The Geopolitics of Technology

Big Data, Artificial Intelligence and 5G in a Multipolar World

AUTHOR:
Erik Brown, Research Analyst, Global Risk Institute

ABSTRACT

Emerging technologies like Big Data, Artificial Intelligence and 5G telecommunications are of critical importance to the financial services industry, underpinning new products and services and transforming operational processes. These innovations are also sources of increasing geopolitical rivalry, as economic giants like the United States, China and the European Union vie for leadership in research, commercialization and deployment. Galvanized by concern for national security and economic competitiveness, the ongoing contest between states for technological leadership is not without its costs. Efforts to impose sovereign controls over the internet are dividing cyberspace along national borders, while new economic barriers threaten to restrict trade, limit information exchange and stifle the free flow of capital. As conduits for global commerce, financial institutions are acutely vulnerable to the disruption underway. Thus, robust geopolitical analysis of the 21st century tech race should be a key feature of enterprise risk management and strategic decision-making in the financial sector.

INTRODUCTION

In his celebrated address to Rice University in September 1962, President John F. Kennedy looked toward the "opening vistas of space" and pledged that the United States would land on the Moon within 10 years. The project would serve to concentrate the nation's energies and its talents in service of a collective human endeavour.[1] The space program had a pacific objective at its core,[2] as an undertaking to ensure the cosmos would not be "governed by a hostile flag of conquest but by a banner of freedom and peace."[3] Yet Kennedy also alluded to the political implications at stake, declaring that "no nation which expects to be the leader of other nations can expect to stay behind in this race for space."[4] To some extent, the "moonshot" would become yet another theatre in the larger Cold War with the Soviet Union. A scientific effort would assume strategic dimensions.

On the 50th anniversary of the Apollo 11 mission, technology feeds geopolitical competition once more. Schumpeterian advancements in fields like data analytics, artificial intelligence and telecommunications attract global attention and drive investment. This "Fourth Industrial Revolution" also pits emerging and incumbent powers against each other. A growing hub of innovation, China is primed for rivalry with the United States, and to a lesser extent, the European Union and other high-value added economies. The Communist Party (CCP) has prioritized advanced technological development with its "Made in China 2025" policy, aiming to reduce dependence on foreign imports, ascend the economic value chain and overcome the Middle-Income Trap. However, the U.S argues that the 2025 strategy builds upon illegal and discriminatory trade practices like forced technology transfer, cyber espionage, and the theft of intellectual property, and other countries share similar concerns.[5] The Trump Ad-

ministration now frames China as a revisionist power seeking "to shape a world antithetical to U.S. values and interests,"[6] while the European Commission labels it "an economic competitor in the pursuit of technological leadership" and "a systematic rival promoting alternative models of governance."[7] In contrast, many among the Chinese elite perceive the hard line taken on trade in Washington as an attempt to contain China's rise rather than a sincere effort to create a more balanced economic relationship.[8]

In the race to innovate, the geopolitical determinants of big data, AI and 5G are critical to the financial services industry. These technologies can help institutions responsibly leverage client data to improve product development and customer relations, refine human capital procurement, investment strategies and loan assessment, bolster cybersecurity and fraud detection and develop new mobile services and capabilities. However, public policy, macroeconomic interest and national security priorities could ultimately restrict their commercial applications. To check global rivals, states could impose new sovereign controls over the internet that balkanize cyberspace in line with physical borders. Governments fearful of losing their technological advantage could also enforce new restrictions on trade, market access, intellectual property and capital flows that fragment supply chains and stifle growth. These actions can manifest downstream to affect business lines in complex and ambiguous ways and test the efficacy of risk management systems. A financial services provider must first understand the political dimensions of emerging technologies before it can assess the associated enterprise risks, test its resiliency and design appropriate governance strategies.

Big Data

Technical Overview

The proliferation of digital technologies has produced an unprecedented quantity of data. This progress has also had transformative effects on the meaning and sources of value in the modern economy. Increased computing power has reduced the cost of collection and analysis and data is now a lucrative form of capital.[9] It has become "the new oil", serving as the key underpinning commodity for the 21st century.[10] The emergence of "big data" marks not only an increase in the volume of recorded information but also an increase in its complexity.[11] Cyberspace provides for newfound variety in data sets. The internet yields a diverse reservoir of unstructured content (in addition to structured and semi-structured),[12] like social media posts, documents, and video, to which conventional analytical methods do not apply.[13] These unstructured sets are collected at high velocity, in an iterative process, but their disorganization can also lead to problems of quality control or questionable accuracy.[14] Regardless, the commercial applications of big data analytics are vast, and in some cases well-established across industries and sectors. It is the emerging data governance system that now serves as a primary source for geopolitical stress rather than the technology itself, as jurisdictions adopt conflicting regulatory regimes and states compete to influence global standards.

When Data Gets Political

A set of divergent ecosystems for data privacy and storage are solidifying around the globe, each shaped by different philosophies and value systems. By one account, four prevailing regulatory models exist. A pioneer of the digital age, the U.S. has produced two distinct but interrelated systems: A "Silicon Valley Model" that adopts an open, libertarian vision of the

internet, with the kind of government participation that cultivates rather than stifles innovation (like providing for free information flow);[15] and a "Washington Model" that treats cyberspace as a primarily commercial entity.[16] The state effectively plays a secondary role to private interest in both cases. In the EU, a "Bourgeois Model" is developing where the dignity of the individual is prioritized above the fast-paced open market; an attitude manifest in the new General Data Protection Regulation (GDPR). The European formula relies on public trust in government to defend the interests of the citizen against the corporation.[17] Finally, in the world's second largest economy, a unique "Chinese Model" is emerging where domestic companies predominate in a siloed internet, mass-surveillance is enhanced, and the state serves as the key organizing node.[18]

This nomenclature may not represent the full diversity of data governance systems in both developed and emerging markets. Local cultures and circumstances will ultimately shape national regulation to some extent. With a focus on the United States, China and the EU, however, the four-tier framework does include the markets that are most likely, through their shear political and economic heft, to influence technology policy in foreign jurisdictions and multilateral fora. Close attention to these three examples may indicate which standards will hold the greatest international clout.

