a shadow map of New York to avoid surveillance cameras, creating breeding grounds for crime. Shift to the real world, and governments are ramping up camera coverage in cities to stop these hotspots from emerging and are using big-data driven tech like computer vision to cut crime.
>
> “By analyzing people’s behavior in video footage, and drawing on other government data such as identity, economic status, and circle of acquaintances, AI could quickly detect indications of crimes and predict potential criminal activity, just like Machine on Person of Interest.”[35]

The article depicts a multi-pronged and multi-sensory information environment that draws on neighborhood and home security systems, street lights, and environmental monitoring systems—in addition to more traditional security cameras—to provide full-picture surveillance. In particular, the pooling of resources from “telcos” and local governments illustrates the full-spectrum nature of the Future Internet, and the interconnections among infrastructure, application, and governance dimensions:

> “When constructing safe cities, different municipal departments and telcos will be able to pool resources and build integrated systems that combine street lamps, mini base stations, and surveillance cameras, so that all areas with street lighting can be placed under surveillance. It will be possible to beam footage from front-line police officers equipped with wearable cameras live to control centers on wireless networks.
>
> “In the fully connected cities of the near future broadband is fast and ubiquitous, allowing public spaces to be covered by surveillance equipment, with unified platforms incorporating information from a range of sources, including environmental monitoring equipment, road surveillance cameras, neighborhood and home security systems, and network information security surveillance. Control and dispatch centers will use this information to help carry out unified surveillance, safety management, and dispatch of public safety resources.”[36]

To be sure, there are numerous challenges to implementing these futuristic police systems. One Huawei points out is the inability of local authorities to access information from private cameras absent a fusion platform. Another is the technical and processing challenge of fusing all this data and deriving behavior insight from it.

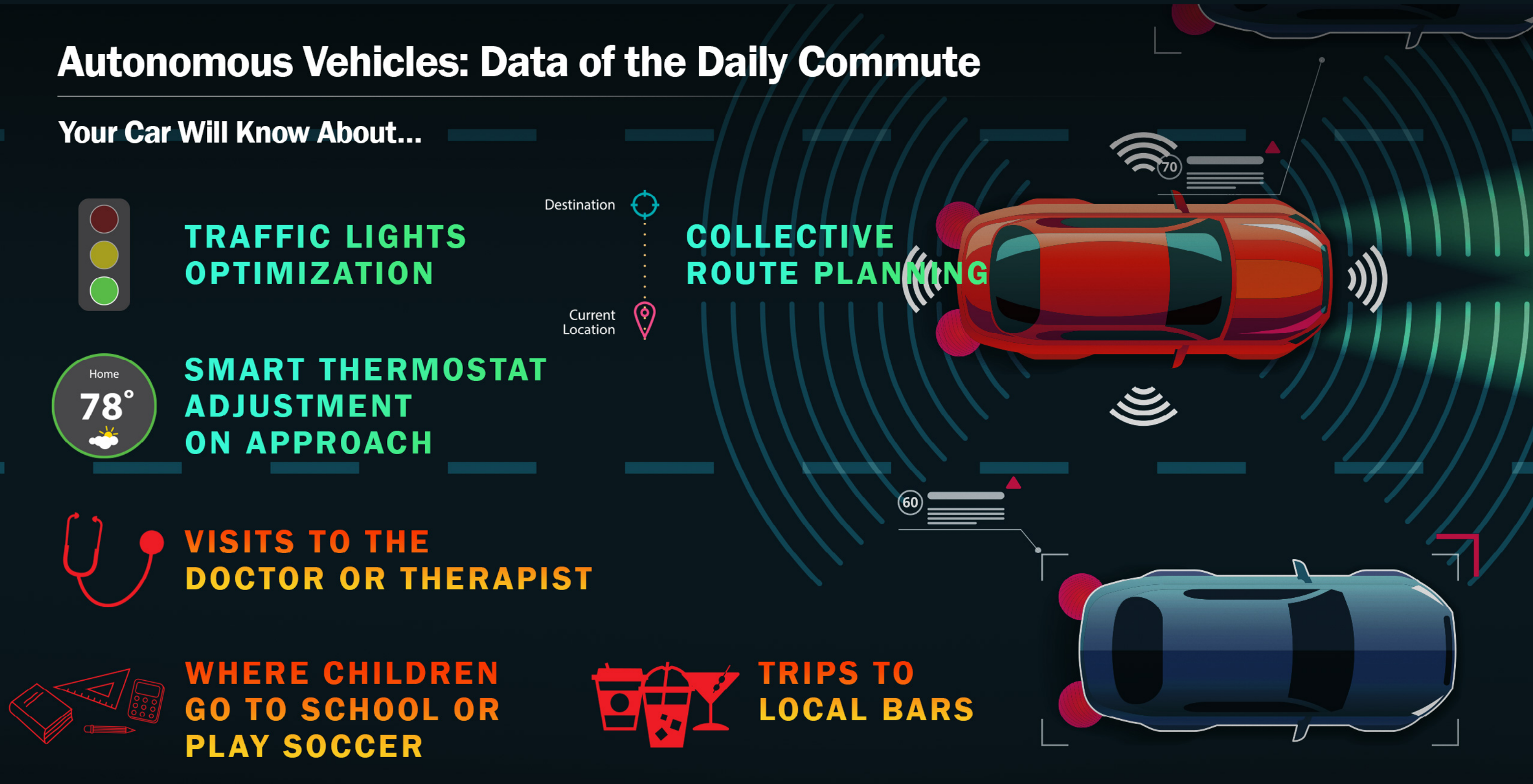
But treating 5G and 6G infrastructure, application layer information systems, and surveillance technologies independently in not reflective of the information environment Beijing aspires to create. A Future Internet for democracies needs to move beyond these siloes to compete in and re-envision modern public squares and private living rooms in a way that accords with universal rights.

Vignette 1: Data of the Daily Commute

When Steve gets in his 2030 Toyota Prius, 5G-enabled edge computing will shape much of his daily commute. Data storage and processing localized to the car could alert him to nearby drivers and pedestrians based on their IoT devices. 5G edge computing could enable his car to communicate with his house or office to adjust lighting, temperature, and energy consumption as he approaches. It could even try to ease the traffic on his route by connecting the car, traffic lights, and GPS to set up an optimal path.

However, 5G will have less obvious—and less benign—effects as well. The proliferation of 5G applications relating to autonomous vehicles also means that many systems and companies will have access to potentially sensitive information about Steve's location, habits, or consumption. Firms could track his every move from data on any drive, from how often he visits his doctor or therapist, to his trips to local bars. They'd know how often, and from where, Steve gets takeout for dinner. They could determine where his children go to school or have soccer practice. They could figure out when his house is empty. Ominously, Steve may have no influence over how companies use the information, or to whom they might sell 5G-enabled data.

Autonomous Vehicles: Data of the Daily Commute



Your Car Will Know About...

TRAFFIC LIGHTS OPTIMIZATION

COLLECTIVE ROUTE PLANNING

SMART THERMOSTAT ADJUSTMENT ON APPROACH

VISITS TO THE DOCTOR OR THERAPIST

WHERE CHILDREN GO TO SCHOOL OR PLAY SOCCER

TRIPS TO LOCAL BARS

alliance for securing democracy
G|M|F

A Future Internet For Democracies

G | M | F The German Marshall Fund of the United States

Vignette 2: Urban Surveillance

When Alexis moved to New York, she was excited to enjoy all the attractions of the Big Apple, as well as the anonymity that she thought came from living in a metropolis. However, new 5G-enabled facial recognition software meant that government and private companies could track her whereabouts on a real-time, near-constant basis. Interconnected systems of cameras, sensors, local storage, processing, and data integration platforms could potentially mean the end of privacy as we currently know it.

5G-enabled facial recognition could tell governments and firms exactly where people are in public spaces. Visits to the grocery store, the gym, school, and work could be monitored. Still more chilling, facial recognition could stifle public participation in core elements of the democratic process. Devices could potentially track who attends local community meetings (from city council hearings to PTA meetings), as well as who participates in protests, demonstrations, and other means of activist expression. People would live their lives under relentless, unceasing surveillance, with little or no guarantee of proper oversight and accountability related to these 5G-enabled systems.

Facial Recognition: Urban Surveillance

NAMING AND SHAMING INDIVIDUALS FOR PUBLIC BEHAVIOR

IDENTIFICATION & TRACKING OF PROTESTERS

1 CAMERA PER 14 PEOPLE IN LONDON

3 MILLION CAMERAS IN SHANGHAI

1.5 BILLION HOURS OF VIDEO FOOTAGE ANNUALLY IN MOSCOW

alliance for securing democracy

G|M|F

A Future Internet For Democracies

G | M | F The German Marshall Fund of the United States

Vignette 3: Convenience at a Cost

Jay thought he would enjoy the convenience of 5G-enabled devices contributing to a “smart home” of the 21st century. What he did not initially consider, however, was the loss of privacy that the smart home devices would cause. The firms behind these devices could learn all about his daily habits, behavior, and lifestyle.

For instance, a smart fridge could determine how much juice, wine, and milk he and his wife drink in a week, and observe the progress of their diet and nutrition. Other smart devices could show which side of the bed Jay sleeps on, and potentially how much sleep he gets each night. A smart TV would know how often and what shows his family watches. Smart devices could recognize when no one was at home, too.

Devices like Amazon’s Alexa, by connecting to or syncing with other devices, could incorporate video or audio recordings of pretty much anything occurring within the home. Whether or not Jay and his family consciously realize it, the 5G-enabled devices could be feeding companies vast streams of highly personal, often sensitive data. If bad actors sought to control the devices or otherwise compromise that data, Jay’s family would likely have limited options to respond; they might not even be aware a breach had occurred.

Smart Home: Convenience at a Cost

Your Home Will Track...

AMOUNT OF MILK OR BEER CONSUMED IN THE FRIDGE

AUDIO AND VIDEO FEEDS OF HOME ACTIVITIES

FRIENDS AND ASSOCIATES STOPPING BY

WHEN THE HOUSE IS EMPTY

alliance for securing democracy

G|M|F

A Future Internet For Democracies

G | M | F The German Marshall Fund of the United States

The Authoritarian Internet: A Global Threat

Key Findings

- **The CCP has a history of creating infrastructure dependence and using it for geopolitical leverage.** As such, global market dominance in Future Internet infrastructure carries unacceptable risks for democracies. Vietnam's rejection of territorial claims by China in the South China Sea provides an illustrative case-in-point. From 2014 to the present day, Chinese investors have frozen energy infrastructure projects in Vietnam and cyber groups linked to China have launched cyberattacks on Vietnamese airports and government officials in response to disagreements over China's maritime claims in the South China Sea. If Chinese companies grow to dominate even more of the Future Internet market, networks around the world could be shut off in response to political disagreements or at the onset of or during a military engagement.
- **Personal Data Exfiltration: CCP entities see "Alternative Data" as "New Oil."** In the Internet-of-Everything, AI-driven applications provide new and expanded avenues for vacuuming data, an essential input to technology which China aims to lead. One CCP subsidiary, Global Tone Communication Technology (GTCOM), held a conference in January 2019 with a tagline that crystallizes this mission: Alternative Data: New Oil. As the Australian Strategic Policy Institute has found, GTCOM collects global data in over 65 languages and bills itself as "the world's leading company in big data and artificial intelligence."
- **Data in, propaganda out.** Future Internet technology presents opportunities for influencing the information environment, including in applications that simultaneously perform big data collection. Chinese companies are building information platforms into application technologies, reimagining the public square and private locales as tools for propaganda—political or otherwise. ZTE's Smart Street light standard, for example, includes an advertising platform; a China-led standards group envisions future cars as "infotainment spaces;" Huawei is promoting its big data approach to "smart tourism" and cultural heritage information; and the China Broadcasting Network is a contributor to Future Internet standards-setting efforts.
- **Already victims of Chinese intellectual property theft, the United States and its democratic partners are ill-prepared to secure sensitive information as the Future Internet ecosystem explodes access points.** According to the Commission on the Theft of American Intellectual Property, trade secret theft reduces U.S. GDP by 1 to 3 percent, or approximately $180 billion to $540 billion per year. China is the world's principal IP infringer and accounts for approximately 80 percent of cases brought by the U.S. Department of Justice (DOJ) National Security Division since 2012. While the EU's data protection regime provides some natural security measures, a holistic understanding of the cost of IP theft in Europe is limited. The report calls for a comprehensive cyber risk assessment for 5G and the IoT and a European Commission to study Intellectual Property Theft in Europe.

While 5G, 6G, and the Internet generations to follow will offer significant economic opportunity around data and connected devices, they will also introduce new risks to democratic societies. For the United States, much of the turmoil surrounding the question of allowing a Chinese presence into allied telecommunications networks has focused on the threat of traditional espionage. If a Chinese vendor with unclear ties to the authoritarian one-party state and a legal requirement to cooperate with Chinese intelligence services installs—or worse, owns and operates—the backbone by which all information travels, the access afforded could render moot efforts to classify and guard sensitive information. According to the U.S. intelligence community, that concern is very real.[37] Yet the risks of a sizeable authoritarian presence in the democratic Internet go beyond espionage. Focusing narrowly on the espionage threat—as U.S. diplomatic efforts in Europe and elsewhere have—fails to play to U.S. strengths.

Instead, a more holistic understanding of the threat space is necessary, both to sharpen allied engagement on 5G and 6G and to construct collective solutions across infrastructure and application layers.

Three Risks of Data Siphoning Through Authoritarian Internet Dominance

Traditional Espionage

The chief, and at times the sole, national security argument made against using Chinese telecommunications equipment in allied networks is that it allows the CCP a clear window into classified information through a "backdoor" that can be inserted in network equipment. As such, European efforts to assess Huawei's safety have been about finding a "smoking gun" that proves Huawei equipment siphons data back to China. In January 2020, Guillaume Poupard, head of France's national cybersecurity agency ANSSI said they had not uncovered evidence of Huawei using European communications infrastructures for espionage: "There is no Huawei smoking gun as of today in Europe...There is no situation with Huawei being caught massively spying in Europe. Elsewhere maybe it's different, but not in Europe."[38]

"One Firmware Update Away"

Two facets complicate this picture. First, the absence of a smoking gun today is no guarantee that there will be no future efforts at espionage—especially as tensions between China and democracies deepen.[39] In fact, the story of China's authoritarian rise is one of building increasing dependence without significant provocation until such time that it can be used for military, economic, or political advantage—the sharp and coercive power model.[40] While that dependence is being built, there is a strong incentive by China to resist the public backlash that would arise from more brazen activity. More importantly, an increasing prevalence of software-based-systems—as 5G boasts as a feature—creates a large attack surface for software updates to introduce vulnerabilities remotely.[41] As Senator Mark Warner has put it, "This is not about finding "backdoors" in current Huawei products—that's a fool's errand. Software reviews of existing Huawei products are not sufficient to preclude the possibility of a vendor pushing a malicious update that enables surveillance in the future. Any supposedly safe Chinese product is one firmware update away from being an insecure Chinese product."[42] Vulnerabilities and bugs are a part of the software development lifecycle, as the over $100 billion global cybersecurity industry shows.[43] Actors looking to penetrate networks seek to find those vulnerabilities in order to exploit them. It is far easier and more cost-efficient for an ill-intentioned adversary to find vulnerabilities that have been self-introduced than those it needs to hunt for and which can be patched. Ultimately a risk mitigation framework is about raising the costs of adversary network penetration. In March 2019, an annual U.K. security review on Huawei equipment pointed to issues with "shoddy" engineering and basic "cyber security hygiene" giving rise to exploitable vulnerabilities.[44] Most significantly, the report concluded, "It is not possible to be confident that the source code examined by the HCSEC is precisely that used to build the binaries (software) running in the U.K. networks."[45] That is, ultimately, the U.K. body designed to oversee Huawei infrastructure in the country is unable to review the precise code running Huawei network equipment. If a vulnerability had been or is introduced, they would not necessarily see it.[46]

> *"Closer collaboration will be necessary to track, assess, and respond to threats from China, Russia, and Iran.*

Moreover, in late 2019, the U.S. government shared intelligence with allies including Germany and the United Kingdom that provided evidence of that elusive, if ancillary, backdoor. With most telecommunications companies, a lawful intercept mechanism is typically inserted into equipment for tightly controlled access by telecom operators and authorized law enforcement officers in the execution of court-ordered surveillance. There are strict restrictions on who can access that information. Intelligence reportedly indicates that in Huawei's equipment, that mechanism is designed to allow them to access the data as well—instead of bypassing the equipment vendor and going straight to the telecom operator and designated personnel.[47]

Huawei's own public messaging on this topic is also reason for suspicion. The oft-cited Chinese National Intelligence Law of 2017 requires telecommunications firms to comply with CCP data demands, clearly contradicting Huawei public statements to the contrary. Moreover, a long history of scholarship on the relationship between the CCP and Chinese companies suggests that the idea that any company could meaningfully refuse CCP demands is fanciful, built on a Westernized conception of the role of the private sector.[48]

Allied Intelligence Sharing and Mixed Messaging

The above concerns have given rise to complications over allied intelligence sharing arrangements, as some U.S. allies have yet to exclude Chinese-made infrastructure.[49] In particular, the Five Eyes intelligence sharing partnership among the United States, United Kingdom, Australia, Canada, and New Zealand is a particularly crucial fault point. Beyond Five Eyes, allied intelligence sharing, including at NATO, forms the basis of security engagement on threats from counterterrorism to disinformation.[50] Closer collaboration will be necessary to track, assess, and respond to threats from China, Russia, and Iran in the cyber and information arenas. Rifts over secure mechanisms to share information play directly into the hands of an authoritarian divide-and-conquer strategy.