In the case of the U.S., the largest data companies in the world operate under a largely patchwork set of privacy standards. There is no comprehensive federal regulation in force beyond some sector-specific provisions (healthcare, financial services, etc.), while measures at the state-level can be inconsistent and contradictory.[19] U.S. privacy law centres on protecting the individual from government rather than from private corporations,[20] and internet companies have largely self-regulated thus far.[21] Still, recent policy changes may reflect a growing appetite for reform. The new California Consumer Privacy Act (CCPA) significantly empowers individuals with greater control over their data, and outlaws its sale without consent.[22] Furthermore, the major U.S. technology companies have even begun to lobby in Washington for a federal privacy bill, although they may be seeking to shape pro-industry standards to supersede less advantageous state law like the CCPA.[23] In any event, the Trump Administration seems largely disinterested in technology policy and disinclined toward further regulation.[24]

Apart from questions of privacy, the U.S. has also taken a decidedly liberal approach to the storage and management of big data. National governments can oblige a company to store information in the same country where it was first collected. These measures can create operational problems for businesses, as companies increase their overhead costs to set up local storage facilities.[25] Washington generally opposes data localization laws of this kind, interpreting the provisions as a trade barrier.[26] However, the U.S. stands out as an outlier in a global move toward greater restrictions on information flow. As measured by the European Centre for International Political Economy, significant data transfer restrictions around the world increased almost three-fold between 2006 and 2016.[27]

China stands at the forefront of data protectionism. The "Great Firewall" effectively isolates the Chinese internet from the global cyberspace. State authorities curate content and control user access within a "walled garden." Many international websites and service providers are either inaccessible or unavailable on the Mainland, while a domestic technology suite dominated by national champions like

Baidu, Tencent and Alibaba has grown in place of American or other foreign equivalents. To encapsulate this vision for the digital realm, Beijing has evoked the principle of "cyber-sovereignty." It argues that the digital sphere should essentially reflect physical borders, and that the nation-state should have strict authority over internet activity within its own legal jurisdiction.[28] The CCP has not only promoted greater technological self-sufficiency, but drafted new security regulations to protect critical infrastructure like cloud-computing and financial services.[29] Government access to data has also expanded through legislation. In the Cyber Security Law of the People's Republic of China (effective 2017), legislators not only enshrine localization requirements, with some exceptions subject to government regulation, but mandate that "Network operators shall provide technical support and assistance to public security organs and national security organs that are safeguarding national security and investigating criminal activities in accordance with the law."[30]

The Cyber Security Law may grant the state greater oversight and surveillance powers, but the CCP is also seeking more stringent rules on commercial data collection and use. An early example of this commitment is the Personal Information Security Specification (effective May 2018), which sets forth new corporate data governance standards, drawing inspiration from the EU while adapting to domestic circumstances.[31] To balance innovation against consumer privacy, Beijing is keen to prevent commercial usage restrictions from inhibiting data-driven industries like AI.[32]

In contrast, Brussels may fall short of an equilibrium that satisfies its privacy and security priorities without undermining its own competitiveness in data-driven technologies. The EU has labelled privacy a "fundamental right" to be enforced and promoted across industries and member-states. GDPR mandates that consumers provide "affirmative consent" to the commercial use of their data, and grants users a "Right to Be Forgotten."[33] The law is also applicable even when a entity has no physical presence in the EU.[34] In terms of data localization, GDPR offers some compromise between the American and Chinese models. Article 45 stipulates that "A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organization in question ensures an adequate level of protection."[35] In this respect, the EU holds its own data governance rules as a benchmark from which to measure the quality of competing international frameworks, and makes restrictions contingent on whether other jurisdictions meet those standards. Foreign nations are beholden to European rules if their companies are to freely transfer data out of the Common Market.

The Systems Collide

If big data is indeed the new petroleum, the political dynamics that have influenced commodities markets in the past could increasingly hold sway in the cyber domain. Since the nation that controls the data supply and writes the underpinning governance rules can have a distinct advantage in future economic determinants, including the revolutions in AI and 5G, national economic and strategic interests are set on a collision course.

Big data geopolitics manifests when companies face punitive costs or obligations in foreign jurisdictions. Given the comparatively more stringent rules in Europe and China, some illustrative examples involve U.S. technology companies operating in the two markets. Google

is a good case study in this regard. The company incurred a €50 million penalty for violations under GDPR,[36] with billions more levied in EU anti-trust fines,[37] while its Project Dragonfly seeks to adapt a new search engine to filter content in line with Chinese government restrictions.[38] In these scenarios, Brussels and Beijing effectively leveraged their market power to impose legal restrictions on Alphabet, above and beyond those to which it is subject in its home market.

Geopolitical tensions also rise when competing technology powers seek to project their standards abroad and tilt international regulation in their favour. The U.S. has sought to prohibit localization requirements in formal trade negotiations with some measure of success. The Trans-Pacific Partnership (TPP) included American provisions on data transfer that the 11 remaining signatories carried forward after the Trump Administration withdrew from the agreement.[39] More recently, the United States-Mexico-Canada Agreement (USMCA) liberalized data storage and flow for digital trade in general (Chapter 19, Sec. 11 & 12)[40] and financial services in particular (Chapter 17, Sec. 17 & 18).[41] Through its Belt and Road Initiative (BRI), China is also using economic relationships to proliferate its homegrown data infrastructure and state-centered internet ecosystem.[42] The proposed "Digital Silk Road" includes improved satellite networks and cross-border/underwater fiber optic cabling,[43] and a number of African countries have already started to adopt cyber regulations in the Chinese mold.[44] Beijing has pushed for multilateral cooperation on internet governance within the United Nations, a forum in which it can draw support from likeminded developing countries and bolster state influence at the expense of the private-sector and civil society.[45] And in the EU, the privacy laws to which foreign companies are subject within the Common Market encourage other governments to adjust their regulatory systems to match,[46] and are pushing Silicon Valley to apply European standards across its global infrastructure for the sake of operational simplicity.[47]