For months, U.S. officials threatened to withdraw intelligence sharing from allies that refuse to exclude Huawei from 5G networks.[51] This debate came to a head in January 2020, when the United Kingdom announced an initial decision to exclude high-risk vendors like Huawei and ZTE from only "sensitive" parts of the network (including those previously labelled the 'core' as well as critical infrastructure, legal intercept, or sensitive military and intelligence systems) and capped the presence of high-risk vendors to 35 percent of the access network.[52] That week, U.S. Secretary of State Mike Pompeo visited the United Kingdom and provided reassurances that the U.S.-U.K. intelligence sharing relationship would find a way to operate securely despite a decision that did not issue a complete ban: "With respect to information and the Five Eyes relationship, that relationship is deep, it is strong, it will remain," he said. "All the elements of the five eyes will work together on this to ensure that the systems are sufficiently secure."[53] In February 2020, however, U.S. officials sent mixed messages on the future of allied intelligence sharing. Within the span of a few days overlapping with the Munich Security Conference, President Trump's senior advisor Robert Blair said in reference to the United Kingdom that there would be "no erosion in our overall intelligence-sharing," while U.S. Ambassador to Germany Richard Grenell repeated the caution that "any nation who chooses to use an untrustworthy 5G vendor will jeopardize our ability to share intelligence and information at the highest level."[54] Deputy Assistant Secretary of State for Cyber and International Communications and Information Policy Robert Strayer also noted that the United States was "required by law to reassess our intelligence sharing relationship with anyone who uses Huawei." The upshot of this mixed messaging is little clarity for U.S. allies on the extent to which allied intelligence sharing will be undermined by the inclusion of untrusted Chinese vendors into parts of the network.

Cordoning Off the Network

The ability for the United States to share intelligence with allies that continue to use Huawei equipment in select, non-critical parts of their 5G networks and the ability of those allies to protect their own sensitive information partly hinges on the ability to cordon off some parts of the network from others. At least publicly, there has been disagreement, including within Five Eyes, on whether this separation is possible. Implicit in the U.K.'s January 2020 decision was that with exclusions and regulatory safeguards, it would be possible to construct a system architecture that sufficiently mitigates risk, while including high-risk vendors in portions of the network. By contrast, in a post for the Australian Strategic Policy Institute, former head of signals intelligence and offensive cyber missions for the Australian Signals Directorate Simeon Gilding asserted that the Australian government attempted to design cybersecurity controls to "prevent a sophisticated state actor from accessing our networks through a vendor. But we failed."[55] Australia banned Chinese vendors Huawei and ZTE from its 5G networks in August 2018. [56] Gilding writes that the United Kingdom has "doubled down on a flawed and outdated cybersecurity model to convince themselves that they can manage the risk that Chinese intelligence services could use Huawei's access to U.K. telco networks to insert bad code." The United States arrived at similar conclusions back in 2012. A seminal House Intelligence Committee report assessed that "Huawei and ZTE cannot be trusted to be free of foreign state influence and thus pose a security threat to the United States and to our systems."[57] The United Kingdom has toughened its stance, but the considerations therein should serve as a guide to democratic nations examining these decisions in the coming months and years.

State of the 5G Landscape in Europe

In January 2020, European Union member states adopted the EU Toolbox for 5G Security and EU Toolbox of Risk Mitigation Measures for cybersecurity of 5G networks that provided guidance on holistic risks, including from high-risk vendors and potential mitigations.[58] It leaves up to individual member states how each will implement the toolkit, and the past year has seen some nations move to exclude or phase out Huawei from 5G networks. In other cases, national telecom operators have chosen to move away from high-risk vendors and opt for trusted European suppliers. In some countries, Huawei is expected to remain. In the east, Romania, Poland, Estonia, Latvia, and the Czech Republic have signed joint statements with the United States on 5G and some have moved to exclude Huawei.[59] Poland is considering legislation that would restrict the new purchase of Huawei equipment, but not require a rip-and-replace of the gear from 4G networks.[60] The Czech Republic hosted the 5G Security Conference and spearheaded the establishment of the Prague Proposals for 5G Security, which outline vendor-neutral considerations for the adoption of secure 5G systems. The Proposals fall under four categories: Policy; Technology; Economy; and Security, Privacy, and Resilience. In particular, they reference a vendor's rule of law environment and economic fairness.[61]

Since the summer of 2020 and in the wake of Beijing's failed "wolf warrior" diplomacy initiative over the coronavirus, there has been a small shift in European approaches to Huawei. In July, France moved to phase out Huawei by restricting the renewal of Huawei licenses once they expire, amounting to a de-factor exclusion by 2028.[62] Around the same time, the United Kingdom decided to pursue a similar approach, despite a January 2020 decision to allow high-risk vendors in non-sensitive areas of the network (capped at 35 percent). By July, Britain had decided to ban the new purchase of Huawei equipment after December 31, 2020 and to require a phase out of Chinese 5G equipment by 2027.[63] And in a significant finding in October 2020, a U.K. parliamentary committee concluded directly that there was "clear evidence of collusion" between Huawei and the "Chinese Communist Party apparatus," suggesting a possible expediting of the phase-out timeline to 2025.[64] The report cited Huawei's state subsidies from the CCP and came on the heels of an October 2020 report by the country's GCHQ National Cyber Security Centre finding that Huawei had failed to adequately address security flaws and only "limited progress" in remediation of identified problems had been made.[65]

Among the most significant developments in fall 2020 was in Germany, which has been considered a linchpin state for 5G in Europe that smaller nations might follow. An IT security bill that Chancellor Merkel's cabinet is reported to pass in fall 2020 would also move to phase out Chinese vendors. While not providing an explicit ban, the legislation would likely raise the bar so high in terms of a "trustworthiness" assessment that Huawei would be incapable of clearing it.[66]

In the face of national government-level moves to reconsider Huawei's presence in 5G networks, leading telecom operators in some countries have selected alternative vendors to build out 5G in advance and in possible anticipation of regulatory decisions. In October, Belgian operators Orange Belgium and Proximus dropped Huawei in favor of European suppliers Nokia and Ericsson, selecting Nokia to build out the radio access network and Ericsson to supply the 5G core. Telenet, the third major operator in Belgium, which holds strategic importance due to its seats of the EU and NATO in Brussels, has relied on China's ZTE in the past and plans to make a supplier decision by mid-2021.[67] After economic threats from Beijing over the decision, Denmark's minister of defense announced a desire to use suppliers from countries with whom there are existing alliances.[68]

Some states have been slower to act on the EU's recommendations for cyber risk mitigation, leaving Huawei an option especially in the RAN. In Italy, the future of Huawei is still up in the air. Telecom Italia, Italy's major carrier which also builds networks in Brazil, excluded the Chinese vendor from a 5G core network tender, and deeper discussions are ongoing.[69] In Spain, Huawei was granted a security clearance in June 2020.[70] In Portugal, no ban is on the horizon, but its major operators have chosen to exclude Huawei from the 5G core.[71] Ireland has made no public moves to exclude high-risk vendors, with its top telco provider Eir affirming trust in Huawei's security and stating in September 2020 that it would move ahead with the Chinese vendor for its RAN (Eir uses Ericcson for the core).[72] States such as Austria, Sweden, and Finland have yet to take a clear position.

Commercial Espionage

Even if military-sensitive portions of 5G networks could be cordoned off, classified national security information is far from the only information that democracies should be concerned about protecting from authoritarians. Targeting of the private sector, a key pillar of democratic nations, through the theft of commercial and trade secrets has long formed an essential part of China's strategy to compete in emerging technologies.[73] The Made in China 2025 plan, released in 2015, outlines ten critical technology areas in which China intends to reduce foreign dependence to achieve homegrown leadership from robotics and IT to aviation, transportation, and biopharma. The DOJ has issued charges of IP theft against Chinese actors in eight of those fields.[74]

The CCP, People's Liberation Army (PLA) cyber activity groups, and connected technology firms pursue a range of tactics to steal intellectual property, with cyber intrusions an important element of that toolkit. U.S. and allied companies are uniquely susceptible. According to the 2018 Section 301 investigation report from the Office of the United States Trade Representative, "For over a decade, the Chinese government has conducted and supported cyber intrusions into U.S. commercial networks targeting confidential business information held by U.S. firms." The report further assesses that information gained through cyber intrusion by the Chinese government is then fed as competitive intelligence to state-owned firms through a formalized process. [75] These firms have the resources of the world's second largest economy as corporate espionage providers.

In the United States, this targeted strategy of cyber-enabled IP theft of critical technology has resulted in tremendous costs to both the U.S. economy and its technological competitiveness. According to the Commission on the Theft of American Intellectual Property, trade secret theft reduces U.S. GDP by 1 to 3 percent, "meaning that the cost to the $18 trillion U.S. economy is between $180 billion and $540 billion."[76] China is the world's principal IP infringer and accounts for approximately 80 percent of cases brought by the DOJ's National Security Division since 2012.[77]

> *"The long-term competitiveness of European advanced technology companies depends on securing its innovation.*

Huawei itself is a notable case-in-point. The company's rise to prominence in the telecommunications market is littered with flagrant intellectual property theft, backed by the leverage of government-controlled access to the Chinese market to pressure accusers into continuing business relationships with Huawei.[78] A February 2020 Justice Department indictment details Huawei's theft of nonpublic intellectual property including robotics equipment, cellular-antenna technology, and Internet router source code from six U.S. companies—Cisco, T-Mobile, and Motorola identifiable among them.[79] Huawei's deliberate and deceptive scheme to steal proprietary phone testing technology from T-Mobile was documented in the January 2019 charging documents from the Western District of Washington. After carefully cultivating a relationship with T-Mobile US (the U.S. subsidiary of Germany's Deutsche Telekom) to gain entry into the U.S. mobile phone market, Huawei sought to acquire—first by licensing, then by theft—the designs for a robotic phone tester called Tappy, which allowed T-Mobile a competitive market advantage in producing error-free phones. The indictment cites e-mail exchanges between Huawei China headquarters and engineers in T-Mobile's Bellevue facility over the course of nine months with taskings, requests, and reminders for the Seattle-based engineers to photograph and provide specifications of Tappy so that Huawei China could replicate the testing device for its own phones. After numerous reports to Huawei China that T-Mobile would not provide the information and that their questions were angering T-Mobile, Huawei China sent an engineer working on Huawei's Tappy copy, the xDeviceRobot, to the United States to take unauthorized photos of the device, improperly accessing the secure facility in which Tappy was housed with the badges of Huawei's U.S.-based employees. Eventually, one Huawei engineer absconded with Tappy's robotic arm in his backpack. Huawei claimed that the employee acted on his own and fired him.

The indictments also detail a formal bonus program instituted in 2013 to reward Huawei employees who stole confidential information, with the reward based on the value of the information obtained:

> "Employees were directed to post confidential information obtained from other companies on an inter-

> nal HUAWEI website, or, in the case of especially sensitive information, to send an encrypted email to a special huawei.com email mailbox. A 'competition management group' was tasked with reviewing the submissions and awarding monthly bonuses to the employees who provided the most valuable stolen information. Biannual awards also were made available to the top "Huawei Regional Divisions" that provided the most valuable information. A memorandum describing this program was sent to employees in the United States."[80]

At times, Huawei employees were required to give fake company names at trade shows and to foreign law enforcement officials in order to conceal their affiliation. More subtly, Huawei capitalizes on funding relationships with universities around the world to access patented technology. Universities, too, have been the targets of Chinese state-sponsored cyber espionage.[81]

Of course, Huawei is far from the only Chinese company engaged in wide-scale corporate espionage. A directive from China's Ministry of State Security, for example, is thought to be responsible for a large-scale hacking operation to acquire technology to build state-owned Comac's C1919 airplane to compete with Airbus and Boeing.[82] Beyond the theft of costly R&D itself, Chinese hackers target cost and pricing data, internal strategy documents, negotiating positions, trade secrets, sensitive communications, and other valuable business information.[83] According to FBI Director Christopher Wray, the FBI has about 1,000 pending cases against China's attempted technology theft actors across 56 field offices.[84]

Chinese IP Theft: U.S. Policy

Despite efforts by the Obama administration to quell Chinese economic espionage, most notably a 2015 joint statement with Chairman Xi Jinping pledging to cease corporate IP theft, the scale of these activities is on the rise.[85]

The DOJ's renewed focus on quelling commercial IP theft from China through its 2018 initiative to combat Chinese economic espionage is a helpful step towards prosecuting these cases and raising awareness on how these firms exploit U.S. innovation.[86] However, more needs to be done to align private sector incentives in the direction of reporting this behavior to federal authorities in the first place. A 2019 investigation by NPR and PBS found that for decades U.S. businesses failed to report Chinese IP theft, as they feared action by the U.S. government against Chinese firms would threaten their business prospects in China. Even when companies did call in suspicions of cyber activity by China, and authorities identified covert Chinese PLA Unit 61398 as responsible for an array of attacks, no U.S. companies were willing to be plaintiffs. To this day, most still will not come forward.[87]

Additionally, a more thorough understanding of the entry points of cyber intrusion into business and personal networks that can lead to the exfiltration of corporate data is needed in the 5G and Internet-of-Everything era. The United States has not produced a comprehensive risk assessment of future networks or a plan to mitigate these risks.

Chinese IP Theft in Europe

Although European nations have studied cybercrime and IP theft to varying degrees, the scope and scale of IP theft, especially by China, is not comprehensively understood at the EU-level. The BfV, Germany's domestic intelligence agency, estimated that German firms lost €55 billion ($65.3 billion) to espionage, sabotage, and data theft in 2016. Chinese hackers in particular have targeted Germany's leading manufacturing technology sector. In the telecommunications realm, Deutsche Telekom AG said it detected 30,150 cyberattacks from China in a single month in 2017.[88] In the Netherlands, the Military Intelligence and Security Service (MIVD) warned of the threat of the theft of dual-use technical knowledge by China in a 2019 annual report.[89] The Ministry of Foreign Affairs also discussed this threat in a 100-page strategy on China.[90] Germany's BfV has issue similar warnings.[91] In 2018, the United States and United Kingdom jointly accused Chinese hackers from the APT10 group of what the U.K. foreign minister called "one of the most significant and widespread cyber intrusions against UK and allies uncovered to date, targeting trade secrets and economies around the world" in industries from pharmaceuticals to aviation.[92] A 2011 U.K. report concluded that the cost of cybercrime due to IP theft totaled £9.2 billion per annum.[93]

The long-term competitiveness of European advanced technology companies depends on securing its innovation. Fortunately, the EU is ahead on some of the tools. The breach notification requirement in the EU's General Data Protection Regulation (GDPR) is excellent grounding for expanded requirements on the reporting of IP theft. The EU has already brought a World Trade Organization (WTO) suit against China, while recognizing in some countries that WTO tools are inadequate. However, a greater, more public understanding of how China illegally appropriates IP and the economic cost to European innovation is needed.

Personal Data Exfiltration

In the information age, personal data has also taken on increased economic and national security import—and with it, an escalation of concerns surrounding privacy and government access. For democracies, protecting the explosion of citizen data that the Internet-of-Everything generates will be vital for securing both their values and global competitiveness vis-à-vis authoritarian regimes.

Authoritarian states like China, Russia, and, increasingly, Iran have seized on the value of personal data, boosted by advances in AI and specialized processors that analyze it. China in particular is engaged in efforts to vacuum up global data, including that of citizens in democracies. In 2017, Chinese military-based hackers stole addresses, birth dates, Social Security numbers, and other data on approximately 145 million Americans in a cyberattack on consumer credit reporting agency Equifax. The FBI described the intrusion as "the largest known theft of personally identifiable information ever," and identified it as one of many examples of China's interest in collecting Americans' person data.[94] In late 2018, the Marriott hotel chain announced a breach of its systems, which allowed the exfiltration of hundreds of millions of customer records, including credit card and passport numbers. In February 2020, the U.S. DOJ attributed the attack to China just weeks before a second Marriott data breach was announced targeting account passwords or PINs, payment card information, passport information, national IDs, and driver's license numbers.[95] Chinese hackers have also been linked to major personal data breaches at the Office of Personnel Management (OPM) and medical insurance company Anthem.

> *"Part of data's value is its ability to shape the narrative.*

In the bio-economy, the Chinese government is amassing DNA surveillance information on its Uyghur population in Xinjiang.[96] Outside Xinjiang, China's biotechnology behemoth BGI Group collects genetic information for use in the future of the biotechnology industry with personalized medicine.[97] BGI also partners with Huawei on big data storage for its genetic research. A key element of BGI's rise from the scientist-founded nonprofit Beijing Genome Initiative to gene giant status was its $118 million acquisition of California-based Complete Genomics in 2013—a sale that received clearance from CFIUS back in 2012. At the same time as China is amassing DNA information on its own population and beyond, the government seeks to limit the ability of genetic data to flow outside the country. [98] The much-hyped "social credit systems" too rely on concatenating massive quantities of personal behavioral information.[99]

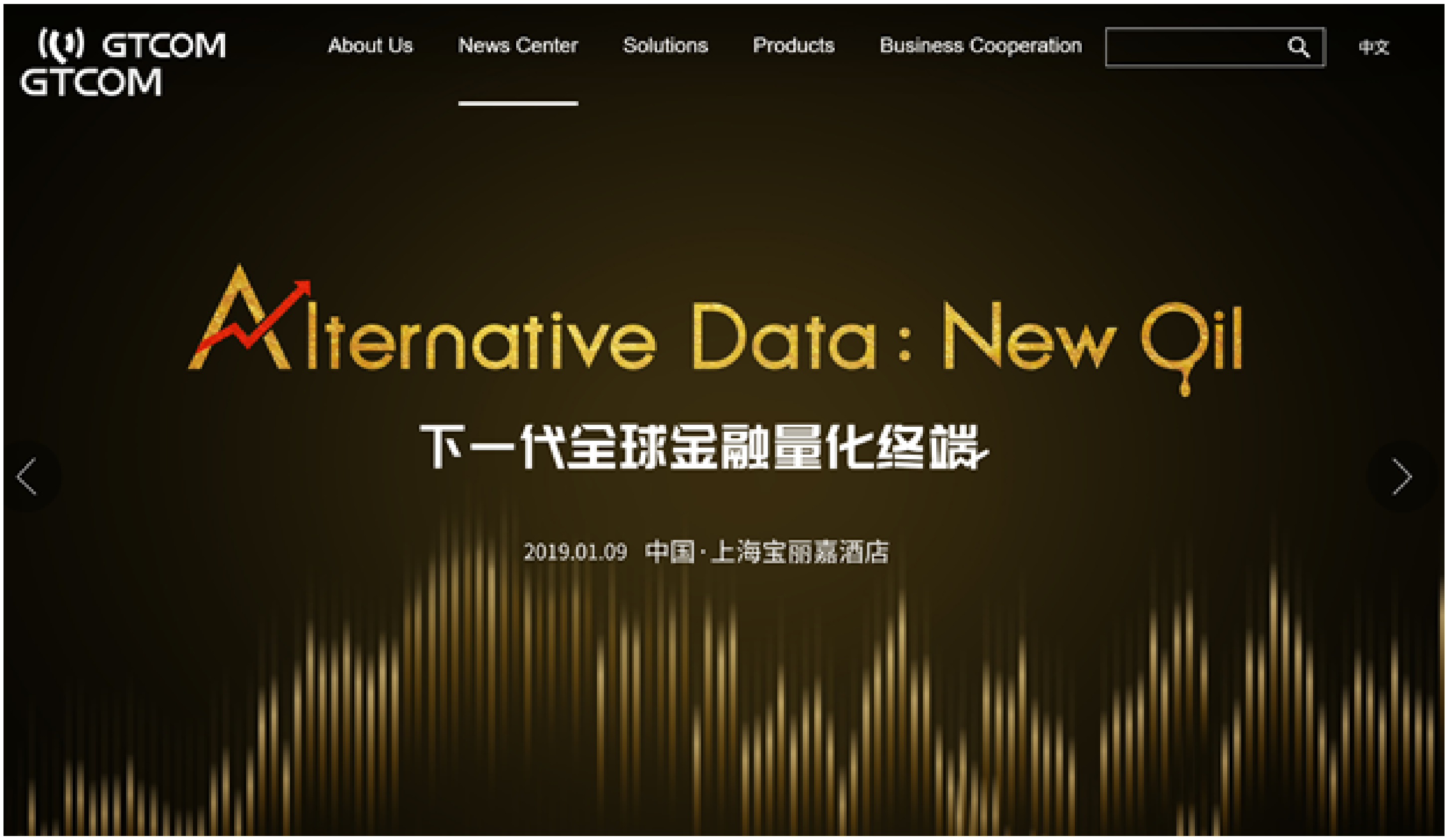
China's Central Propaganda Department: "Alternative Data: New Oil"

China recognizes the economic and geopolitical value of data and is building a Future Internet apparatus to gain and harness this advantage across the information environment. This apparatus is partly connected to China's Central Propaganda Department, which should alert democracies to the nexus between Future Internet application technology and the ability of authoritarians to shape our information realities.

A 2019 report by the Australian Strategic Policy Institute (ASPI) assessed that China is building a "massive and global data-collection ecosystem" using state-owned enterprises, Chinese technology companies, and partnerships with foreign actors and institutions, including universities.[100] One notable entity that ASPI analyst Samantha Hoffman details in the report, the Global Tone Communications Technology (GTCOM) is a subsidiary of the China Publishing Group, a state-owned enterprise under the direct supervision of China's Central Propaganda Department.[101]

Far from being a mere publisher, GTCOM bills itself as "the world's leading company in big data and artificial intelligence," marketing products from speech recognition and machine translation to chatbots, FinTech solutions, educational platforms, and virtual conferencing software. In so doing, GTCOM vacuums up global data in over 65 languages, analyzes it, and likely pipes that data back to China for government and corporate use. One platform highlighted in the ASPI report called Insidersoft collects ten terabytes of data every day and the equivalent of 20 billion Facebook photos annually through machine translation and speech and video recognition software.

Drawing on an analogy popularized by the Economist between data and oil to highlight the growing geopolitical importance of data, GTCOM held a conference in January 2019 with a tagline that crystallizes its mission: Alternative Data: New Oil.[102]



Source: GTCOM, Screenshot 5.13.20.[103]

In addition to indicating that China's personal data exfiltration ambitions come from the CCP, of particular concern from the standpoint of the deployment of Future Internet and smart city technology is that GTCOM has strategic partnerships with Huawei and Alibaba Cloud.[104] In a May 2019 agreement touting "the strategic synergy between the two in the field of AI big data," Huawei promised GTCOM "powerful global data transmission and marketing support in order to expand the scenario-based application of AI, big data technologies in different fields by deeply mining and exerting its impressive resource value."[105]

The uses of these troves of personal data collected by GTCOM, Chinese hackers, and future IoT vendors range from surveilling populations and arresting dissident journalists to tracking intelligence assets, exploiting personal information for kompromat, feeding personal data into AI systems, and developing micro-targeted manipulation for information warfare narratives. With social engineering and targeted phishing, personal data is also a window into corporate or other intrinsically sensitive data.[106] It is also notable that the CCP's global data collection and processing efforts are tied to its propaganda department, signaling that whether through surveillance or content generation, part of data's value is its ability to shape the narrative.

The connection between information influence and big data platforms is borne out across the application layer of the Future Internet, as the Internet-of-Everything presents new opportunities for influence. Chinese companies are building information platforms into application technologies, re-imagining the public square and private locales as tools for propaganda—political or otherwise. ZTE's Smart Street light standard, for example, includes an advertising platform; a China-led standards group envisions future cars as "infotainment spaces"; Huawei is promoting its big data approach to "smart tourism" and cultural heritage information; and the China Broadcasting Network Corporation is a contributor to Future Internet standards-setting efforts.[107] China Broadcasting Network Corporation's business includes "Cable television network planning, construction, operation, and maintenance; technical research, technical development, and information consulting for the aforementioned developments; design, production, representation, and publication of advertisements; broadcast television programming production, conveying programing, and Video-on-Demand service; value-added telecommunication service."[108]

Personal Data in the United States and EU

In recent years, the United States has begun to recognize the counterintelligence problem posed by personal and sensitive data ownership and taken steps to block certain transactions. In March 2019, the Committee on Forum Investment in the United States (CFIUS), which can review corporate transactions of national security concern, required Beijing Kunlun Tech, the Chinese owner of LGBTQ dating app Grindr, to divest from the company reportedly over concerns that access to the personal information—messages, locations, sexual orientation, and even in some cases HIV status—of Grindr's 3.3 million daily users constitute a national security issue.[109] The sale was completed a year later.[110] In March 2020, the White House ordered Beijing Shiji Information Technology to divest from cloud-based hotel software company StayNTouch and its assets on similar grounds of access to personal information on hotel customers.[111] Most publicly, the acquisition of Musical.ly by Chinese firm ByteDance, now the owner of explosive video sharing app TikTok was also reviewed by CFIUS, leading up to the Trump Administration's Executive Orders and moves to ban TikTok.[112] While the review was initiated by lawmaker inquiries, the national security process gave way to chaos from the White House over a potential outright ban of the app. The increased CFIUS scrutiny of Chinese-owned platforms that can collect Americans' data comes as U.S. reforms to CFIUS provide for expanded use of this mechanism.

European countries from France and Germany to the United Kingdom and Norway have also expanded or created CFIUS-like authorities that may be able to address such threats on the Continent.[113] The EU also issued its own foreign screening mechanism that includes specific mention of the threat of data acquisition, though concerns remain that the mechanism will lack efficacy even when fully implemented.[114] In general, EU nations benefit from stronger data protection authorities through GDPR, which may be drawn on in cases where there is clear, non-consensual data transfer.

In the case of TikTok, democracies must rely on process. A growing cadre of democracies is raising concerns about TikTok and Chinese information influence in the wake of Beijing's failed coronavirus diplomacy offensive.[115] India has already banned TikTok; the app has drawn recent scrutiny from U.K. lawmakers and the Australian parliament questioned; the EU data protection regulator and several EU member states including France, Denmark, and the Netherlands are also investigating TikTok for its data security and privacy practices.[116] Rather than defaulting to unilateral action on TikTok and WeChat, advancing democratic principles and national security over U.S. economic interests requires the United States to act in concert with allies.

Even if the military sensitive areas of 5G networks are free of high-risk vendors, there is a strong counterintelligence case for protecting the rest of the network as well. As the vignettes in Section 2 illustrate, much of 5G computing will happen at the edge, and more and more of the data generated may be vulnerable to exfiltration—either by dedicated hacker groups or by IoT platforms or "apps" that run atop 5G networks. At the same time, research into 5G networks has already uncovered security flaws that expose inter alia a user's location.[117]

The EU has recognized the importance of protecting that data at the application layer and putting it in the hands of consumers that generate it. This data must also be protected at the infrastructure layer—in part by excluding high-risk vendors throughout the network. But banning Huawei and ZTE from 5G networks alone is not sufficient to solve the problems of data siphoning. To secure networks against these threats, comprehensive cyber risk assessments for 5G and 6G are needed.

Infrastructural Dependence and Geopolitical Manipulation

Beyond the economic, national security, and geopolitical risks of data siphoning presented by inadequately secured 5G networks and those built by high-risk vendors, a dependence on Chinese infrastructure increases economic and political leverage for the CCP.

The CCP has already shown its willingness to use infrastructural dependence for geopolitical leverage. Vietnam's rejection of Chinese territorial claims in the South China Sea provides an illustrative case-in-point. In 2014, when a tussle erupted between Vietnam and China over China's maritime claims, Chinese investors froze energy infrastructure projects in Vietnam.[118] In 2016, when the UN's Permanent Court of Arbitration rejected China's territorial claims, hackers attributed to mainland China disabled television screens and sound systems in the Hanoi and Ho Chi Minh City airports for hours—filling them with CCP propagandist messages and requiring agents to check passengers in by hand.[119] More recently in May, a hacking group with suspected ties to the Chinese government known as Pirate Panda launched a spear phishing campaign targeting Vietnamese government officials in Da Nang, Vietnam, near the disputed Paracel Islands in the South China Sea.[120] Discovery of the campaign came just days after Vietnam again rejected China's claims to the Paracel and Spratly islands.[121]

> ***"Setting governance standards to accord with its own censorship and suppression practices is part of the CCP's mission to make the world safer for China.***

If Chinese companies grow to dominate even more of the market and further expand the CCP's infrastructural influence, Huawei and ZTE-dominated networks around the world could be shut off in response to political disagreements or at the onset of or during a military engagement. The mere threat of this activity would endow the CCP with coercive geopolitical, diplomatic, and military leverage even in relative peacetime. Therefore, to ensure the continued competitiveness of trusted vendors, maintaining the overall health of the global telecommunications industry is an allied national security imperative.

On the present trajectory, however, Huawei is able to undercut its competitors by 20 to 30 percent, buoyed by over $75 billion in state support from the CCP and over a decade of determined IP theft.[122] If these anti-competitive measures are allowed to continue unchecked, and Huawei further consolidates market share, there is a risk that when it comes time to build future generations of the Internet, trusted vendors will have been completely pushed out of an already competitive market. Instead of high-risk vendors comprising 35 percent of a network, that number could grow to 80 or 90 percent.

For democracies reliant on secure communications systems, free from the possibility of data siphoning by authoritarian regimes or Internet shutoffs, this dependence would be an unacceptable scenario. Thus, care is needed to ensure the health of a democratic telecommunications industry. Commercial actors within the United States and its democratic allies regularly assess this industry, but national security apparatuses should do so as well.

Governance Propagation

Finally, 5G inroads at the infrastructure layer pave the way for Huawei smart and "safe" city technology purchases at the application layer, which come with police and cyber governance trainings which diffuse authoritarian norms for surveillance, crowd control, and population monitoring. Whether learning how to identify threats in a crowd by studying an individual's walking gait or "public opinion guidance"—a euphemism for censorship that uses AI to monitor citizens' speech—as Chinese-made 5G technology spreads worldwide, so too do the norms that govern its innovation.

Moreover, as a 5G first mover, Huawei holds a competitive advantage in the myriad big data applications 5G enables in the markets it dominates. How companies, governments, and societies think about data collection, privacy, the ability of the government to find citizens, access communications, and control dissent is set by technology first movers. In the case of China, setting governance standards to accord with its own censorship and suppression practices is part of the CCP's mission to make the world safer for China. After installing Huawei 4G equipment, video surveillance software, and facial recognition technology, Kenya, Tanzania, Vietnam, and Zimbabwe have to varying degrees seen the adoption of draconian cybercrime laws restricting Internet freedom and clamping down on speech against the government.[123] ZTE and China Mobile pushed for the adoption of an international standard that codifies the ability to add video monitoring capabilities to smart street lights. And by policy, the CCP's "Standards China Unicom Joint Construction 'One Belt, One Road' Action Plan" calls for Chinese 5G standards to be implemented in Belt and Road countries.[124]

The Need for a Global Solution

The distributed reality of today's global telecommunications market, as well as the technocratic process by which international standards on next generation networks are set also demand a collaborative response from U.S. allies and partners.

The Global 5G Industry Landscape

- The 5G industry consists of five layers: foundational technologies, cellular infrastructure, chipsets, devices, and carrier networks. A quick examination of the dominant players in each layer shows the globally distributed marketspace and suggests cooperative business models for 5G.
- Foundational technologies. The research, patented innovations, and standards underlying 5G advances, such as advanced channel coding, massive MIMO, and mobile mmWave that open up 5G applications. This layer is research and capital intensive. Key players include: Qualcomm (USA), Huawei (China), Ericsson (Sweden), Nokia (Finland), Samsung (South Korea), ZTE (China), NEC (Japan).
- Cellular infrastructure. Base stations, routers, and switches that are traditionally hardware elements but increasingly involve software in 5G. Capital intensive, low payoff without downstream sales. Key players include: Huawei, Ericsson, Nokia, Samsung, ZTE.
- Chipsets. Systems on a chip, including 5G modems and processors. Key players include: Qualcomm, MediaTek (Taiwan), HiSilicon (for Huawei), Samsung (for their own).
- Devices. Phones, tablets. Key players include: Samsung, Huawei, Apple (USA), Xioami (China), Oppo (China), Vivo (China), Motorola (USA), LG (South Korea), HTC (Taiwan) and more.
- Carrier networks. Key players include: AT&T, Verizon, Vodafone, China Mobile, DoCoMo, Deutsche Telekom, and more.

Three key findings follow from this landscape picture:

First, the United States at present cannot go it alone on 5G—if for no other reason than that there is no U.S. cellular infrastructure provider with any significant market share. There is no option for a U.S. firm to supplant Huawei in the developing world or anywhere, so finding a viable alternative requires international cooperation. At present, neither Ericsson, nor Nokia, nor Samsung can compete with Huawei on cost.

Second, joint progress in building viable alternatives is hindered by the distributed origins of different elements of the supply chain in different states. Germany is an interesting case in point. Its national 5G leader, carrier network Deutsche Telekom, has warned against excluding Huawei from German 5G networks on the basis of roll-out delays.[125] Telekom partners with Huawei as its infrastructure provider for thousands of wireless towers as well as cloud products, and has a strong financial incentive not to switch to a costlier Ericsson or Nokia. Secure 5G on the continent is not just a matter of Europeans buying European, but Germans buying Swedish. This complexity is intensified by China's own economic pressure, derived from its manufacturing base for, among other industries, German cars. In December 2019, for example, Chinese Ambassador to Germany Wu Ken issued a thinly-veiled threat against the German auto industry if the nation were to exclude Huawei from its 5G networks. "Can we also say that German cars are not safe because we're in a position to manufacture our own cars? No, that would be pure protectionism," Wu Ken reminded a Berlin audience as he warned "there will be consequences" for a Huawei ban.[126] In 2018, one quarter of vehicles sold in China were German, and China was Volkswagen's largest market, comprising 40 percent of sales.[127] Germany is not alone. India and the United Kingdom have received similar threats of "consequences" over Huawei.[128] Indeed, one of the strongest cases for stemming the expansion of Chinese critical Internet infrastructure in democracies is in limiting the spread of coercive economic leverage.

Third, Huawei enjoys a competitive advantage from vertical integration of all five elements of the 5G technology stack. It is also worth noting that this interoperability can spawn hidden security vulnerabilities as components interface with each other. Indeed, while it is often cited that Huawei is the only company to play in all five 5G domains, Samsung too has cross-cutting capacity, if substantially lower market share.

The market and technical realities are such that simply excluding Huawei from allied 5G networks will not assure a trusted future for global telecom. Moreover, the needs in Western Europe differ dramatically from those in sub-Saharan Africa. A one-size-fits-all-solution is infeasible.