Artificial Intelligence

Technical Overview

Artificial Intelligence (AI) refers to machines that can mimic human cognition and decision-making.[48] The current wave in AI innovation is driven by a key underlying technology called Deep Learning. Massive amounts of data are fed into a neural network – an algorithm with a structure based on the human brain – and the machine extrapolates patterns to inform decisions. In recent years, advances in the scale of data collection and computing power, along with a major breakthrough in training methods, have allowed researchers and innovators to fully tap the potential of neural networks.[49] The training process for these systems can take a few different forms: Supervised learning, where algorithms learn from labelled data; unsupervised learning, where input data is unlabeled; and reinforcement learning, where an algorithm collects data directly from the surrounding environment and identifies optimal actions based on the maximization of rewards it earns from those decisions.[50]

The AI development curve can be broken down into three different phases. Narrow Artificial Intelligence (ANI) refers to an AI system that executes a pre-determined task with pre-defined input data. An ANI cannot move beyond these restrictions to independently perform new tasks or train on new data sources.[51] All current applications of AI technologies fall into the ANI category.[52] However, Kai-Fu Lee maps the future course of Narrow AI in four "waves": Internet AI that interprets human preferences, curates and

recommends content;[53] Business AI, that applies AI to an organization's structured data for optimization purposes;[54] Perception AI that merges the online and offline worlds by integrating sensory technology with AI;[55] and Autonomous AI that incorporates the previous three phases into one system operating independently and capable of adapting to changing conditions.[56]

The two other as-of-yet unrealized phases of AI development are General Artificial Intelligence (AGI) and Artificial Superintelligence (ASI). An AGI is a sentient machine with capabilities fully analogous to that of a human, including reasoning, problem-solving, creativity and innovation.[57] ASI is a system with intellectual abilities beyond those of a human being, capable of superior cognitive performance across disciplines.[58] Despite the predictions and warnings of scientists and intellectuals, however, Lee forecasts that it will be many decades before AGI (or by extension ASI) is fully realized, perhaps even centuries.[59]

The Race to Innovate

For China, the "Sputnik Moment" that inspired its massive AI push came in 2017 when Google's AlphaGo deep learning system defeated world champion Go player Ke Jie. AlphaGo's triumph in this match, and in its victory over Korean player Lee Sedol the previous year, garnered massive attention in Beijing and sparked a wholesale leap in funding, policy and education.[60] At the core of this national effort is the New Generation Artificial Intelligence Development Plan (NGDP). The document casts AI as a primarily state-driven project, although the Chinese private-sector will likely continue to set the industry pace.[61] The NGDP labels AI "a new focus of international competition" and frames it as "the core driving force for a new round of industrial transformation."[62] Elsa Kania of the Center for New American Security describes the "'three-in-one'" set of objectives for the NGDP: to foster new AI applications and products, grow the domestic industry, and overcome barriers in research and development.[63] Apart from these economic targets, Beijing may have another strategic objective in-mind: specific commitments are made to "Strengthen military-civilian integration in the AI domain" and to "Promote military-civilian two-way transformation of AI technology."[64]

The CPP defines a three-stage process to reach its goals, with clear objectives and timelines. According to the NGDP, by 2020, China should be "in step with globally advanced levels" in both its AI technology and applications. By 2025, it should "achieve major breakthroughs in basic theories for AI, such that some technologies and applications achieve a world-leading level." And by 2030, China's "theories, technologies, and applications should achieve world-leading levels," and the country should become "the world's primary AI innovation center."[65] Reflecting on the plan, Kai-Fu Lee compares the NGDP specifically to President Kennedy's moonshot speech, noting that it sets forth "an all-hands-on-deck approach to national innovation."[66] In contrast, past iterations of a U.S. AI strategy have not captured American attention to the same extent.[67]

However, the winds may be shifting in Washington. The Trump Administration has made AI a policy priority to some extent and taken measures to support and defend private-sector innovation. In February 2019, President Trump issued an "Executive Order on Maintaining American Leadership in Artificial Intelligence," which recognized the critical importance of AI dominance for "maintaining the economic and national security of the United States" and set forth a set of policy objectives, including the protection of "critical AI technologies from acquisition by strategic

competitors and adversarial nations."[68] This "American AI Initiative" also calls for increased R&D investment within federal agencies, greater access to federal data and resources, increased investments in education and skills-training, new governance standards, and a global marketplace beneficial to U.S. industry.[69] Ethical considerations were also at play in the announcement. In an accompanying op-ed for *Wired* magazine, Michael Kratsios, Deputy Assistant to the President for Technology Policy, underscored that the Executive Order is designed to ensure the U.S. wins "the race for AI," but stipulated that it should not be harnessed "at the expense of our civil liberties and freedoms."[70]

Europe not only shares the American attention to principle, but seeks to go further and cement "ethical AI" as its primary competitive advantage. With the GDPR, the EU contributed to building its "sustainable approach to technologies" and is set to follow a similar line with respect to AI.[71] Its 2018 Coordinated Plan on Artificial Intelligence suggested that "Europe can become a global leader in developing and using AI for good and promoting a human-centric approach and ethics-by-design principles."[72] Brussels is intent on maintaining a competitive global presence in the AI field while also accounting for both potential economic disruption and the moral and social implications of the technology.[73] To realize its pan-continental vision, the Commission has also recognized the need to cooperate with national governments;[74] some member-states like France[75] and Germany[76] have independent AI strategies in place.

Strengths and Weaknesses of the AI Titans

Geopolitics can shape AI in much the same way it does big data. States may increasingly take efforts to protect their domestic industries and leverage their influence over regulation and governance in other countries to secure more access to critical input data.[77] Yet if AI is indeed a paradigm-shifting technology, the course of geopolitical competition in the domain will hinge on the relative strengths and weaknesses of the American, Chinese and European markets. National advantages will become even more important if political concerns drive further segmentation between the three national AI ecosystems.