International Standards Setting

Key Findings

- **The contest to shape 6G standards is already underway—with China leading the charge internationally.** China leads the international technical focus group developing the first input into 6G standards, and is already using that focus group to promote a new Internet protocol standard that would help centralize Internet control in the hands of the state. As the United States plays catch up on 5G, this "Network 2030" initiative of the ITU has been underway since 2018 under Chinese leadership and is setting the conversation on 6G. To avoid being caught on the back foot yet again, the United States should join with democratic partners to establish 6G partnership centers for R&D and governance.
- **China outnumbers the United States nearly two-to-one in participation and leadership of critical international Future Internet standards-setting efforts.** At the Third Generation Partnership Project (3GPP), 174 China-based member companies, universities, and government research institutes dwarf the United States' 93 full voting members. At the ITU (whose overall membership includes more U.S. members than Chinese), ongoing Telecommunications Focus Groups on Future Internet technologies from next generation networks to autonomous driving are chaired twice as often by Chinese members as by U.S. members.
- **The world's oldest UN agency is being leveraged as a propaganda mouthpiece for the CCP's Artificial Intelligence and Future Internet agenda, whitewashing human rights abuses.** The ITU aggressively promotes Chinese companies, universities, government entities, and AI principles, whitewashing their human rights abuses under the banner of "AI for Good." The focus on AI-driven Future Internet applications with societal benefit in support of the UN Sustainable Development Goals (SDG) and irrespective of individual rights builds on and supports China's effort to shape human rights at the UN to put economic development, not individual liberty, at their center.
- **A symbiotic relationship has developed between China's Belt and Road Initiative and UN agencies involved in Future Internet and digital development.** The UN is increasingly linking the SDGs and the Belt and Road Initiative, as seen in organizations like the ITU and UNESCAP. At the same time, China is exporting its domestic technology standards along the Belt and Road Initiative by including standardization clauses in BRI MOUs.

In light of the geographic and capacity distribution of telecommunications market players, international standards for new technologies are necessary for components and operations developed by one company in one country to function in other parts of the world. As the patents included in international standards are then used by countries and companies that implement the standard, how these standards are set—and which patents developed get included in the global standards—have implications for the success of these firms. Qualcomm, for example, derived more than one-fifth of its 2018 revenue—$5.2 billion—from technology licensing fees deriving from its patents.[129] Given the technical and market complexities of the information and communications technology (ICT) sector, there exist numerous international bodies with engineers from a range of countries and companies coming together to define the standards governing next generation networks and infrastructure. Increasingly, international standards-setting bodies for Future Internet technologies have also decided not just which technologies are used, but how.[130]

> *"China is already shaping the development of 6G.*

At present, China outnumbers the United States in full voting membership by nearly two-to-one at 3GPP, one of the two principal organizations responsible for the development of next generation telecommunications standards.[131] At the other organization, the ITU, China leads the focus group charged with developing the initial input into 6G standards, with work commencing two years ago. China also outnumbers the United States two-to-one in its chairmanship of key emerging technology focus groups of the ITU's Telecommunications branch (ITU-T) that chart the development of Future Internet technologies at the infrastructure and application layers from the autonomous vehicles for transport to its use as an "infotainment space and smart living platform."[132] As the United States ponders how it ended up on the back foot with regards to 5G, China is already shaping the development of both 6G and the applications that will sit atop both networks for years to come.

China's Strategy: An Industrial vs. Decentralized Approach to Future Internet Standards

In contrast to the decentralized, industry-led approach that has historically been the mainstay of activity at international standards-setting bodies, China has taken a state-coordinated approach to leadership and prominence in setting Future Internet infrastructure and application standards. It has coordinated industry and government policy towards the rapid development and deployment of both Non-Standalone (NSA) and Standalone (SA) 5G.

The 5G Promotion Group

In 2013, three Chinese government ministries—the Ministry of Industry and Information Technology, the National Development and Reform Commission, and the Ministry of Science and Technology—came to together to form the IMT-2020 5G Promotion Group. This group includes the major Chinese telecom players—research institutes, operators, infrastructure providers, and mobile device manufacturers—and coordinates government and industry on 5G development and standards. Its work also includes collaborations with the United States, the European Union, Japan, and South Korea.[133]

Standards Strategy: China Standards 2035

In March 2018, the Standards Administration of China (SAC) and Chinese Academy of Engineering launched a two-year standards strategy research project, "China Standards 2035."[134] The four subjects of the project include strategic research on the orientation and objectives of standardization, China's standardization system, requirements for a high-quality development standardization system, and military-civil integration development. Its initial focus is on 5G, virtual reality, integrated circuit design, and intelligent health care, with plans to expand to the IoT, and integrated equipment.[135] In one notable example of this focused, whole-of-society attention, state-sponsored academics used game theory to design an information standardization approach in manufacturing.[136]

Flooding the Landscape

China's recognition of standards setting as a strategic priority has borne fruit in its growing influence in 5G standards. As of February 4, 2019, Huawei leads the world with 1,529 5G "standards-essential patents." Because these patents are incorporated into 5G standards through the 3GPP, they entail significant revenue in licensing fees when the standards are implemented—regardless of which company implements them. Along with Huawei, Chinese companies as a bloc (including ZTE, Oppo, and state-owned China Academy of Telecommunications Technology) own 36 percent of 5G standards-essential patents. By some measures, Huawei similarly leads the industry in the number of 5G technical standards proposals submitted with 11,423.[137] By sending larger delegations to standards meetings, reportedly directly incentivizing standards submissions, and providing bonuses to Chinese representatives who secure a leadership position in standards working groups, China is flooding the standards landscape with its own 5G contributions.[138]

Leveraging the Belt and Road Initiative (BRI)

Finally, China can leverage its "digital silk road" initiative to build de facto technical standards on the ground, and increase international support for its own standards.[139] As Chinese technology diffuses through the BRI, additional entities can support its standards in international meetings. This symbiotic relationship between standards bodies and the BRI goes both ways. Through its leadership in the UN-based standards setting body, the ITU, China directs UN advocacy directly in support of the BRI.[140]

The Polar Coding Issue

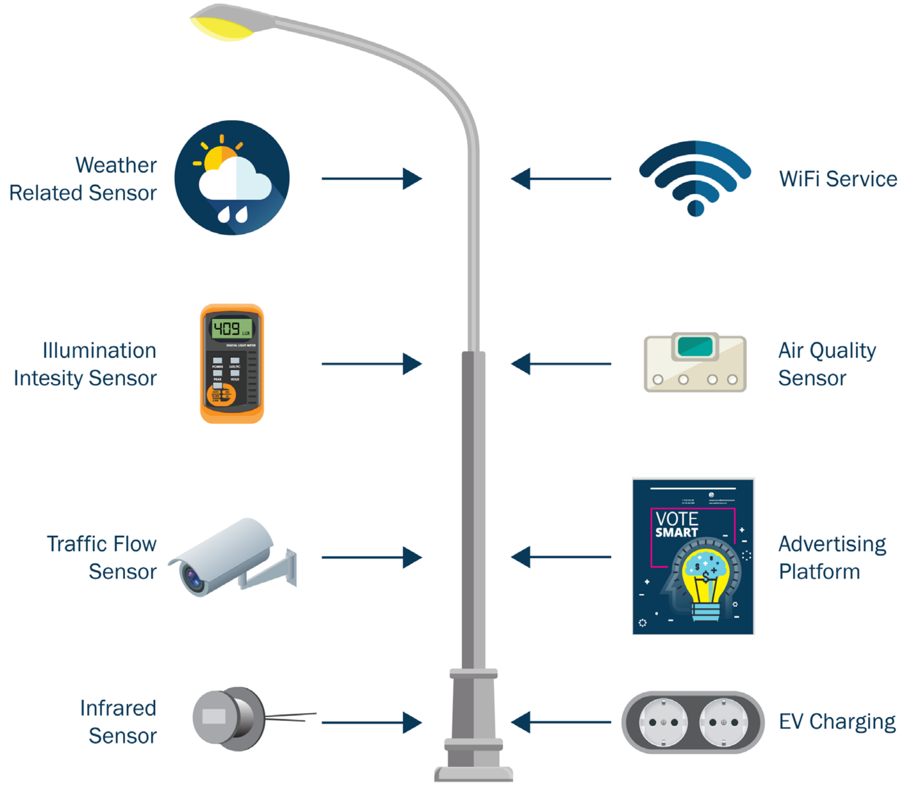
China's coordination and united private sector front in international standards came to a head over Huawei's promotion of "polar coding" (a technical method for encoding data in radio control channels) in the 3GPP 5G standard. Huawei invested significantly in developing polar coding, and it became a symbol of national pride at standards meetings. When Chinese firm Lenovo initially voted for an alternative coding scheme, LDPC, developed by Qualcomm, the decision was met with a public outcry in China for Lenovo taking an "unpatriotic vote." In a subsequent meeting in November 2016, during which companies voted on the use of coding channels in a second part of the standard, Lenovo reversed course and voted for Huawei's polar coding option. When the polar coding standard was partially adopted in 2016, Huawei founder Ren Zhengfei reportedly "threw an opulent ceremony at the company's Shenzhen headquarters to celebrate."[141] Lenovo founder Liu Chuanzhi also published a public statement in 2018 in which he explains the companies' resolution in voting for the Huawei option and reiterates the importance of Chinese companies acting in a united fashion: "We all agree that Chinese companies should be united and cannot be played off one another by outsiders."[142]

Governance Propagation at Standards Bodies

Beyond the nuts and bolts of the 5G technical standard, Chinese firms have already begun to submit standards proposals that shape governance norms around Internet-of-Everything technologies. In June 2019, the ITU adopted a standard for a smart street light architecture proposed by ZTE and China Mobile that includes the ability to "add video monitoring capabilities when deploying smart street lights." In addition to the standard giving ZTE a competitive advantage in smart street light technology because the standard closely mirrors ZTE's own back-end technology, it sets a clear precedent and blueprint for deployment of surveillance technology, absent guardrails for civil liberties.[143] A forthcoming ITU standard on facial recognition technology also codifies database storage of detailed biometric and demographic features on people, including face style, birthmarks, race, and skin color. Use cases such as police surveillance of public spaces and "black list alarms" to spot suspected criminals in schools, temples, hospitals, airports, and malls are also included in the standard.[144] Most recently, at ITU's September 2019 meeting, Huawei submitted a "New IP" proposal to reinvent the Internet protocol (IP) underlying modern Internet architecture in a way that would allow governments more direct control over private citizens' data as well as their ability to access the Internet.[145] Technical standards bodies are not only forums for companies to promote specific technologies, but also for the diffusion of the authoritarian governance norms those technologies impute.[146]

> *"China's use of its leadership role at the ITU to promote technology through the BRI should concern democractic countries that seek to protect both their own competitiveness and civil liberties worldwide.*

Example of a Smart Street Light



Source: ITU Smart Street Light Standard: "Requirements and functional architecture of a smart street light service."[147]

U.S. and EU Approach

In contrast, the U.S. and European approach to international standards bodies has been largely bottom up, driven by open competition from the private sector in a free-market, multi-stakeholder fashion that resists central planning. When U.S. and European companies dominated telecommunications and Internet technologies, this lack of coordination did not hinder U.S. and EU competitiveness in these arenas. The CCP's growing presence in and increased attention to these organizations calls into question the sufficiency of this hands-off approach. Given China's focused efforts to promote not only technology, but governance norms through these bodies, a coordinated allied picture is needed.[148]

While not intended to be comprehensive, the subsequent sections provide an introduction to key standards bodies in 5G and Future Internet technologies. They present a partial picture of the state-of-play at these organizations, and identify areas for allied engagement.

About the Standards Bodies: The Third Generation Partnership Project (3GPP)

3GPP is the overarching technical coordination body by which global telecommunications standards are proposed.[149] The process was designed to be technocratic and is based on consensus—that said, individual companies have strong economic incentives to promote their patents into global standards.

Membership

Membership of 3GPP consists of seven telecommunications standards organizations from around the world: ARIB (Japan), ATIS (USA), CCSA (China), ETSI (Europe), TSDSI (Korea), TTA (Japan), and TTC (India). A member of one of these seven organizational partners is automatically a member of 3GPP. Such members consist of small and large private companies, research entities, academic institutions, government, and public organizations.[150] Most of the major telecommunications players—or their subsidiaries—hold memberships in each of the seven standards bodies. For example, even in ATIS, the U.S. organization, Huawei's U.S. subsidiary Futurewei, Inc. holds membership. As these are international organizations based on international, supposedly technocratic consensus, they are not set up to withstand a coordinated takeover.

Structure

3GPP's work is structured into three technical standards groups (TSG): one focused on radio access networks (TSG RAN), the second on the overall architecture of telecommunications systems and services, including security (TSG SA), and the third focused on the core network and terminals. Each TSG comprises a number of technical working groups, where features are examined and developed.

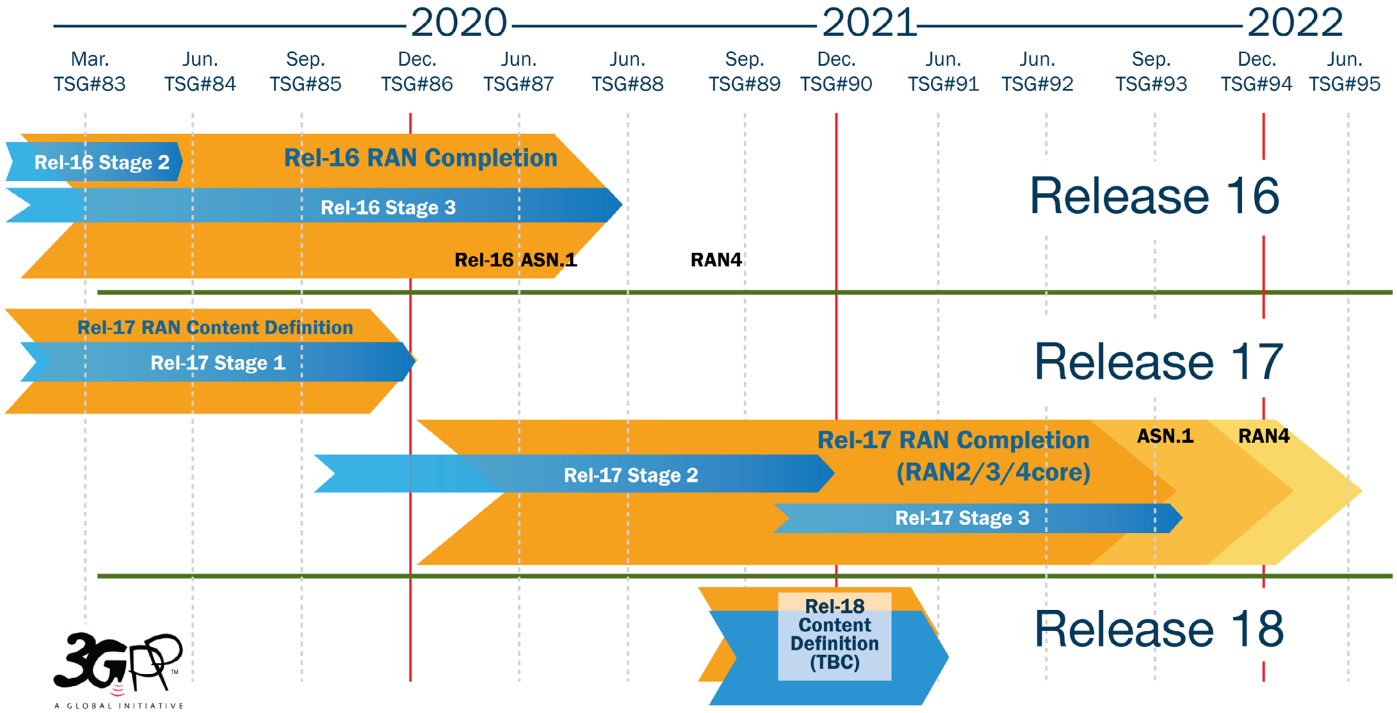
5G Standards Process and Timeline

The technical specifications for the 5G standard are being developed over three 3GPP releases: Release 15 (August 2019), Release 16 (mid-2020), and Release 17 (2021).

- Release 15 (2018–2019): As the first 5G technical standard, Release 15 pioneered technical specifications for the New Radio standard in Non-Standalone (NSA) and Standalone (SA) versions. The former harnesses existing 4G LTE infrastructure, whereas the latter—pursued aggressively by Huawei—does not. In this Phase 1 of the 5G system, standards include specifications for the Internet of Things (IoT), Vehicle-to-Everything Communications (V2x) for the future of self-driving cars, and spectrum slicing, among other technologies. Importantly for China, polar coding was included in this standard for the enhanced mobile broadband (eMBB) application. According to an Institute of Electrical and Electronics Engineers (IEEE) report, it is possible that different coding methodologies can be used in future New Radio applications.[151]
- Release 16 (mid-2020): Planned for completion in mid-2020, Release 16 describes Phase 2 of the 5G system. In addition to continued work on V2x communications for automated and remote driving, Release 16 is set to introduce specifications for Industrial IoT, Ultra-Reliable and Low Latency Communication (URLLC) enhancements, 5G efficiency, and New Radio access to unlicensed spectrum.[152]
- Release 17 (2021): Planned for completion in 2021, Release 17 is still under discussion, primarily within TSG SA and TSG RAN. TSG SA is considering, among other topics, specifications on critical medical technology, factories of the future, unmanned aerial systems, and asset tracking. TSG RAN's scope is even less defined, but topics under consideration include New Radio evolution above 56.2 GHz, New Radio for Non-Terrestrial Networks (i.e. satellite communications), and further IoT enhancements. [153]

For the introduction of new features into the 5G standard and beyond, U.S. and allied companies would need to act now.

5G Technical Standards Development Timeline



Source: 3GPP.[154]

About the Standards Bodies: The UN International Telecommunications Union (ITU)

In recent years, China's increasing influence at UN organizations from the Food and Agriculture Organization and UNESCAP to the World Health Organization has drawn scrutiny for its advancement of a more authoritarian-friendly model of global governance and universal human rights.[155] In particular, a sustainable development agenda that puts economic opportunity—not individual liberty—at the center of human rights is a goes hand-and-hand with a strategy for Future Internet dominance based on mass data collection and surveillance. The ITU is no exception. China's use of its leadership role at the ITU to promote technology through the BRI should concern democratic countries that seek to protect both their own competitiveness and civil liberties worldwide.