Kai-Fu Lee perceives a transition underway from an age of AI invention to one of implementation that could benefit Chinese developers more than their international competitors. For Lee, the current focus of the AI industry is less about achieving new scientific breakthroughs as it is the application of existing technologies to produce new widgets and solutions.[78] The U.S. and other Western countries hosted the expertise that drove AI research in the past,[79] but China's large quantities of data, hyper-competitive entrepreneurial culture, beneficial policy environment and its abundance of competent AI engineers give it a leg up moving forward.[80]

Lee's argument is not without its critique. Zwetsloot, Toner and Ding insist that he oversimplifies and exaggerates the strengths of the Chinese ecosystem. They argue that the "implementation age" concept builds on the false assumption that deep learning will be the defining AI technology in the 21st century, even though this claim is in no way a consensus view among field experts. Deep learning itself is the product of lab-based refinement, and if this pattern holds, American-led research will still be a key source of value.[81] Furthermore, Anne-Marie Slaughter, CEO and President of New America, grants the U.S. a decisive advantage over China in the development of the human-centric AI Lee also deems essential, but its success is conditional on companies and

policymakers leveraging American diversity and national values like "individualism, openness, rebellion, and humanism" to produce new innovation.[82] The question remains whether these U.S strengths can outweigh China's surplus in one of the primary resources driving AI development.

As the fuel for algorithmic training, data is among the more critical components of the AI supply chain. Lee sees the Chinese ecosystem benefit from both data breadth and depth. The shear diversity of mobile services deployed in China, anchored by the WeChat application, draw rich maps of user habits that can refine deep learning algorithms to an extent beyond that achieved in Silicon Valley.[83] In contrast, Samm Sacks, Cybersecurity Policy and China Digital Economy Fellow at New America, submits that China's data advantage could be overplayed. The new standards on commercial use may limit the extent to which AI companies can apply their large data sets for training purposes. Furthermore, Sacks notes that the data gathered across Chinese platforms is culturally homogenous, sampling an almost exclusively domestic consumer base. Algorithms trained on these sets will not necessarily deploy well in export markets where user habits and preferences differ.[84] With a far more dispersive presence internationally, it is possible that American tech companies can better account for cultural and regional characteristics when developing AI products and services.

Notwithstanding Sacks' argument, Lee suspects that the differences between Chinese and American expansion strategies may help to nullify Silicon Valley's insight into foreign markets. Unlike U.S. tech companies that seek to export their own brands, Chinese companies invest in locally-grown firms and cultivate cooperative relationships through which they can leverage local data. In this regard, Chinese AI can take advantage of the "localization quotient" critical for input data, without incurring the costs of a full-fledged market presence.[85] It is unclear, however, to what extent this approach can compensate for the homogeneity problem.

Other dimensions of the American and Chinese AI ecosystems may endow one or the other competitor with relative advantages. While the US maintains a clear lead in business AI applications, particularly given its strength in financial services,[86] China's mass deployment of sensor technology helps it to excel at online-offline integration and lead in perception AI.[87] American companies also predominate the market for critical computing chips, although China is making significant investments in an effort to close the gap.[88] With world-leading academic institutions, investment and immigration, the U.S can better recruit world-class talent, [89] yet disparities in coordination and national culture may ultimately favour Beijing. Apart from the state's heavy involvement in China's AI industry, private companies often identify themselves as national champions that are subject to state oversight and direction. In comparison, American tech leaders in Silicon Valley do not self-identify with the U.S. government in the same way. They may recognize a loose affiliation with the U.S. system, but behave more as representatives of international companies accountable to their investors rather than to the state. Politics exacerbates the divide: Heavy opposition to the Trump Administration has left the tech sector somewhat estranged from Washington.[90] This disconnect could inhibit public-private cooperation critical to optimizing AI research and innovation.

Finally, given the increasing U.S.-China duopoly, the EU could remain a tertiary AI player along its current trajectory. European regulations like GDPR may stifle the capacity of European

companies to fully leverage deep learning.[91] With its focus on ethical AI development, however, Brussels may sacrifice the first-mover advantage in exchange for a less socially disruptive technology in the long term. An earlier focus on issues like explainability, algorithmic bias and negative externalities could help the EU develop better consumer AI applications while avoiding the problems of rushed deployment in the U.S. and China.[92]

5G

Technical Overview

An increasingly prevalent albeit cryptic term, "5G" refers to the fifth-generation of wireless telecommunications, the next step in a technological evolution from the basic mobile networks of the 1970s-80s to the 3G and 4G infrastructure supporting smartphone functionality.[93] 5G will provide both greater connectivity and reduced latency to mobile systems: it will allow more devices to communicate interchangeably, a foundation for the Internet of Things (IoT), while nearly eliminating the delay between the sending and receiving of digital information.[94] Mobile speeds are forecasted to clock up to 10 gigabytes per second, more than 600 times faster than existing 4G phone networks. In the United States, cellular carriers have committed to rolling out 5G by 2020, although it will likely take some time before the networks achieve their full capabilities.[95]

In its optimal state, 5G operates along "millimeter waves" on the high-frequency band of the radio spectrum (the range of wavelengths over which wireless signals can transmit). Millimeter waves do not travel as far as their equivalents across 4G networks, however, and are vulnerable to physical obstructions like trees. As a result, a full speed 5G system cannot rely on conventional cellular towers; it requires the mass deployment of additional access points.[96] These receivers or "base stations" constitute the "edge" of the system, connecting directly to individual mobile devices, while also linking to a "core" of computer systems that facilitate the network.[97] Equipment manufacturers play an important role in servicing the "backbone" components at the core, providing services like monitoring and updates through a "dedicated channel." Moreover, when it accesses the system, a supplier is not always detectible by network operators. It is these technical features that could advantage a nefarious actor looking to surveil wireless communications. [98]

Worries Over Huawei

The Chinese government has identified advanced telecommunications as an economic priority. The 13th Five Year Plan (2016-2020) labels 5G a "'strategic emerging industry,'" while Made in China 2025 commits to major breakthroughs in the technology. With the evolutionary changes underway, Beijing has an opportunity to seize a leadership position in the wireless sector, and in so doing, bolster its national prestige.[99] The CCP has helped to coordinate the network rollout thus far, through its controlling influence in the major cellular carriers.[100] National champions account for a significant proportion of global hardware sales: Huawei and ZTE are two of the four leading suppliers of 5G network equipment.[101] Chinese firms are at the forefront of intellectual property development in the 5G space, accounting for 34% of all major patent applications in the field.[102] Beijing is also actively seeking to shape international governance standards for 5G networks, which can give domestic firms an added advantage as they look to license their technologies in foreign markets.[103]

At first glance, the U.S. appears to lag behind its principal rival. American and European

companies stood at the vanguard of 3G and 4G innovation,[104] but the U.S. now lack a major presence in the market for 5G core equipment.[105] Nevertheless, its suppliers do still lead in the production of key underlying technologies upon which Chinese manufacturers rely, including semiconductors.[106] Government attention may also help to strengthen American competitiveness in the near term. The Trump Administration views the 5G network as critical to future economic prosperity and is taking action to facilitate innovation and bolster deployment. President Trump has framed the technology in the context of "a race America must win," and stressed that the American people "cannot allow any other country to outcompete the United States in this powerful industry of the future."[107] Unlike the Chinese approach, however, the U.S. plan assigns a supporting role to government in an otherwise private-sector initiative.[108] The Federal Communications Commission (FCC) launched a 5G Fast Plan in 2018, with three central objectives at its core: Expand the radio spectrum available for 5G signals, update infrastructure policy and modernize obsolete regulations.[109] In April 2019, the FCC supplemented the FAST plan with a third spectrum auction (set for December) and a $20.4 billion Rural Digital Opportunity Fund to expand connectivity in rural areas.[110]

On the other side of the Atlantic, the EU is home to major 5G equipment suppliers Ericsson and Nokia,[111] but lags behind the U.S., China and South Korea on infrastructure deployment.[112] As with AI, the rollout delays in Europe may yield some advantage in the long-term, however, as the EU corrects for the mistakes of first-mover competitors when building out its own network infrastructure.[113] Brussels has set forth an 8-step 5G Action Plan, calling for internal market coordination on a timetable for 5G rollout and new spectrum allocation, among other moves.[114]

The Pressure Mounts

The U.S. instigated the ongoing debate over 5G infrastructure with its response to Chinese multinationals operating in domestic and international markets. The dispute has pitted Congress and the Trump Administration against China's leading technology giants and divided American allies and partners. Washington labelled major Chinese telecoms a national security threat as early as 2012 when a House Intelligence Committee report singled out Huawei and ZTE for criticism.[115] Government agencies are now prohibited from sourcing equipment from either company under Section 889 of the National Defense Authorization Act.[116] The American response to the conduct of Chinese telecom companies has even risen to the level of direct legal action. On January 28, 2019, the U.S. Department of Justice (DOJ) announced charges against Huawei and affiliates for offences relating to fraud, money laundering, obstruction of justice and violations of the International Emergency Economic Powers Act (IEEPA)[117] imposing American sanctions against Iran.[118] Previously, at Washington's request, Canadian authorities had arrested Huawei's CFO Meng Wanzhou at Vancouver Airport in December 2018 for possible extradition.[119] The DOJ has charged her "with bank fraud, wire fraud, and conspiracy to commit bank and wire fraud,"[120] while Ottawa grapples with a diplomatic fallout over the case.[121] Legal measures have been taken against Canadian citizens,[122] and Beijing has blocked certain canola imports on what are officially health and safety grounds, although onlookers suspect that the ban is a form of retaliation for the Meng case.[123] As some measure of support, the U.S. Senate passed a formal, albeit non-binding resolution backing the Canadian government.[124]

Apart from the legal indictments against the company, its affiliates and CFO, opposition to Huawei is not necessarily informed by specific

cases of surveillance as much as from the company's suspected relationship with the Chinese state.[125] Under the leadership of Xi Jinping, the CCP has markedly increased its influence in the economy, where internal Party committees have a more assertive role in corporate decision-making.[126] This kind of state intervention in the private-sector feeds concern outside of China that private business cannot resist CCP influence.[127] As referenced previously, the Cyber Security Law mandates that the private-sector "provide technical support and assistance" to state security authorities.[128] Chinese national security exceptions are not without analogues in other countries, including the U.S. However, the U.S. judiciary still subjects the state to a far more rigorous legal process than its Chinese counterpart before the government can gain access to private information.[129]

Huawei Founder/CEO Ren Zhengfei rejected accusations that his company is a threat to the national security of the foreign states in which it operates. He also confirmed that Huawei has never provided data to the Chinese government in the past, and that he would not hand over said information to the state, even if a request was ever made.[130] These claims have failed to convince many international security observers, who maintain that Huawei would have little option but to concede to an information request from Beijing.[131] The Trump Administration has campaigned for allies and partners to follow suit with its own policy and limit Huawei's participation in their 5G networks; a request that both Australia and Japan took steps to fulfil in 2018.[132] For those states that choose to pursue the opposite course, however, Washington has forewarned that the decision could compromise their defence relationship with the U.S. In February 2019, Secretary of State Mike Pompeo confirmed that the American security apparatus will not cooperate and exchange information with partners that incorporate Huawei equipment into their "critical information systems."[133]

In an interview for *BBC News*, Ren iterated Huawei's business strategy in view of U.S. efforts to limit its global customer base, stating that "If the lights go out in the West, the East will still shine, and if the North goes dark, then there is still the South. America doesn't represent the world."[134] To wit, performance indicators suggest that American interventions could have only a moderate effect on the company's bottom line. Huawei reported an almost $9 billion record profit for 2018, with the Chinese domestic market alone accounting for approximately 50% of all sales.[135] 45 of the world's 50 largest mobile carriers are Huawei customers,[136] and the company controls approximately 40% of the European market for telecom equipment.[137] Most telling, some key U.S. allies have hesitated or even refused to shut off their 5G networks carte blanche to Chinese imports. New Zealand seemingly reversed its initial decision to ban Huawei in February 2019 when Prime Minister Jacinda Ardern entertained a future collaboration with Spark, a national mobile carrier, subject to approval from the Government Communications Security Bureau.[138] German officials have indicated that their telecom market will remain open to Huawei if it complies with applicable security regulations,[139] and the UK government is reportedly set to open up the edge of its 5G network while blocking access to the system core.[140] In Canada, the Trudeau government has yet to make a decision on Huawei's status for 5G roll-out, and it may not release any final ruling until after the upcoming general election in October.[141] Altogether, this pushback against the U.S. campaign may reflect the opportunity cost of a blanket ban. As James A. Lewis of the Center for Strategic and International Studies (CSIS) observes, Huawei attracts market interest because it can deliver high quality technologies at a subsidized cost.[142]

Thus, as with data governance, the geopolitics of 5G manifest both at home and in global export markets. American, Chinese and European lawmakers can take prohibitive measures to block entry in their own networks on national security grounds, or they can encourage foreign governments to erect analogous barriers that either facilitate or inhibit trade in 5G technologies.