The ITU's membership comprises 193 Member States and over 900 companies, universities, and international and regional organizations. Its work is organized into three sectors for radiocommunications (ITU-R), standardization (ITU-T), and development (ITU-D). Much of the substantive work in the standardization process happens through study or focus groups.

Whereas 3GPP coordinates national and regional standards development organizations to produce technical specifications, the ITU is where many 5G standards are formally adopted. The ITU also sets the goal metrics in latency, data rates, and other specifications by which 3GPP and its Organizational Partners set timelines and for which they develop technical specifications.

> *“ Opportunities exist now to set requirements for the next generation of mobile standards.*

Because of nation state influence in the ITU, the United States has not historically been an active participant, preferring standards to be developed in a bottom-up, private-sector driven manner. Some U.S. firms, including Microsoft and Google, only joined the ITU for the purpose of engaging on specific matters of particular relevance.[156] But China's increased activity and leadership in the ITU has forced a greater governmental role in ICT decisions. The ITU's mission has also evolved to include Internet governance standards, in line with China's vision of increased state power on these matters as opposed to the decentralized, free Internet model. Nevertheless, in order to contest this presence, the United States has begun to recognize the body's importance.[157]

With much of the “IMT-2020” standard on 5G already set, the United States and its allies missed opportunities to require stronger cybersecurity protections in 5G and develop a coordinated spectrum allocation strategy. Additionally, the Defense Innovation Board in April 2019 recommended that the United States add the allocation of C-band spectrum to the agenda of the World Radiocommunication Conference 2019 (WRC-19), hosted by ITU-R in October and November 2019. As of September 27, however, that item remained off the agenda, and the conference made no allocations of C-band spectrum.[158]

Network 2030 Focus Group Led by Futurewei Technologies and New IP

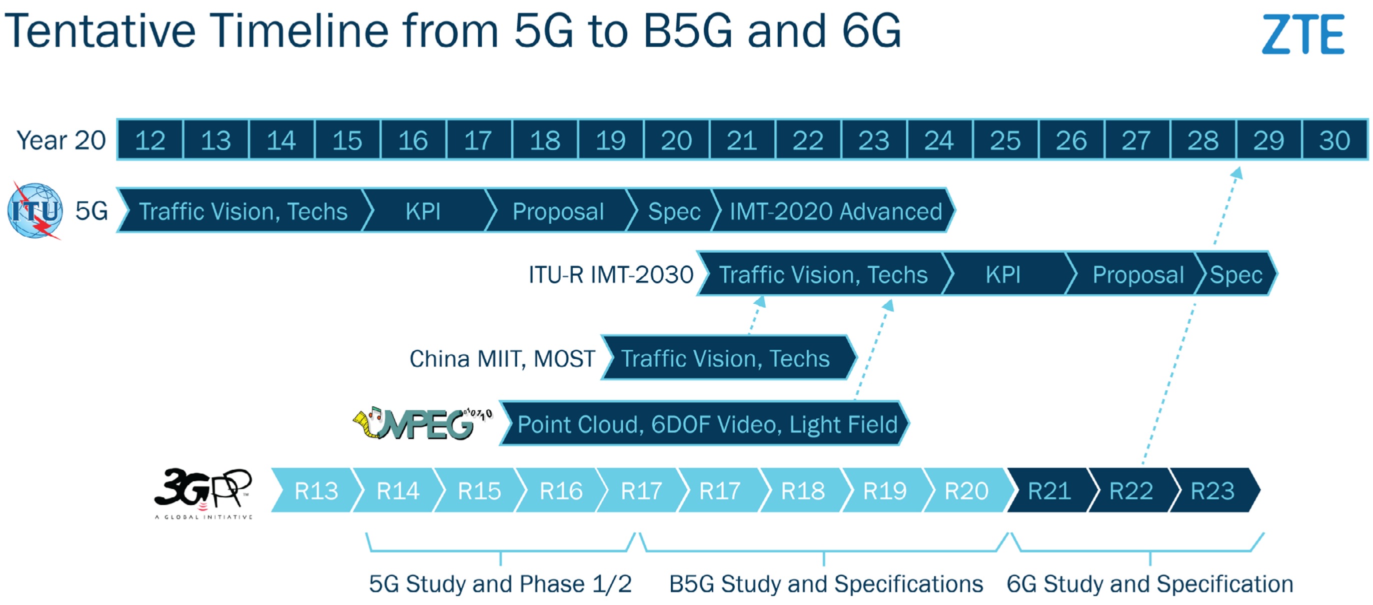
Looking beyond 5G, opportunities exist now to set requirements, such as on cybersecurity, for the next generation of mobile standards, IMT-2030, which is likely to form the basis of the 6G standard. Already, a focus group under ITU-T Study Group 13 is underway: The ITU-T focus group Technologies for Network 2030 is charged with the mission of formulating all aspects of “Network 2030” and providing guidelines for the standardization roadmap. Its chairman Richard Li from Futurewei Technologies (the U.S. subsidiary of Huawei) described his group as “Network 2030: A pointer to the new horizon for the future digital society and networks in the year 2030 and thereafter.”[159] Its mandate is:

- To study, review and survey existing technologies, platforms, and standards for identifying the gaps and challenges towards Network 2030, which are not supported by the existing and near future networks.
- To formulate all aspects of Network 2030, including vision, requirements, architecture, novel use cases, evaluation methodology, and so forth.

- To provide guidelines for standardization roadmap.
- To establish liaisons and relationships with other Standards Development Organizations (SDOs).[160]

Part of Dr. Li's agenda for this group involves introducing the New IP proposal to rework the technical foundations of the existing Internet, which have grown to support a multi-stakeholder, inclusive and open model. Of concern is New IP's ability to facilitate top-down Internet control, authoritarian shut-downs through its creation of Internet "islands," and so-called "shut-up commands" that could silence activists, journalists, or anyone who runs afoul of the government. Put simply, the proposal puts Internet control in the hands of the state. According to Réseaux IP Européens (RIPE), an EU-based Internet development group, the proponents of the New IP proposal "depart from the core philosophy behind TCP/IP and the later Internet: an open and flexible system that is much more the result of decades of evolution rather than a single master plan…The most problematic and dangerous part of the proposal is not the technology," they argue, "but the fundamental beliefs behind it, which represent a departure from the Internet's fundamental values of openness, transparency and putting the end user in control."[161]

The New IP proposal advances the authoritarian vision of cyber sovereignty, in which individual countries have sovereign authority to exercise control over the Internet within their borders and therefore over the digital rights therein—a direct rejection of open information and universal human rights in the digital age. Huawei has championed the New IP proposal and is already beginning its lobbying and communications effort to paint the proposal as a benign and necessary technical advancement without governance or political implications, mirroring its lobbying campaign around 5G.[162] Huawei is also rumored to be building New IP Internet infrastructure overseas.[163] Details are scarce, but building the technology before the international community has agreed to the norms would be consistent with the facts-on-the-ground strategy the company has taken to the deployment of 5G, "safe cities," and surveillance technology beforehand. Saudi Arabia, Russia, and Iran are reportedly indicating support for the proposal.[164] Through Dr. Li's ITU-T Network 2030 leadership, Huawei is working to incorporate the New IP into the ITU's next generation standardization process, arguing that "there is an obvious limitation in the current Internet."[165]

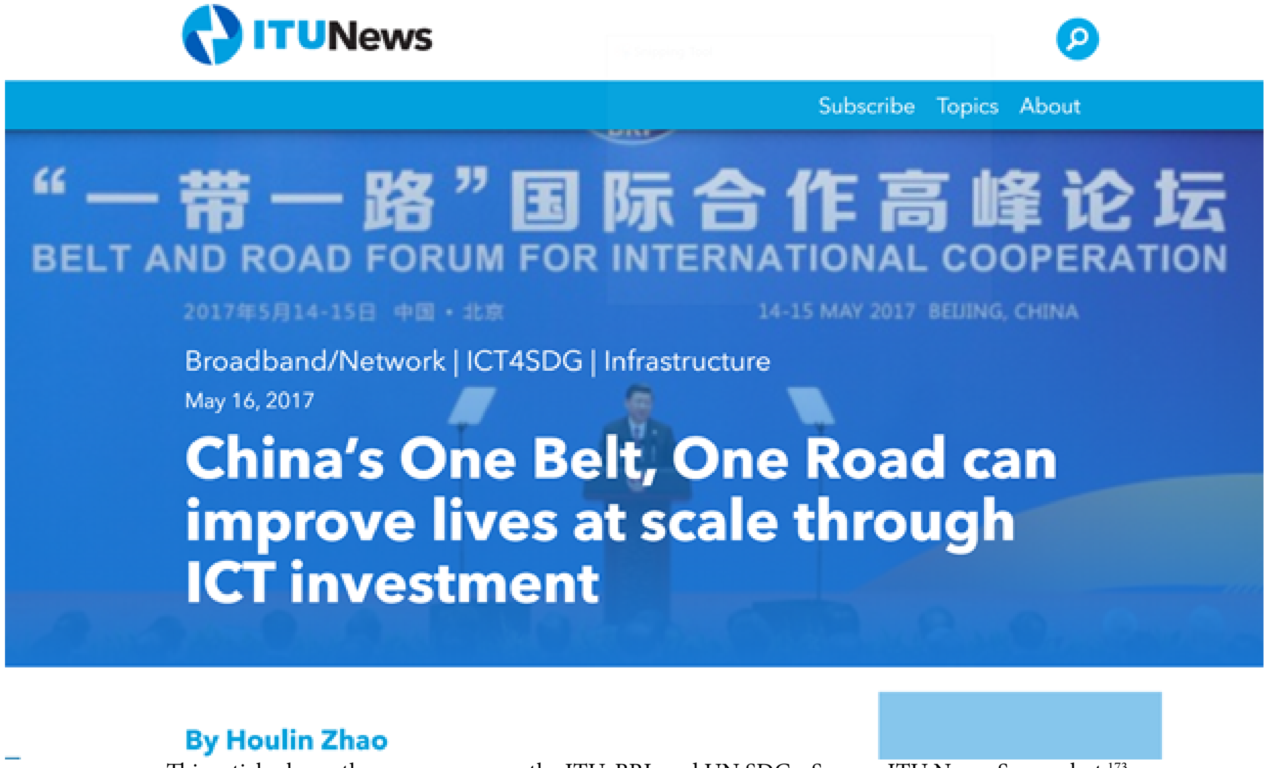


Source: ZTE Keynote at the 6G Wireless Summit 2020 via telecoms.com.[166]

The ITU and the BRI: A Synergistic Tango

Finally, under the leadership of Chinese national Houlin Zhao (formerly an engineer for China's Ministry of Posts and Telecommunications), the ITU has wholeheartedly embraced China's Belt and Road Initiative and become an explicit venue for the promotion of Beijing's interests, message, and technology. The synergistic pairing of the ITU and the BRI helps create facts on the ground and norms of use for Chinese-made Future Internet technology, especially in the developing world. In particular, the ITU is a forum in which China is able to align the UN SDG that are at the heart of the UN's economic mission with China's own digital connectivity agenda, the "Digital Silk Road."[167] Specific SDG targets include 9.1, focused on developing quality reliable, sustainable, and resilient infrastructure for economic development and 9.c, which aims to significantly increase access to ICT and the Internet.[168] According to a People's Daily article, at the May 2017 Belt and Road Forum, the ITU signed an agreement with China to "collaborate on projects under the Belt and Road Initiative." In the words of ITU Secretary-General Houlin Zhao, "The Belt and Road Initiative recognizes the critical role played by information and communication technology (ICT) as a foundation for development.[169] Of course, Zhao has also put his thumb on the scale when it comes to Huawei, saying U.S. security concerns appeared to be driven by politics and trade, not by any evidence.[170] At the same time as standardization advances foreign policy, China uses its signature foreign policy tool to export domestic standards—by including standardization clauses in BRI Memorandum of Understanding (MOU) agreements.[171]

The ITU-BRI collaboration agenda also receives assistance from the broader UN. In September 2017 the UN Economic and Social Commission for Asia and the Pacific (UNESCAP) released a report entitled "A Study of ICT Connectivity for the Belt and Road Initiative in China-Central Asia Corridor." The Study found that "ESCAP-China cooperation could increase inclusiveness among 62 ESCAP member economies to achieve a higher level of ownership and therefore support to the BRI initiative. In addition, the ESCAP-China cooperation strengthens synergies between The Asia-Pacific Information Superhighway (AP-IS) and BRI initiatives respectively to attain mutual benefits, sustainable development, and strengthen economic relations among the ESCAP member countries."[172]


ITUNews
Subscribe
Topics
About
"一带一路"国际合作高峰论坛
BELT AND ROAD FORUM FOR INTERNATIONAL COOPERATION
2017年5月14-15日 中国・北京
14-15 MAY 2017 BEIJING, CHINA

Broadband/Network | ICT4SDG | Infrastructure

May 16, 2017

China's One Belt, One Road can improve lives at scale through ICT investment

By Houlin Zhao

This article shows the synergy among the ITU, BRI, and UN SDGs. Source: ITU News, Screenshot.[173]

This synergy between the UN SDGs and Future Internet infrastructure, incubated at the ITU, is now appearing in 6G technical documents beyond the UN. The Finnish 6Genesis Flagship project, for example, brings together international researchers and corporations towards the development of 6G technologies for input into the standardization process. In June 2020, the 6Genesis project released a series of 6G white papers authored by an international expert group run through the University of Oulu. Its "White Paper on 6G Drivers and the UN SDGs" asserts that "the relationship between these potentially mutually reinforcing forces [of the promise of 6G and the framing of the UN SDGs] is currently under-defined." It proposes "a novel linkage between 6G and the UN SDGs." The White Paper does not advocate for a particular company's or country's digital infrastructure, but references the ITU and Huawei to draw the connection between 6G advances and the UN SDGs, including using digital health records and remote patient monitoring to support the goal of "good health and well-being" and smart grid solutions, distributed energy systems, and smart metering to support the goal of "affordable and clean energy." The two chapters detailing this connection and outlining the 6G-SDG vision were edited by a Huawei engineer.[174] It is important to note that there is nothing inherently undemocratic or problematic about the synergy between 6G and the UN SDGs (SDG 16 is in fact "peace, justice, and strong institutions"). The linkage is an attractive and powerful framing that democracies would do well to embrace and imbue with values based also on universal rights. At present, however, PRC diplomats and companies are out front shaping the technical and governance dimensions of the synergy between 6G and the UN SDGs.

The Beijing AI Principles and the ITU's "AI for Good"

The ITU's advancement of Chinese Future Internet technology extends beyond the infrastructure layer to championing the Future Internet application technologies that pose concerns for democratic governance. An October 2019 statement by ITU Deputy Secretary General Malcolm Johnson entitled "How ITU is ramping up its efforts on AI for Good" sheds particular light on how Beijing whitewashes its AI-enabled human rights abuses through a sycophantic ITU.[175] The document touts China; Chinese companies Baidu, Alibaba, and Tencent; Beijing's AI Principles; and Chinese universities Peking University, Tsinghua University, the Institute of Automation, and Institute of Computing Technology of the Chinese Academy of Sciences no less than 15 times. No other country, no company from another country, no university from any other country, and no other efforts to set principles on AI are mentioned even once in the statement—despite significant international activity on all of these dimensions. A Harvard University study from January, for example, on "Principled Artificial Intelligence" mapped out 36 prominent "AI Principles" documents—including the Beijing AI Principles—from government, private sector, and civil society organizations around the world, and more have been added since.[176] In the aforementioned article on "AI for Good," the ITU showcases only one of them.

The ITU's singular focus on China's AI efforts in its "AI for Good" initiative functions as something of a propaganda arm for Chinese technology giants who have embraced the slogan while still engaging in censorship and surveillance. Here are four particularly illustrative quotations:

> "As the UN specialized agency for information and communication technologies, ITU plays an important role in shaping the future of AI and other emerging technologies ranging from the Internet of Things to 5G … It is in this context that we should consider the national AI strategies launched by a number of countries around the world, including China's 'Next Generation Artificial Intelligence Development Plan.'"[177]
>
> "Last May, for example, the Beijing Academy of Artificial Intelligence released the 'Beijing AI Principles'. These principles were developed in collaboration with prominent technical organizations and tech companies, including Peking University, Tsinghua University, the Institute of Automation and Institute of Computing Technology in Chinese Academy of Sciences, as well as Baidu, Alibaba and Tencent. These 15 principles call for 'the construction of a human community with a shared future, and the realization of beneficial AI for humankind and nature.' The very first principle is to 'Do Good.'"
>
> "We hope more Chinese companies will join us in this effort by coming to our next 'AI for Good Global Summit,' which will take place in Geneva from 4 to 8 May 2020. As a leading global player on AI, it is important for China to have a voice on this platform."
>
> "Just as important is China's engagement in ITU activities on AI. And I am pleased to say that just last week, ITU launched a new Focus Group on 'AI for autonomous and assisted driving' that received strong backing from China." [178]

That Tencent's all-encompassing chat platform WeChat regularly censors political content and even discussion of the coronavirus in China or that it has helped the CCP jail journalists receives no mention. Neither does any reference to the myriad ways in which Chinese AI technology has done the opposite of good (from the perspective of individual liberty) in Xinjiang and around the world. The world's oldest UN agency's public efforts on AI focus on extolling China's achievements and minimizing its threats to universal rights.

This promotion extends to Future Internet technologies including the intersection of 5G and COVID-19. On June 18, 2020, Deputy Secretary Johnson opened a virtual session of the ITU's World Summit on the Information Society on the topic of 5G Technology for COVID-19 Prevention and Control, organized by the China Academy of Information and Communications Technology. His remarks began: "Good morning, good afternoon and good evening - especially to my friends in China!"[179] In the absence of democratic leadership, China is shaping the international landscape of Future Internet technologies, combining infrastructure advancements with data-driven applications.