Risk Appraisal

Regulatory Risk

As internet governance thickens, the worldwide web could segment into a collection of independent digital ecosystems or "splinternets." This emerging model could be attractive to states and businesses that seek to exert greater market control in cyberspace and exclude foreign competition. It could also threaten to disrupt multinational tech firms that operate in different fragments of a once free and open internet, and for which the maintenance of legal compliance across jurisdictions becomes immensely challenging.[143]

In a splinternet age, companies will face regulatory risk as they grapple with competing technology governance regimes. Although North America currently takes a more liberal approach, competing jurisdictions that opt for even stricter rules could create significant challenges for cross-border commerce. Some authorities like the EU could enforce hard restrictions on corporate data use to protect consumer rights, while others like China will expect greater state access and control. As regulatory disparities increase, companies that collect and transfer data will have to adapt country-specific best practices for privacy protection and construct independent storage and management facilities at the cost of fully optimizing their systems architecture. Financial services rank among the sectors with the greatest exposure to the splinternet. Commercial and retail lenders, insurers and investors are heavily data dependent and rely on low barriers to exchange across a globalized financial system. As alluded to by Victoria Espinel, President and CEO of Software Alliance (an industry lobby group), it is much harder for a bank to deliver products and services beyond its local market when national storage requirements constrain global data flows. Furthermore, Espinel identifies "interoperability" in privacy standards as a key goal for data-based companies, where national regulations can differ in some respects as long as they still work in tandem.[144] It follows then that financial institutions will find it challenging to remain legally compliant when data governance standards polarize along national lines and grow to directly contradict each other. In financial services, this dilemma is further complicated by unique industry conditions: some countries may subject financial data to more stringent regulation than other varieties given its sensitivity.

As a corollary, the splinternet poses a secondary risk to corporate reputation. Companies that violate their legal obligations can lose the trust of regulators and face increased scrutiny and oversight. Furthermore, if an institution fails to meet consumer expectations, particularly around privacy and security, the public backlash can be severe. The Cambridge Analytica scandal that rocked Facebook in 2018 is a case study for the reputational damage that poor data governance can inflict. In a segmented cyberspace, where both consumer cultures and regulatory regimes are non-aligned, a financial institution could share a similar fate if it fails to manage its data accordingly.

Macroeconomic Risk

The global economy could soon enter a phase in which the competitive dimensions of AI, 5G and Big Data stifle international cooperation on the research and deployment of cutting-edge

innovation; a scenario that the political risk consultancy Eurasia Group describes as an "Innovation Winter."[145] The U.S., EU and China exhibit early signs of this technological protectionism. In Washington, the Foreign Investment Risk Review Modernization Act (passed 2018) granted new powers to the Committee on Foreign Investment in the United States (CFIUS), a federal body responsible for conducting security reviews of foreign transactions with American companies, evidently as a response in part to predatory Chinese investment practices.[146] To protect against potential espionage and IP theft, the Trump Administration is also considering new vetting procedures for Chinese nationals studying in the U.S., and the State Department has already decreased the VISA limit from 5-years to 1-year for Chinese graduate students in certain key technology fields.[147] Similar to CFIUS, the European Parliament has created a new mechanism to assess foreign direct investment in the Common Market, applying to interventions "in critical sectors and technologies made by opaque, state-owned companies with government ties."[148] Finally, China has increased barriers to foreign investment with limits on capital flows and forced technology transfers,[149] although a new Foreign Investment Law may begin to reverse this trend.[150]

All of these prohibitive measures can amount to trade barriers as much as conventional tariffs or duties, segmenting supply chains, limiting human capital flows, increasing production costs, and shrinking profit margins. The long-term macroeconomic costs of such retrenchment could be significant, weakening future growth in technology industries and increasing market and credit risk for financial institutions.

Conclusion

Schumpeterian leaps are often a two-edged sword: at once nourishment for growth and the catalyst for antagonism. Much like the hydrogen rockets that lifted humankind to the stars while propelling the Space Race, big data, AI and 5G may yield newfound prosperity while sowing great power competition. Risk managers should monitor the geopolitical dimensions of these innovations and stand ready to meet the obstacles that arise. Only then can financial services safely explore the opening vistas of a new technological age.

Endnotes

[1] John F. Kennedy, Address At Rice University On The Nation's Space Effort, *John F. Kennedy Presidential Library and Museum*, Video, 18:27, September 12, 1962, https://www.jfklibrary.org/learn/about-jfk/historic-speeches/address-at-rice-university-on-the-nations-space-effort.
[2] Douglas Brinkley, moderated by Fredrik Logevall, *American Moonshot: John F. Kennedy And The Great Space Race*, YouTube Video, 1:29:29, April 4, 2019, https://www.youtube.com/watch?v=_Dbwx_SMzbM.
[3] Kennedy, Address At Rice University On The Nation's Space Effort.
[4] Ibid.
[5] James McBride and Andrew Chatzky, "Is 'Made In China 2025' A Threat To Global Trade?" *Council on Foreign Relations (CFR)*, last modified May 13, 2019, accessed May 14, 2019, https://www.cfr.org/backgrounder/made-china-2025-threat-global-trade.
[6] "National Security Strategy Of The United States Of America," *The White House* (December 2017): 25, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905-2.pdf.
[7] "EU-China – A Strategic Outlook," *European Commission* (March 12, 2019): 1, https://ec.europa.eu/commission/sites/beta-political/files/communication-eu-china-a-strategic-outlook.pdf.
[8] As argued by Zhang Baohui, Lingnan University: Bloomberg News, "In New Trump Tariffs, China Sees Master Plan To Thwart Its Rise," *Bloomberg*, last modified September 18, 2018, https://www.bloomberg.com/news/articles/2018-09-18/in-new-trump-tariffs-china-sees-master-plan-to-thwart-its-rise.
[9] "What Is Big Data?" *Oracle*, accessed April 29, 2019, https://www.oracle.com/ca-en/big-data/guide/what-is-big-data.html.
[10] Nandan Nilekani, "Data To The People: India's Inclusive Internet," *Foreign Affairs*, September/October 2018, https://www.foreignaffairs.com/articles/asia/2018-08-13/data-people.
[11] Dawn E. Holmes, *Big Data: A Very Short Introduction* (Oxford, UK and New York: Oxford University Press, 2017), 15-16.
[12] Ibid., 17.
[13] Ibid., 5-6.
[14] Ibid., 17-19.
[15] Kieron O'Hara and Wendy Hall, "Four Internets: The Geopolitics Of Digital Governance," *Centre For International Governance Innovation CIGI Papers No. 206* (December 2018): 1, 6, https://www.cigionline.org/sites/default/files/documents/Paper%20no.206web.pdf.
[16] Ibid., 1.
[17] Ibid., 6-8.
[18] Ibid., 1, 8-9.
[19] Nuala O'Connor, "Reforming The U.S. Approach To Data Protection And Privacy," *Council on Foreign Relations (CFR)*, January 30, 2018, https://www.cfr.org/report/reforming-us-approach-data-protection.
[20] Larry Downes, "The Business Implications Of The EU-U.S. 'Privacy Shield,'" *Harvard Business Review*, February 10, 2016, https://hbr.org/2016/02/the-business-implications-of-the-eu-u-s-privacy-shield.
[21] Larry Downes, "GDPR And The End Of The Internet's Grand Bargain," *Harvard Business Review*, last modified April 9, 2018, accessed May 3, 2019, https://hbr.org/2018/04/gdpr-and-the-end-of-the-internets-grand-bargain.
[22] Heather Kelly, "California Passes Strictest Online Privacy Law In The Country," *CNN Business*, June 29, 2018, https://money.cnn.com/2018/06/28/technology/california-consumer-privacy-act/index.html.
[23] Issie Lapowsky, "Get Ready For A Privacy Showdown in 2019," *Wired*, December 27, 2018, https://www.wired.com/story/privacy-law-showdown-congress-2019/.
[24] As argued, O'Connor, "Reforming The U.S. Approach To Data Protection And Privacy."
[25] Alan Beattie, "Data Protectionism: The Growing Menace To Global Business," *Financial Times*, May 13, 2018, https://www.ft.com/content/6f0f41e4-47de-11e8-8ee8-cae73aab7ccb.

[26] William Alan Reinsch, "A Data Localization Free-For-All?" *Center For Strategic And International Studies (CSIS)*, March 9, 2018, https://www.csis.org/blogs/future-digital-trade-policy-and-role-us-and-uk/data-localization-free-all#_ednref6.
[27] Beattie, "Data Protectionism: The Growing Menace To Global Business."
[28] Adam Segal, "When China Rules The Web: Technology In Service Of The State," *Foreign Affairs*, September/October 2018, https://www.foreignaffairs.com/articles/china/2018-08-13/when-china-rules-web.
[29] Ibid.
[30] Rogier Creemers, Paul Triolo and Graham Webster, "Translation: Cybersecurity Law Of The People's Republic Of China [Effective June 1 2017]," *New America*, June 29, 2018, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/.
[31] Samm Sacks, "China's Privacy Conundrum," *New America*, February 14, 2019, https://www.newamerica.org/weekly/edition-236/chinas-privacy-conundrum/.
[32] Samm Sacks, "China's Emerging Data Privacy System And GDPR," *Center for Strategic and International Studies (CSIS)*, March 9, 2018, https://www.csis.org/analysis/chinas-emerging-data-privacy-system-and-gdpr.
[33] "A New Era For Data Protection In The EU: What Changes After May 2018," *European Commission*, accessed April 30, 2019, https://ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-changes_en.pdf.
[34] Helen Dixon, "Regulate To Liberate: Can Europe Save The Internet?" *Foreign Affairs*, September/October 2018, https://www.foreignaffairs.com/articles/europe/2018-08-13/regulate-liberate.
[35] Refer to General Data Protection Regulation (GDPR) text: "Regulation (EU) 2016/679 Of The European Parliament And Of The Council Of 27 April 2016," *Official Journal of the European Union*, (May 4, 2016): 61, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN.
[36] Chris Fox, "Google Hit With £44m GDPR Fine Over Ads," *BBC News*, January 21, 2019, https://www.bbc.com/news/technology-46944696.
[37] Charles Riley and Ivana Kottasová, "Europe Hits Google With A Third, $1.7 Billion Antirust Fine," *CNN Business*, last modified March 20, 2019, accessed May 6, 2019, https://www.cnn.com/2019/03/20/tech/google-eu-antitrust/index.html.
[38] Mark Bergen, "Google In China: When 'Don't Be Evil' Met The Great Firewall," *Bloomberg Businessweek*, November 8, 2018, https://www.bloomberg.com/news/features/2018-11-08/google-never-stopped-trying-to-go-to-china.
[39] Beattie, "Data Protectionism: The Growing Menace To Global Business."
[40] "Chapter 19: Digital Trade," *United States Office of the Trade Representative (USTR)*: 6, https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/Text/19_Digital_Trade.pdf.
[41] "Chapter 17: Financial Services," *United States Office of the Trade Representative (USTR)*: 15-16, https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/Text/17_Financial_Services.pdf.
[42] Stewart M. Patrick and Ashley Feng, "Belt and Router: China Aims For Tighter Internet Controls With Digital Silk Road," *Council on Foreign Relations*, July 2, 2018, https://www.cfr.org/blog/belt-and-router-china-aims-tighter-internet-controls-digital-silk-road.
[43] Ibid.
[44] Samm Sacks, "Beijing Wants To Rewrite The Rules Of The Internet," *The Atlantic*, June 18, 2018, https://www.theatlantic.com/international/archive/2018/06/zte-huawei-china-trump-trade-cyber/563033/.
[45] Segal, "When China Rules The Web: Technology In Service Of The State."
[46] Refer to Mark Scott and Lauren Cerulus, "Europe's New Data Protection Rules Export Privacy Standards Worldwide," *Politico*, last modified February 6, 2018, accessed May 6, 2019, https://www.politico.eu/article/europe-data-protection-privacy-standards-gdpr-general-protection-data-regulation/.
[47] Refer to Nitasha Tiku, "Europe's New Privacy Law Will Change The Web, And More," *Wired*, March 19, 2018, https://www.wired.com/story/europes-new-privacy-law-will-change-the-web-and-more/.
[48] Alex LaPlante, "Ethics & Artificial Intelligence In Finance," *Global Risk Institute (GRI)* (April 1, 2019): 1, https://globalriskinstitute.org/publications/ethics-artificial-intelligence-in-finance/.
[49] Kai-Fu Lee, *AI Superpowers: China, Silicon Valley, And The New World Order* (Boston and New York: Houghton Mifflin Harcourt, 2018), 7-10.