CCP Surveillance at the UN

Of course, the ITU is not the only UN organization carrying water for the CCP's efforts to rebrand its surveillance regime. In April 2020, the UN announced a partnership with Tencent to stream coverage of its 75th anniversary over Tencent's videoconferencing platform Voov, a competitor to Zoom.[180] Tencent is one of the most aggressive accomplices in the CCP's censorship and surveillance regime, and has actively helped China achieve Freedom House status as the world's worst abuser of Internet freedom. Recent research now indicates it surveills users outside of China as well in order to train and improve its censorship algorithms.[181] The Tencent-UN partnership received significant backlash from lawmakers and human rights groups alike and is now under review.[182] The press release has been removed from the UN75 website as of the time of publication of this report. Yet the circumstances by which Tencent came to partner with the UN tell an even more shocking tale of UN complicity in China's technology-enabled censorship regime. Internal UN documents indicate that the Tencent-UN75 partnership arose because a major global UN75 survey was "not readily accessible in China"—that is, CCP censors blocked it. Tencent was then retained so that UN75's activities could be accessible around the world—that is, accessible in China and in compliance with its censorship regime.[183] The incident raises significant questions about the role of Future Internet technologies in international communications, when only censored versions of speech are allowed in parts of the world. The Tencent-UN agreement would have provided the UN with Tencent's videoconferencing and text services, VooV Meeting platform, WeChat Work, and an AI-based language translation service, Tencent Artificial Intelligence Simultaneous Interpretation. Natural language processing and machine-enabled translation are core technical objectives of the CCP's Central Propaganda Department.[184] Coming full circle, this department, through GTCOM, discussed in Section III, is also a strategic partner of China's Central Construction Bank—one of China's four largest state-owned banks financing the BRI.[185]

A Plethora of Standards Organizations—Some with Chinese Leadership

Beyond 3GPP and the ITU, numerous additional international bodies develop telecommunication and Internet standards: The O-RAN Alliance develops technical specifications for virtualized networks, an infrastructure replacement for hardware that shows promise in creating trusted vendor diversity in 5G networks. The GSM Association represents multinational organizations on subscription management and embedded Subscriber Identity Module (eSIM). The IEEE develops aspects of IoT connectivity. OneM2M works on eHealth and telemedicine, industrial applications, and home automation.[186] The ISO develops ICT standards for computer and IT security, among other areas. One ISO subgroup, SC-42 has responsibility for the governance of AI, and has drawn an interest from Beijing.[187] Elsewhere at the ISO, China recently obtained clearance for a proposal to establish a research group on integrating IoT and the blockchain.[188] By contrast, ONIF, the video surveillance industry's standards body, recently gave Huawei the boot for its position on the U.S. Commerce Department's Entity List.

“ An international security approach that puts allied cooperation on the Future Internet front and center is the United States’ best defense against China’s approach to global leadership in 5G.

In addition to the ITU, of which Houlin Zhao has been Secretary-General since 2014, starting his second four-year term in January 2019, China has pursued technical leadership positions across related international standards organizations that shape the Future Internet, including the ISO and the International Electrotechnical Commission (IEC). Zhang Xiaogang has been president of the ISO’s Technical Management Board (the committee charged with setting the ISO’s agenda) since 2015. And Shu Yinbiao, who runs China’s State Grid Corporation assumed the presidency of the International Electrotechnical Commission (IEC) in January 2020, after serving as vice president since 2013.[189] The IEC publishes standards and conducts conformity assessments on all electrical and electronic technologies. Its recent work has focused on smart cities, the smart grid, AI, IoT platforms and wireless sensor networks—much of it in the context of the UN SDGs.[190]

Conclusions

Conclusions

- China's coordinated strategy presents an asymmetric advantage in both international standards-setting bodies and more broadly the Future Internet deployment landscape.
- Huawei's vertical integration of the 5G technology stack presents deployment advantages. Open and interoperable standards are crucial to allow new entrants to compete.
- In the telecommunications industry, deployments finance R&D, so regaining overall competitiveness by the United States requires both incentivizing (and protecting) future R&D and creating the conditions for telecom deployments.

There is an inherent tension between upholding the technocratic nature of the technical standards-setting bodies and promoting specific features in 5G (and future) standards. The United States should adopt an approach which minimizes the politicization of technical standards-making processes, while advancing policies conducive to open Internet ideals and pushing back on China's co-option of standards bodies like the ITU to promote cyber sovereignty and the digital silk road. In many cases, advocacy for specific technical features of the 5G standard and the inclusion of specific patents should be done by the private sector. But countering coordinated efforts from authoritarian regimes to manipulate the system should also be on the U.S. government's agenda. Allied cooperation on a private sector level can produce market-based coordination on telecommunication standards setting. Ultimately, the United States and its allies will need a strategic approach to standards-setting that distinguishes the areas where the private sector can continue to lead successfully from those where deeper national and international coordination is needed.

An international security approach that puts allied cooperation on the Future Internet front and center is the United States' best defense against China's top-down, industrial policy-driven approach to global leadership in 5G. Cooperative funding models for R&D and infrastructure development will organically align interests in the standards for the Future Internet without unduly corrupting the technocratic standards-setting process. In doing so, these efforts can fuse international alliances and guard against the authoritarian divide-and-conquer strategy that seeks to upend the liberal alliance structure.

Policy Recommendations

Counter China's Structural Advantages in Future Internet Development and Deployment

The White House Should

- **Adopt a national and international security approach to 5G, 6G, and the future of the Internet.** Fighting for a democratic Internet means cooperating creatively with likeminded partners and leveraging complementary advantages at all stages of the 5G technology stack. While the NTIA and FCC have a vital role to play, they are not resourced in mission or in structure for this purpose. Such a shift has been called for by Pentagon officials including Undersecretary for Acquisition and Sustainment, Ellen Lord.[191]

The President Should

- **Create a Technology Directorate at the National Security Council and appoint a Future Internet Director with a joint appointment at the White House Office of Science and Technology Policy.** The director should coordinate an interagency task force on U.S. and democratic global competitiveness on the Future Internet, consisting of representation from DOD, State, CISA/DHS, NTIA/FCC, OSTP, and DNI/CIA to build out and implement a cross-cutting Future Internet strategy.

The Future Internet Director Should

- **Develop a democratic Future Internet strategy.** The Director should lead the task force's development of a Future Internet strategy along infrastructure, application layer, and governance dimensions to increase the competitiveness of the United States and likeminded democracies.

- **Establish a private sector coordination mechanism.** The Director should include in the task force's outreach a working group of industry representatives from the telecom sector to explore joint public-private efforts on standards and business development.

- **Facilitate 5G deployment.** The Director should coordinate the rapid deployment of nationwide 5G and serve as a focal point for interagency coordination. Disputes between DOD and the FCC over 5G spectrum sharing illustrate the need for leadership from the White House on this deployment.[192]

- **Plan for 6G now.** The Director should lead a public-private coalition on 6G experimentation and guide long-term planning on spectrum allocation for 6G and beyond in coordinating with FCC. The NTIA's forthcoming National Spectrum Strategy should provide an entry into these efforts.

- **Develop a digital development agenda.** The Director should draft in coordination with the State Department Technology arm, USAID, and the Development Finance Cooperation, a Digital Development Agenda that (a) identifies priority countries for engagement on different aspects of the Future Internet (infrastructure, application, and governance) and (b) tailors Future Internet engagement to local conditions, recognizing that a Huawei ban is unlikely in much of the developing world and providing safeguards and standards to mitigate potential governance implications of Chinese Internet and surveillance technology.

- **Provide economic policy input to the President and senior officials.** The Director should provide national security input to ongoing economic policy discussions with China, especially those involving communications technologies, to ensure that the geopolitical implications for the Future Internet are evaluated and account for in real time.

Congress Should

- **Require the DNI to include an annual update on the health of the Future Internet industry as an**

annex to its worldwide threat assessment. While on the one hand, the United States should continue to harness private sector innovation, on the other, China's state-driven, anti-competitive approach has exploited this model. As a national and international security matter, the DNI should proactively assess and monitor the health of the global communications infrastructure market with a future outlook to ensure that the United States can forecast and avoid a situation where authoritarian firms dominate the global landscape—at the infrastructure (e.g. telecommunications networks, undersea cables) and base application (e.g. smart cities, smart grid) layers.

- **Appropriate funding for the creation of academic and/or federally funded research and development centers or 6G innovation hubs modelled after Finland's 6Genesis Flagship project.** The purpose of these hubs is to spur and lead international technical research and development on the next generation of Future Internet technology and increase United States' and democratic competitiveness in the Internet-of-Everything ecosystem.
- **Pass legislation similar to the USA Telecommunications Act. Such legislation should establish a Commerce Department fund to support pilot projects for the development of infrastructure supplier diversity using the OpenRAN framework, as well as a Multilateral Telecommunications Security Fund to aid in allied coordination.**
- **Create a State Department Technology Ambassador to establish and represent the United States in a trans-national alliance of democracies, such as the D10, to share threat intelligence and coordinate action in the Future Internet arena.** Ideally, this position should be part of a larger effort to beef up technology expertise in the State Department, such as through the creation of an Assistant Secretary of State leading a new Bureau of Cyberspace Security and Emerging Technologies, as recommended by the Cyberspace Solarium Commission.[193] Denmark, as an example, presently has a Technology Ambassador.[194]

The Defense Department Should

- **Elevate 5G planning within DOD to the CIO's office.** Current DOD plans call for 5G efforts to sit within the charge of the USD (R&E).[195] While R&E should provide input to 5G, especially in so far as technology selection and funding of new R&D (such as on virtualized networks) goes, it is not equipped to handle policy on trade, acquisition, or allied coordination. A higher-level effort driven by the Chief Information Officer, whose mission set includes network policy, spectrum management, and securing DOD IT infrastructure would encompass a fuller spectrum of national security concerns.

European Capitals Should

- **Adopt similar or analogous structural changes and tailor them to national environments to bolster the development of a collective democratic vision for the Future Internet.** In particular, bureaucratic structures that bridge communication and decision-making and build common understanding across economic, technology, and national security agencies (such as ministries of foreign affairs or ministries of defense) can mute the effects of Beijing's weaponization of its economy to advance technology and geopolitical goals.

A Trans-National Alliance of Democracies Such as the D10 Should

- **Support U.S. innovation on the Open RAN models through national and international technology summits and joint R&D investment.** Virtualized networks create options for open infrastructure and new market entrants, with the potential to reduce U.S. and allied dependence on foreign or untrusted infrastructure vendors. A common argument against excluding Huawei from allied 5G networks is that it would reduce competition in the infrastructure market. New entrants developing virtualized networks could restore this competition while reducing the expense associated with building out telecommunications infrastructure via a shift to software. Such R&D initiatives should be both national and developed in partnership with allies, especially those who have chosen to exclude untrusted Chinese firms from their networks.

Construct Allied Solutions for the Developed and Developing Worlds

The White House Should

- **Refocus its strategy, allied engagement, and public messaging on China away from wrangling allies to get on side with bilateral US-China competition and tit-for-tat action and towards ensuring a trusted future for free and open communications in democracies.**

The Defense Department Should

- **Create an allied 5G and 6G infrastructure pilot program fielding proof-of-concept experiments with Future Internet technologies at U.S. and allied military installations in Europe and Asia.** At present, the DOD is piloting 5G in CONUS installations.[196] Congress should appropriate funds to extend this program to a few select installations in allied countries, such as Australia, with trusted 5G infrastructure

The State Department, USAID, Development Finance Coorporation, and Future Internet Directorate Should

- **Craft and execute a Digital Development Strategy, a key piece of which should be financing coordination with D10 nations.** In particular, a $500 million Multilateral Telecommunications Security Fund would help accelerate trusted Internet infrastructure roll-out globally.[197] D10 nations should also supplement this fund for digital development to include Future Internet application development and deployment and advance an open Internet governance model.

A Trans-National Alliance of Democracies Such as the D10 Should

- **Create a "Trusted Internet" or "Trusted Cyber" standard based on the Prague Proposals for 5G and 6G infrastructure systems, and extend those principles to the application and governance layers of the Future Internet.** Crafted in May 2019, the Prague Proposals outline a 5G cybersecurity framework based on four categories: policy; technology; economy; and security, privacy, and resilience.[198]

- **Operationalize these principles by implementing secure 5G architecture explicitly in accordance with these proposals—going beyond simple bans to fostering robust R&D investment and risk management frameworks to ensure privacy—and developing and sharing detailed adoption plans among allies.**

- **Create a "Trusted Internet/Cyber" standard certifying the implementation of the Prague Proposals and develop a pathway to certification for countries both inside and outside the D10.**

- **Consider this "Trusted Internet/Cyber" certification as a factor in new membership of the Organization of Economic Co-operation and Development (OECD).** According to the OECD's Paris 2018 OECD Membership and Values of the Organization document, countries wishing to become OECD members must demonstrate a readiness and commitment to being: "(i) democratic societies committed to rule of law and protection of human rights; and (ii) open, transparent and free-market economies." Because Future Internet technology implicates so much of the future of human rights, democratic societies, and open market economies, progress towards the "Trusted Internet/Cyber" standard should be weighed by D10 nations when considering backing countries' bids for OECD membership. Indeed the Prague Proposals, on which the standard should be based, place a premium on transparency and open market competitive principles.

- **Extend these principles to the application and governance layers of Future Internet technologies to develop a framework for democratic countries' development of Internet-of-Everything applications and governance norms around data protection, privacy, and lawful access beyond the infrastructure layer.**

- **Develop sustainable off-ramp plans for nations using high-risk vendors.** While a number of nations have chosen to exclude high-risk vendors from 5G networks, the D10 should help its own members as well as others to craft and, if need be, incentivize sustainable off-ramp plans that mitigate economic harm while increasing security.

- **Explore joint business models for critical Internet infrastructure, including supporting infrastructure sharing agreements, especially in developing countries, joint infrastructure funding, and digital development assistance.**

- **Establish joint R&D Centers of Excellence and pilot projects on Future Internet infrastructure, applications, and governance.** The D10 should establish three Future Internet R&D Centers of Excellence—one in North America, one in Europe, and one in Asia/Oceania—to conduct academic and industry research on 5G and 6G infrastructure and applications including smart cities, smart grids, digital health, wireless and networking devices, and advanced IoT.

NATO Should

- **Update its telecommunications security requirements to align with the Prague Proposals and conduct a forward-looking security assessment of future NATO communications infrastructure into 5G and 6G. Secretary General Stoltenberg has already announced that NATO defense ministers will agree to update their "baseline requirement for civilian telecommunications."**[199] The United States and likeminded allies should back an update that accords with the Prague Proposals. NATO should coordinate and share civilian baseline requirements with EU states implementing the 5G Toolkit.

- **Count a portion of excess nation spending on secure 5G infrastructure towards its 2 percent defense spending goals.** To the extent that secure 5G infrastructure or rip-and-replace programs cause cost overflows, NATO should allow members to count a portion of those outlays on secure 5G systems towards national 2 percent defense spending goals. There are a number of ways 5G-inclusive targets could be defined, including one-time commitments or line-item funds, but if investing in technology built by trustworthy vendors is a priority—and it should be—the alliance's cost-sharing structure should reflect it.[200]

Increase Activity in International Standards Bodies

The State Department Should

- **In coordination with the National Institute of Standards and Technology (NIST) and the private sector, perform a landscape analysis of relevant international standards organizations to advance a democratic Internet and develop a standards strategy for the Future Internet.** In particular, they should identify key areas where competitiveness in or governance of the Future Internet is being shaped and assess where the private sector can continue to lead successfully, and where deeper national and international coordination is needed.[201] Part of this effort should involve putting forth standards that shore up cybersecurity in IoT devices, include additional cybersecurity requirements (versus optionality) into future 5G and 6G standards, limit immediate state access to private citizen data, and contemplate what smart cities should look like in democracies.

- **In coordination with allied democratic governments and the private sector, conduct ongoing monitoring of the proceedings of the 3GPP, ITU, and ISO to assess PRC bloc action to advance specific features that advantage Chinese companies or promote authoritarian Internet governance norms in infrastructure or application standards.** It should also develop an allied information sharing and coordination mechanism in advance of key meetings to defend democratic governance values.

- **In coordination with democratic partners such as the D10 nations and the private sector, contest the ITU as a forum for promotion of the digital silk road.** As 5G and 6G become increasingly wrapped up in China's digital development agenda, the United States and its allies can raise the alarm on individual rights issues and 5G and 6G enabled societal surveillance instantiated in ITU standards.

- **In coordination with the private sector, advance a multilateral human rights framework to AI governance in ISO/IEC JTC 1/SC-42. SC-42 serves as the focal point for the Joint Technical Committee's**

standardization program on Artificial Intelligence, providing guidance to the IEC and ISO on AI application development. The organization's working groups include, among others, big data, trustworthiness, and the governance implications of AI.[202]

The National Institute of Standards and Technology (NIST) Should

- **Review the ITU-T Network 2030 agenda and "New IP" proposal to assess its promotion of a cyber-sovereignty model.** If the assessment concurs with that of industry analysts that remaking the Internet will make it easier for nation states to control access to the Internet, a coalition of democracies should put forward an alternative Network 2030 architecture for the 6G standard that preserves the existing Internet Protocol architecture.

- **In coordination with the private sector, assess the feasibility of an alternative to polar coding in 3GPP Releases 16 and 17.** 3GPP's Release 15 codified Huawei's Polar Codes for the enhanced mobile broadband (eMBB) application due to coordinated action and pressure from the CCP. While there is no appeals process in 3GPP, other 5G applications with standards currently under discussion could employ different coding methodologies, such as LDPC.

A Trans-National Alliance of Democracies Should

- **Aggressively challenge the UN on cyber sovereignty, Internet censorship, and artificial-intelligence-enabled human rights abuses.** PRC strategy has been to normalize abuses of freedom of expression and human rights by casting them as a difference of opinion or of culture. In fact, they are direct violations of the UN Declaration of Human Rights. The United States should lead and marshal likeminded allies and partners in calling out the dark sides of PRC techno-authoritarianism—for strategic, not only humanitarian reasons. It should point out that these abuses are enabled by the very technology the CCP promotes worldwide.

- **Increase representation in key Future Internet leadership positions such as in ITU-T.** A fine balance should be struck between government-led and industry-driven approaches, but the United States and its allies should be willing to compete with China to set global agendas on 5G and 6G enabled technology that protects human rights and civil liberties.

Democratic Legislatures Should

- **Consider tax credits on funds spent by smaller technology companies for participation at key international standards-setting bodies.** In the United States, an expansion of the Research and Experimentation Tax Credit to include standards participation and leadership could incentivize increased U.S. industry presence.

Secure the Future Internet

Congress Should

- **Require the Director of National Intelligence (DNI) to produce an end-to-end cybersecurity risk assessment of 5G and Future Internet applications.** The decision to exclude high-risk vendors Huawei and ZTE from U.S. networks has meant risk management frameworks were not needed in the United States to determine vendor selection. As such, a more comprehensive cyber risk assessment that recognizes that vulnerabilities can derive as much from endpoint failures as from infrastructure is needed to secure the Future Internet.

- **Require the DNI to produce a cybersecurity risk assessment for 6G architecture so that it can inform the development of the 6G standardization process by 2023.** This assessment should also include an assessment of whether a transition to post-quantum cryptography should be started with cybersecurity infrastructure for 6G.

- **Pass comprehensive federal data protection legislation to include a breach notification requirement and cybersecurity standards for IoT devices.** In addition to bolstering cyber resiliency, such legislation will help protect sensitive personal and corporate data at the application layer. A data protection and privacy framework would create further meaningful distance between the profit-driven surveillance capitalism model pursued by private firms and the control-drive surveillance model advanced by CCP techno-authoritarianism. It is also an important step in creating and aligning principles of a democratic model for data in the Future Internet. How and by whom data is stored, handled, accessed, and shared are central to the distinction between democracy and autocracy. Democracies should emphasize that distinction and promote a human rights-based vision in partly free states.

The Defense Department Should

- **Develop a Zero Trust Architecture (ZTA) model for cybersecurity; the commercial sector should examine a similar shift in data security in building out data-driven AI applications.** As the Defense Innovation Board has written, "From a security perspective, ZTA can better track and block external attackers, while limiting security breaches resulting from internal human error. From a data sharing perspective, ZTA can better manage rules of access for users and devices across DoD to facilitate secure sharing, from the enterprise center to the tactical edge."[203] A shift to a cybersecurity model that layers user access by privileges can help prevent intrusions from becoming massive breaches. A similar model could be employed in the commercial, so that access to a home network, for example, need not imply access to the data from every device on that network.

The FBI and DHS Should

- **Increase collaboration with allied counterpart organizations on cyber espionage threats.** This includes establishing regular mechanisms for allied information sharing on cyber espionage threat actors, tactics, techniques and procedures, and motivations and bringing joint actions against any attributions of cyber-enabled economic espionage.

The FCC and NIST Should

- **Raise the bar on cybersecurity by developing and adopting cybersecurity standards that bolster data privacy in the Future Internet era.** Such an effort should be coupled with a modified re-instatement of Obama-era FCC programs to assess building security into 5G and now 6G standards.[204]

Contest Unfair Business Practices in Technology

The EU Should

- **Use anti-dumping measures to bring cases against or penalize Huawei for unfair business practices, such as state subsidies to support undercutting of European competitors.**

- **Study the costs of economic espionage and IP theft in Europe by immediately forming a Commission on the Theft of European Intellectual Property to study the modes, extent, impact, and possible solutions to Chinese intellectual property theft of European technology.** Europe's ability to harness the strengths of its university system to develop technology powerhouses while also maintaining autonomy hinges on not losing that innovation to competitors playing by a different set of rules. The Commission should issue a public report on its findings.

The United States and Allies Should

- **Use investment screening mechanisms (CFIUS and CFIUS-like regimes) to prevent opaque data collection and personal data exfiltration efforts.** The EU in particular can also use its Data Protection Authority to investigate improper data collection, transfer, or storage, though it may require national security input to its deliberations.

- **Prioritize WTO suits against unfair trade practices in the technology realm that opaquely favor Chinese Future Internet firms and decrease open market competition.**

Acknowledgements

The author would like to thank David Salvo, Zack Cooper, and Jessica Brandt for their helpful reviews of previous drafts of this report, as well as Kayla Goodson and Thomas Morley, without whom this project would not have been possible. The work also benefited tremendously over the past year from inputs by the rest of the team at the Alliance for Securing Democracy, including Rachael Dean Wilson, Bryce Barros, Matt Schrader, Joshua Rudolph, Bret Schafer, Sydney Simon, and Etienne Soula. A special thanks to Alliance for Securing Democracy interns Matthew Cohen and Katya Sankow.

The policy recommendations benefit from consultations with current and former executive and legislative branch officials across the Atlantic, Congressional staffers from both parties, telecommunications experts, China scholars, and various other experts.

This project is an outgrowth and extension of work started in support of the U.S. Cyberspace Solarium Commission.

Endnotes

[1] Lindsay Gorman, "A Silicon Curtain is Descending: Technological Perils of the Next 30 Years," The German Marshall Fund of the United States, September 13, 2019.

[2] Laura Rosenberger and Lindsay Gorman, "How Democracies Can Win the Information Contest," The Washington Quarterly, June 16, 2020; Laura Rosenberger, "Making Cyberspace Safe for Democracy: The New Landscape of Information Competition," Foreign Affairs, May/June 2020.

[3] Barry McCall, "5G: a transformative technology," The Irish Times, December 4, 2019.

[4] The State Council of the People's Republic of China, "Made in China 2025,"; The State Council of the People's Republic of China, Made in China 2025, July 7, 2015.

[5] Dan Strumpf, "Where China Dominates in 5G Technology," The Wall Street Journal, February 26, 2019; NB: There is some dispute on how patent power is measured. Tim Pohlmann, Who is leading the 5G patent race? A patent landscape analysis on declared 5G patents and 5G standards contributions, IPlytics, November 2019; Susan Decker, "Huawei Bets Big on European 5G Patents Despite Trump's Pressure," Bloomberg, March 12, 2020; Christina Petersson, "Why you shouldn't believe everything you read about 5G patents," Ericsson, October 11, 2019.

[6] Milo Medin, et al., The 5G Ecosystem: Risks and Opportunities for DoD, U.S. Department of Defense, April 3, 2019.

[7] David E. Sanger, et al., "In 5G Race With China, U.S. Pushes Allies to Fight Huawei," The New York Times, January 26, 2019; U.S. Department of Justice, "Chinese Telecommunications Conglomerate Huawei and Subsidiaries Charged in Racketeering Conspiracy and Conspiracy to Steal Trade Secrets," February 13, 2020; U.S. Department of Justice, "Chinese Telecommunications Device Manufacturer and its U.S. Affiliate Indicted for Theft of Trade Secrets, Wire Fraud, and Obstruction Of Justice," January 28, 2019; Bojan Pancevski, "U.S. Officials Say Huawei Can Covertly Access Telecom Networks," The Wall Street Journal, February 12, 2020.

[8] Mike Rogers et al., Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE ("House Huawei Report"), U.S. House of Representatives, October 8, 2012.

[9] Hugo Yen, Technology Factsheet: 5G, Belfer Center for Science and International Affairs, Spring 2020.

[10] Lindsay Gorman, "5G Is Where China and the West Finally Diverge," The Atlantic, January 5, 2020.

[11] Barclays, "Is your business 5G-ready?", April 3, 2019.

[12] Klint Finley, "The Wired Guide to 5G," Wired, December 18, 2019.

[13] Qualcomm, "The Evolution of Mobile Technologies," June 2014.

[14] Saran Singh Sound, "1G, 2G,…& 5G: The evolution of the G's," Stanford Management Science and Engineering, July 21, 2017.

[15] International Telecommunications Union (ITU), "What really is a Third Generation (3G) Mobile Technology."

[16] International Telecommunications Union (ITU), "About mobile technology and IMT-2000."

[17] Qualcomm, "The Evolution of Mobile Technologies."

[18] International Telecommunications Union (ITU), "Mobile Communications."

[19] Scott Fulton, "What is 5G? The business guide to next-generation wireless technology," ZDNet, June 25, 2020.

[20] Clare Duffy, "The big differences between 4G and 5G," CNN, January 17, 2020.

[21] Walid Saad, Mehdi Bennis, and Mingzhe Chen, "A Vision of 6G Wireless Systems: Applications, Trends, Technologies, and Open Research Problems," Cornell University, July 21, 2019.

[22] Rithu Thomas, Preetha Devan, and Abrar Khan, The Internet of Things: A Technical Primer, Deloitte Insights, 2018.

[23] Ibid.

[24] Fulton, "What is 5G?".

[25] Robert Morgus, Jocelyn Woolbright, and Justin Sherman, The Digital Deciders, New America, October 2018.

[26] James Manyika, et al., "Unlocking the potential of the Internet of Things," McKinsey Global Institute, June 1,

2015.

27 Paul Kennedy, The Rise and Fall of the Great Powers: Economic Change and Military Conflict from 1500 to 2000, Knopf Doubleday, 2010; Joseph S. Nye, The Future of Power, PublicAffairs, 2011; Sören Scholvin and Mikael Wigell, "Power politics by economic means: Geoeconomics as an analytical approach and foreign policy practice," Comparative Strategy, 2018; Ganesh Sitaraman, "Ten Theses on Political Economy and Foreign Policy," The American Prospect, April 29, 2019.

28 Shoshanna Zuboff, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power, PublicAffairs, 2019.

29 Gorman, "Silicon Curtain."

30 In particular, values of data privacy, freedom from government surveillance, and fundamental consumer protection have been put into question by application-layer technologies like facial recognition and the advent of intermediary companies like data brokers. Despite these industries' centrality to upholding democracy in the digital age, the United States has barely scratched the surface when it comes to this charge.

31 Huawei, "Digital Technology Drives Government Transformation."

32 Arjun Kharpal, "China's surveillance tech is spreading globally, raising concerns about Beijing's influence," CNBC, October 8, 2019.

33 Huawei, "White Paper: Safe City - A Revolution Driven by New ICT."

34 Huawei, "Using Technology to Anticipate Crime."

35 Cao Zhihui, "Nowhere to hide: Building safe cities with technology enablers and AI," Huawei, July 28, 2016.

36 Ibid.

37 "House Huawei Report."

38 Helene Fouquet, "No Huawei 'Smoking Gun' in Europe, French Cyber Chief Says," Bloomberg, January 30, 2020.

39 Matt Schrader, Friends and Enemies: A Framework for Understanding Chinese Political Interference in Democratic Countries, The Alliance for Securing Democracy, April 22, 2020.

40 Christopher Walker, et al., "The Cutting Edge of Sharp Power," Journal of Democracy, 2020.

41 Syed Rafiul Hussain, et al., "5GReasoner: A Property-Directed Security and Privacy Analysis Framework for 5G Cellular Network Protocol," 2019 ACM SIGSAC Conference on Computer and Communications Security, November 2019.

42 Colin Lecher and Russell Brandom, "Is Huawei A Security Threat? Seven Experts Weigh In," The Verge, March 17, 2019.

43 Elizabeth Kim, et al., "Forecast Analysis: Information Security, Worldwide, 2Q18 Update," Gartner Research, September 14, 2018.

44 Claude Barfield, "British security agency slams Huawei with 'scathing' report: Will it matter?", American Enterprise Institute, April 3, 2019.

45 Huawei Cyber Security Evaluation Centre Oversight Board, Annual Report 2019, A Report to the National Security Adviser of the United Kingdom, March 2019.

46 Adam Satariano, "Huawei Security 'Defects' Are Found by British Authorities," The New York Times, March 28, 2019.

47 Bojan Pancevski, "U.S. Officials Say Huawei Can Covertly Access Telecom Networks," Bloomberg, February 12, 2020.

48 Google Scholar, search for "Chinese Communist Party AND private companies" executed October 2, 2020.

49 Justin Sherman, "Is the U.S. Winning Its Campaign Against Huawei?", Lawfare, August 12, 2020; Robert Fife, et al., "Canada is now the only Five Eyes member to not ban or restrict use of Huawei 5G equipment," The Globe and Mail, July 15, 2020.

50 Lindsay Gorman, "NATO Should Count Spending on Secure 5G Towards Its 2% Goals," Defense One, December 3, 2019; Reid Standish, "Finland opens a new center to fight 'hybrid threats' from Russia and beyond," Public Radio International, October 3, 2017; Robin Emmott, "NATO cyber command to be fully operational in 2023," Reuters, October 16, 2018.

51 Bojan Pancevski and Sara Germano, "Drop Huawei or See Intelligence Sharing Pared Back, U.S. Tells Ger-

many," The Wall Street Journal, March 11, 2019; Reuters, "U.S. to discuss challenges posed by China, 5G with NATO allies" November 29, 2019; Robbie Gramer and Lara Seligman, "Can the U.S.-U.K. Special Relationship Weather the Huawei Storm?" Foreign Policy, January 30, 2020; Reuters, "U.S. lawmaker seeks ban on intelligence sharing with countries that use Huawei," January 8, 2020.

52 Ian Levy, "The future of telecoms in the UK," U.K. National Cyber Security Centre, January 28, 2020.

53 William James, "Pompeo backs 'Five Eyes' intelligence sharing despite UK decision on Huawei," Reuters, January 30, 2020.

54 Vivian Salama, "US won't change intelligence sharing policy with UK despite Huawei decision," CNN, February 14, 2020; Justine Coleman, "Trump's Germany envoy warns countries against using 'untrustworthy' 5G vendors amid Huawei tensions," The Hill, February 16, 2020.

55 Simeon Gilding, "5G choices: a pivotal moment in world affairs," Australian Strategic Policy Institute, January 29, 2020.

56 BBC, "Huawei and ZTE handed 5G network ban in Australia," August 23, 2018.

57 House Huawei Report 2012.

58 European Commission, "EU toolbox for 5G Security," January 29, 2020.

59 Laurens Cerulus, "Trump and friends: Where European countries come down on Huawei," Politico, May 26, 2020.

60 Reuters, "Huawei fears it may be excluded from Poland's 5G network," September 9, 2020.

61 Government of the Czech Republic, Prague 5G Security Conference, The Prague Proposals: The Chairman Statement on cyber security of communication networks in a globally digitalized world, May 3, 2019.

62 Mathieu Rosemain and Gwénaëlle Barzic, "Exclusive: French limits on Huawei 5G equipment amount to de facto ban by 2028," Reuters, July 22, 2020.

63 Leo Kelion, "Huawei 5G kit must be removed from UK by 2027," BBC News, July 14, 2020.

64 Gordon Corera, "Huawei: MPs claim 'clear evidence of collusion' with Chinese Communist Party," BBC News, October 8, 2020.

65 Huawei Cyber Security Evaluation Centre Oversight Board, Annual Report 2020, A Report to the National Security Adviser of the United Kingdom, September 2020; Gordon Corera, "Huawei 'failed to improve UK security standards'," BBC News, October 1, 2020.

66 Guy Chazan, "Germany crackdown set to exclude Huawei from 5G rollout," Financial Times, September 30, 2020.

67 Campbell Kwan, "Belgian telcos leave Huawei out in the cold for 5G rollouts," ZDNet, October 12, 2020; Supantha Mukherjee and Mathieu Rosemain, "Huawei ousted from heart of EU as Nokia wins Belgian 5G contracts," Reuters, October 9, 2020.

68 Reuters, "Denmark wants 5G suppliers from closely allied countries, says defence minister," June 8, 2020.

69 "TIM CEO says not a problem to develop 5G without Huawei," September 15, 2020; Reuters, "Italy government to discuss security of key networks, Huawei in 5G: sources," September 24, 2020.

70 Business Review, "First security certification granted to Huawei in Spain," June 23, 2020.

71 Sergio Goncalves, "Exclusive: Portugal telcos won't use Huawei for core 5G networks though no government ban," Reuters, July 30. 2020.

72 Jonathon Keane, "Irish telco Eir says it will stick with Huawei as it continues 1 billion euro investment strategy," CNBC, September 11, 2020.

73 William C. Hannas, et al., Chinese Industrial Espionage: Technology Acquisition and Military Modernisation, Taylor & Francis, 2013.

74 Nancy Hungerford, "Chinese theft of trade secrets on the rise, the US Justice Department warns," CNBC, September 22, 2019.

75 Executive Office of the President of the United States, Office of the United States Trade Representative, Findings Of The Investigation Into China's Acts, Policies, And Practices Related To Technology Transfer, Intellectual Property, And Innovation Under Section 301 Of The Trade Act Of 1974, March 22, 2018.

76 The Commission on the Theft of American Intellectual Property, Update To The IP Commission Report, The National Bureau of Asian Research, 2017.

77 Hungerford, "Chinese theft of trade secrets on the rise."

78 Chuin-Wei Yap, et al., "Huawei's Yearslong Rise Is Littered With Accusations of Theft and Dubious Ethics," The Wall Street Journal, May 25, 2019.

79 Corinne Ramey and Kate O'Keeffe, "China's Huawei Charged With Racketeering, Stealing Trade Secrets," The Wall Street Journal, February 13, 2020.

80 United States District Court for the Western District of Washington at Seattle, "Indictment: United States of America v. Huawei Device Co., LTD. ("Huawei Indictment")," January 16, 2019.

81 Christopher Glyer, et al., "This Is Not a Test: APT41 Initiates Global Intrusion Campaign Using Multiple Exploits," FireEye, March 25, 2020.

82 Catalin Cimpanu, "Building China's Comac C919 airplane involved a lot of hacking, report says," ZDNet, October 14, 2019.

83 White House Office of Trade and Manufacturing Policy, How China's Economic Aggression Threatens the Technologies and Intellectual Property of the United States and the World, June 2018.

84 Catalin Cimpanu, "FBI is investigating more than 1,000 cases of Chinese theft of US technology," ZDNet, February 9, 2020.

85 Michael Brown and Pavneet Singh, China's Technology Transfer Strategy: How Chinese Investments in Emerging Technology Enable A Strategic Competitor to Access the Crown Jewels of U.S. Innovation, Defense Innovation Unit Experimental (DIUx), January 2018; The White House Office of the Press Secretary, "FACT SHEET: President Xi Jinping's State Visit to the United States," September 25, 2015; Up-tick in Chinese targeting "against multiple sectors of the economy, including biotech, defense, mining, pharmaceutical, professional services, transportation, and more." CrowdStrike, "CrowdStrike Report Reveals Cyber Intrusion Trends from Elite Team of Threat Hunters," October 9, 2018.

86 U.S. Department of Justice, "Attorney General Jeff Sessions Announces New Initiative to Combat Chinese Economic Espionage," November 1, 2018.

87 Laura Sullivan and Cat Schuknecht, "As China Hacked, U.S. Businesses Turned A Blind Eye," NPR, April 12, 2019.

88 William Wilkes, "Hit by Chinese Hackers Seeking Industrial Secrets, German Manufacturers Play Defense," The Wall Street Journal, September 23, 2017.

89 Didier Burg, "Les Pays-Bas en proie à l'espionnage des Chinois," Les Echos, May 16, 2019.

90 Ministry of Foreign Affairs of the Kingdom of the Netherlands, The Netherlands and China: a new balance, October 2019.

91 Patricia Weiss and Ludwig Burger, "German prosecutors charge Chinese-born engineer in industrial espionage case," Reuters, November 15, 2018.

92 Patrick Wintour, "US and UK accuse China of sustained hacking campaign," The Guardian, December 20, 2018.

93 Detica and the U.K. Cabinet Office, The Cost Of Cyber Crime: A Detica Report In Partnership With The Office Of Cyber Security And Information Assurance In The Cabinet Office, Detica, 2011.

94 U.S. Federal Bureau of Investigation, "Chinese Military Hackers Charged in Equifax Breach: Intrusion Affected Nearly Half of All Americans," February 10, 2020.

95 Sean Lyngaas, "Marriott discloses data breach affecting 5.2 million guests," CyberScoop, March 31, 2020.

96 David Cyranoski, "China expands DNA data grab in troubled western region," Nature, May 24, 2017.

97 Kirsty Needham, "Special Report: COVID opens new doors for China's gene giant," Reuters, August 5, 2020.

98 David Cyranoski, "China's massive effort to collect its people's DNA concerns scientists," Nature, July 7, 2020; Sui-Lee Wee and Paul Mozur, "China Uses DNA to Map Faces, With Help From the West," The New York Times, December 10, 2019; Sui-Lee Wee, "China Uses DNA to Track Its People, With the Help of American Expertise," The New York Times, February 21, 2019; Emma Yasinski, "China Clamps Down on Foreign Use of Chinese Genetic Material and Data," The Scientist, June 17, 2019.

99 Karen Li Xan Wong and Amy Shields Dobson. "We're Just Data: Exploring China's Social Credit System in Relation to Digital Platform Ratings Cultures in Westernised Democracies," Global Media and China, June 2019; Eunsun Cho, "The Social Credit System: Not Just Another Chinese Idiosyncrasy," Princeton Journal of

Public and International Affairs, 2019.

[100] Ben Doherty, "China has built 'massive global data-collection ecosystem' to boost its interests," The Guardian, October 14, 2019.

[101] Samantha Hoffman, Engineering global consent: The Chinese Communist Party's data-driven power expansion, Australian Strategic Policy Institute, 2019.

[102] GTCOM, "GTCOM releases alternative data to explore the unique value of global financial quantification," January 10, 2019.

[103] Ibid.

[104] Doherty, "China has built 'massive global data-collection ecosystem' to boost its interests."

[105] GTCOM, "GTCOM signs a strategic contract with Huawei to build an application ecology on the basis of AI big-data technology," May 9, 2019; cited in Hoffman, "Engineering Global Consent."

[106] Lindsay Gorman, "The challenge in securing critical information," Fifth Domain, July 24, 2019.

[107] International Telecommunications Union, Telecommunications Standardization Sector, "Requirements and functional architecture of a smart street light service ("ITU Recommendation ITU-T Y.4458")," June 2019; International Telecommunications Union, ITU-T Study Group 16, "Focus Group on Vehicular Multimedia (FG-VM),"; Xu Shenglan and Xue Hua, "Dunhuang: On the Silk Road with smart tourism and big data," Huawei, September 19, 2019; 3GPP member list: ETSI, "3GPP MEMBERSHIP."

[108] Company record from qichacha.com.

[109] Carl O'Donnell, et al., "Told U.S. security at risk, Chinese firm seeks to sell Grindr dating app," Reuters, March 27, 2019.

[110] Yuan Yang and James Fontanella-Khan, "Grindr sold by Chinese owner after US national security concerns," Financial Times, March 7, 2020.

[111] Ana Swanson, "Trump Administration Blocks Chinese Acquisition of Hotel Software Company," The New York Times, March 6, 2020; The White House, "Executive Order Regarding the Acquisition of Stayntouch, Inc. by Beijing Shiji Information Technology Co., Ltd.," March 6, 2020.

[112] Kiran Stacey, et al., "US launches national security probe in to TikTok," Financial Times, November 1, 2019; Alex Sherman, "TikTok reveals detailed user numbers for the first time," CNBC, August 24, 2020.

[113] Reid Whitten, "Investments With Borders: CFIUS-Style Foreign Investment Review Goes Global," National Law Review, April 9, 2019.

[114] Joshua Kirschenbaum, et al., "EU Foreign Investment Screening – At Last, a Start," The German Marshall Fund of the United States, September 26, 2019.

[115] Laura Rosenberger, "China's Coronavirus Information Offensive," Foreign Affairs, April 22, 2020.

[116] Maria Abi-Habib, "India Bans Nearly 60 Chinese Apps, Including TikTok and WeChat," The New York Times, June 29, 2020; Saqib Shah, "UK MPs to quiz TikTok on data privacy as government mulls restrictions," S&P Global Market Intelligence, September 21, 2020; Asha Barbaschow, "TikTok tells Australian Senate committee it doesn't want to be a 'political football'," ZDNet, September 21, 2020; Guan Cong and Denise Jia, "EU to probe TikTok's data processing and privacy practices," Caixin, June 12, 2020; Vincent Manancourt and Laura Kayali, "TikTok finds safe haven in Europe," Politico, August 6, 2020; Natasha Lomas, "TikTok is being investigated by France's data watchdog," TechCrunch, August 11, 2020.

[117] Lily Hay Newman, "As 5G Rolls Out, Troubling New Security Flaws Emerge," Wired, November 12, 2019.

[118] Gavin Bowring, "Vietnam yields cautionary tale over Chinese investment," Financial Times, November 27, 2014.

[119] Gorman, "Silicon Curtain," 2019.

[120] Shannon Vavra, "These tiny islands are at the heart of an uncovered Chinese phishing campaign," CyberScoop, April 30, 2020.

[121] The Daily Star, "Vietnam rejects China's claims over two archipelagoes in the East Sea," April 29, 2020.

[122] Chuin-Wei Yap, "State Support Helped Fuel Huawei's Global Rise," The Wall Street Journal, December 25, 2019.

[123] Melanie Hart and Blaine Johnson, "Mapping China's Global Governance Ambitions," Center for American Progress, February 28, 2019.

124 Elsa B. Kania, “China’s play for global 5G dominance—standards and the ‘Digital Silk Road’,” Australian Strategic Policy Institute, June 27, 2018.

125 Patrick Donahue, et al., “Deutsche Telekom Warns Huawei Ban Would Hurt Europe 5G,” Bloomberg, January 28, 2019.

126 Shi Jiangtao, “Chinese ambassador accused of threatening German car industry if Huawei is frozen out,” South China Morning Post, December 15, 2019.

127 Christian Lenz and Etienne Soula, “Germany’s Faustian Bargain on Trade with China,” The Alliance for Securing Democracy, February 26, 2020.

128 Sanjeev Miglani and Neha Dasgupta, “China warns India of ‘reverse sanctions’ if Huawei is blocked,” Reuters, August 6, 2019; Laura Hughes and Helen Warrell, “China envoy warns of ‘consequences’ if Britain rejects Huawei,” Financial Times, July 6, 2020.

129 Strumpf, “Where China Dominates in 5G Technology.”

130 Lindsay Gorman, “The U.S. Needs to Get in the Standards Game—With Like-Minded Democracies,” Lawfare, April 2, 2020.

131 As of August 2020, the 3GPP lists 176 China-based members (not including 14 based in Taiwan and labeled by the ITU as a “Province of China) and 93 U.S. members as full voting members. ETSI, “Individual Members.”

132 *See* International Telecommunications Union, “ITU-T Focus Groups,”; International Telecommunications Union, ITU-T Study Group 16, “Focus Group on Vehicular Multimedia (FG-VM).” The Focus Group on Vehicular Multimedia drafts technical specifications for a future where the vehicle is no longer “mere transport tool,” but an infotainment space and multimedia platform along with the home and office.

133 Eurasia Group, Eurasia Group White Paper: The Geopolitics of 5G, Washington, November 15, 2018.

134 U.S. Information Technology Office, “CAE Commences Research on China Standards 2035.”

135 China Legislation and Standards Platform, “China Standard 2035,” January 2018.

136 Jiang J., Wang J., Li S., and Zhang J. Game Theory Strategy for Information Standardization Work in Manufacturing Enterprise, Springer, London, 2008

137 Strumpf, “Where China Dominates in 5G Technology.”

138 Hilary McGeachy, US-China Technology Competition: Impacting A Rules-Based Order, United States Studies Centre, May 2, 2019.

139 Ibid.

140 Houlin Zhao, “China’s One Belt, One Road can improve lives at scale through ICT investment,” ITUNews, May 16, 2017.

141 Strumpf, “Where China Dominates in 5G Technology.”

142 Frank Hersey, “Lenovo founder in public backlash for ‘unpatriotic 5G standards vote’,” TechNode, May 16, 2018; Weixin, “行动起来，誓死打赢联想荣誉保卫战！[Xíngdòng qǐlái, shìsǐ dǎ yíng liánxiǎng róngyù bǎowèi zhàn!]”, May 16, 2018; John Chen, et al., China’s Internet of Things, SOSI International, October 2018.

143 Anna Gross, et al., “Chinese tech groups shaping UN facial recognition standards,” Financial Times, December 1, 2019.

144 Ibid.

145 Madhumita Murgia and Anna Gross, “Inside China’s controversial mission to reinvent the Internet,” Financial Times, March 27, 2020.

146 Gorman, Lawfare.

147 ITU Recommendation ITU-T Y.4458.

148 Gorman, Lawfare.

149 Technically, 3GPP is not a standards body but a technical coordination body for national standards organizations to come together and propose global standards (to, for example, the ITU).

150 3GPP, “3GPP FAQs.”

151 IEEE Spectrum, “3GPP Release 15 Overview.”

152 3GPP, “2019 Presentation.”

153 Sasha Sirotkin, “5G Standards: 3GPP Release 15, 16, and beyond,” Wireless Russia, June 17, 2019.

154 3GPP, "Release 17," accessed September 9, 2020.
155 Kristine Lee, "It's Not Just the WHO: How China Is Moving on the Whole U.N.," Politico, April 15, 2020.
156 McGeachy, US-China Technology Competition.
157 "United States Proposals and Positions for the U.S. Delegation to the 2020 World Telecommunication Standardization Assembly (WTSA-2020)," 85 Fed. Reg. 6256, 6256-6258.
158 Caleb Henry, "Traction building to add C-band to next World Radiocommunication Conference agenda," SpaceNews, September 27, 2019.
159 International Telecommunications Union, "Focus Group on Technologies for Network 2030."
160 Ibid.
161 Marco Hogewoning, "Do We Need a New IP?" RIPE NCC, April 22, 2020.
162 Huawei, "A Brief Introduction about New IP Research Initiative."
163 Robert Clark, "'New IP' is an actual Huawei threat to networks," Light Reading, April 1, 2020.
164 CNTechPost, "Why did Huawei's 'New IP' encounter new problems?", April 9, 2020.
165 Huawei, Towards a New Internet for the Year 2030 and Beyond.
166 Wei Shi, "Consensus on 6G is gradually forming," Telecoms, March 17, 2020.
167 Houlin Zhao, "China's One Belt, One Road can improve lives."
168 United Nations Economic and Social Commission for Asia and the Pacific (UNESCAP), A Study of ICT Connectivity for the Belt and Road Initiative in China-Central Asia Corridor, September 2017 ("UNESCAP 2017 Report").
169 Du Mingming, "ITU secretary-general: ICT a foundation for development under Belt and Road Initiative," People's Daily, May 23, 2017.
170 Tom Miles, "Huawei allegations driven by politics not evidence: U.N. telecoms chief," Reuters, April 5, 2019.
171 Björn Fägersten and Tim Rühlig, China's standard power and its geopolitical implications for Europe, Stockholm: The Swedish Institute of International Affairs, 2019.
172 UNESCAP 2017 Report.
173 Zhao, "China's One Belt, One Road can improve lives at scale through ICT investment."
174 Marja Matinmikko-Blue et al., White Paper On 6G Drivers and the UN SDGS, Oulu: University of Oulu, June 2020.
175 Malcolm Johnson, "How ITU is ramping up its efforts on AI for Good," ITUNews, October 24, 2019.
176 Jessica Fjeld and Adam Nagy, Principled Artificial Intelligence: Mapping Consensus In Ethical And Rights-Based Approaches To Principles For AI, Berkman Klein Center, January 15, 2020.
177 Malcolm Johnson, "Speech by Malcolm Johnson, ITU Deputy Secretary-General," International Telecommunications Union, October 21, 2019.
178 Malcolm Johnson, "How ITU is ramping up its efforts on AI for Good," International Telecommunications Union, October 24, 2019.
179 Malcolm Johnson, "Opening remarks by Malcolm Johnson, ITU Deputy Secretary-General," International Telecommunications Union, June 18, 2020.
180 Tencent, "Tencent and United Nations announce global partnership to hold thousands of conversations online through platforms including VooV Meeting for the UN's 75th anniversary," April 1, 2020.
181 Jeffrey Knockel, et al., We Chat, They Watch: How International Users Unwittingly Build up WeChat's Chinese Censorship Apparatus, Citizen Lab, May 7, 2020.
182 Colum Lynch and Robbie Gramer, "U.N. Backs Down on Partnership With Chinese Firm for 75th Anniversary," Foreign Policy, April 15, 2020.
183 Ibid.
184 GTCOM, "Summit on Translation in China: 70 Years of Development -- GTCOM CEO Eric Yu Shares Ideas on "HAI, Language Technology 4.0," November 11, 2019.
185 GTCOM, "China Construction Bank works with GTCOM to jointly promote platform for innovation in fintech," July 4, 2019.
186 Jyrki T. J. Penttinen, 5G Explained: Security and Deployment of Advanced Mobile Communications, John Wiley & Sons, 2019.

[187] Jeffrey Ding, et al., "Chinese Interests Take a Big Seat at the AI Governance Table," New America, June 20, 2018.

[188] Guo Guozhong, "中国主导国际物联网与区块链融合标准研究 [Zhōngguó zhǔdǎo guójì wù liánwǎng yǔ qū kuài liàn rónghé biāozhǔn yánjiū]," STDaily, July 18, 2018.

[189] Françoise Nicolas, et al., China's Belt & Road and the World: Competing Forms of Globalization, Alice Eckman, April 2019.

[190] International Electrotechnical Commission.

[191] C. Todd Lopez, "Pentagon Official: U.S., Partners Must Lead in 5G Technology Development," U.S. Department of Defense, March 26, 2019.

[192] Jon Brodkin, "US military is furious at FCC over 5G plan that could interfere with GPS," Ars Technica, May 8, 2020.

[193] United States Congress, Cyberspace Solarium Commission Report, March 2020.

[194] Adam Satariano, "The World's First Ambassador to the Tech Industry," The New York Times, September 3, 2019.

[195] Lauren C. Williams, "Pentagon sets up new 5G shop," FCW, August 13, 2019.

[196] U.S. Department of Defense, "DOD Names Seven Installations as Sites for Second Round of 5G Technology Testing, Experimentation," June 3, 2020.

[197] Office of Senator Mark Warner, "National Security Senators Introduce Bipartisan Legislation to Develop 5G Alternatives to Huawei," January 14, 2020.

[198] Government of the Czech Republic, Prague 5G Security Conference, The Prague Proposals: The Chairman Statement on cyber security of communication networks in a globally digitalized world, Prague, May 3, 2019.

[199] North Atlantic Treaty Organization, "NATO Defence Ministers to address key issues for the Alliance," October 23, 2019.

[200] Gorman, Defense One, 2019.

[201] Gorman, Lawfare, 2020.

[202] International Organization for Standardization, "ISO/IEC JTC 1/SC 42: Artificial intelligence."

[203] Kurt DelBene, Milo Medin, and Richard Murray, "The Road to Zero Trust (Security)," Defense Innovation Board, July 9, 2019.

[204] Tom Wheeler and David Simpson, "Why 5G requires new approaches to cybersecurity," Brookings Institution, September 3, 2019.