[50] Mike Durland and Matthew Killi, "AI Frontiers: Where We Are Today And The Risks And Benefits Of An AI Enabled Future," *Global Risk Institute (GRI)* (March 7, 2017): 4, https://globalriskinstitute.org/publications/ai-frontiers-today-risks-benefits-ai-enabled-future/.
[51] LaPlante, "Ethics & Artificial Intelligence In Finance," 2.
[52] Durland and Killi, "AI Frontiers: Where We Are Today And The Risks And Benefits Of An AI Enabled Future," 2.
[53] Lee, *AI Superpowers: China, Silicon Valley, And The New World Order*, 107.
[54] Ibid., 110-111.
[55] Ibid., 117-118.
[56] Ibid., 128-129.
[57] LaPlante, "Ethics & Artificial Intelligence In Finance," 3.
[58] Durland and Killi, "AI Frontiers: Where We Are Today And The Risks And Benefits Of An AI Enabled Future," 4-5.
[59] Lee, *AI Superpowers: China, Silicon Valley, And The New World Order*, 140-143.
[60] Ibid., 1-4.
[61] Refer to Elsa Kania, "China's AI Agenda Advances," *The Diplomat*, February 14, 2018, https://thediplomat.com/2018/02/chinas-ai-agenda-advances/.
[62] Graham Webster, Rogier Creemers, Paul Triolo and Elsa Kania, "Full Translation: China's 'New Generation Artificial Intelligence Development Plan' [2017]," *New America*, August 1, 2017, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017/.
[63] Elsa Kania, "China's Artificial Intelligence Revolution," *The Diplomat*, July 27, 2017, https://thediplomat.com/2017/07/chinas-artificial-intelligence-revolution/.
[64] Webster, Creemers, Triolo and Kania, "Full Translation: China's 'New Generation Artificial Intelligence Development Plan' [2017]."
[65] Ibid.
[66] Lee, *AI Superpowers: China, Silicon Valley, And The New World Order*, 98.
[67] Refer to Ibid., 97-98.
[68] "Executive Order On Maintaining American Leadership In Artificial Intelligence," *The White House*, February 11, 2019, https://www.whitehouse.gov/presidential-actions/executive-order-maintaining-american-leadership-artificial-intelligence/.
[69] "Accelerating America's Leadership In Artificial Intelligence," *The White House*, February 11, 2019, https://www.whitehouse.gov/articles/accelerating-americas-leadership-in-artificial-intelligence/.
[70] Michael Kratsios, "Why The US Needs A Strategy For AI," *Wired*, February 11, 2019, https://www.wired.com/story/a-national-strategy-for-ai/.
[71] "Communication from The Commission To The European Parliament, The European Council, The Council, The European Economic And Social Committee And The Committee Of The Regions: Artificial Intelligence For Europe," *European Commission* (April 25, 2018): 3 (Cover Page Not Counted), https://ec.europa.eu/digital-single-market/en/news/communication-artificial-intelligence-europe?utm_source=POLITICO.EU&utm_campaign=fb25ba8e0f-EMAIL_CAMPAIGN_2018_04_25&utm_medium=email&utm_term=0_10959edeb5-fb25ba8e0f-189775021.
[72] "Communication From The Commission To The European Parliament, The European Council, The Council, The European Economic And Social Committee And The Committee Of The Regions: Coordinated Plan On Artificial Intelligence," *European Commission* (December 7, 2018): 8, https://ec.europa.eu/digital-single-market/en/news/coordinated-plan-artificial-intelligence.
[73] "Communication from The Commission To The European Parliament, The European Council, The Council, The European Economic And Social Committee And The Committee Of The Regions: Artificial Intelligence For Europe," *European Commission*, 5-16 (Cover Page Not Counted).
[74] Ibid., 17 (Cover Page Not Counted).
[75] Mathieu Rosemain and Michel Rose, "France To Spend $1.8 Billion On AI To Compete With U.S., China," *Reuters*, March 29, 2018, https://uk.reuters.com/article/us-france-tech/france-to-spend-1-8-billion-on-ai-to-compete-with-u-s-china-idUKKBN1H51XP.

[76] Janosch Delcker, "Germany's €3B Plan To Become An AI Powerhouse," *Politico*, last modified April 19, 2019, accessed May 14, 2019, https://www.politico.eu/article/germanys-plan-to-become-an-ai-powerhouse/.
[77] For more on the AI segmentation argument, refer to Nicholas Thompson and Ian Bremmer, "The AI Cold War That Threatens Us All," *WIRED Magazine*, October 23, 2018, https://www.wired.com/story/ai-cold-war-china-could-doom-us-all/.
[78] Lee, *AI Superpowers: China, Silicon Valley, And The New World Order*, 12-14.
[79] Ibid., 11-12.
[80] Ibid., 13-19, 82-84.
[81] Remco Zwetsloot, Helen Toner and Jeffrey Ding, "Beyond The AI Arms Race," *Foreign Affairs*, November 16, 2018, https://www.foreignaffairs.com/reviews/review-essay/2018-11-16/beyond-ai-arms-race.
[82] Anne-Marie Slaughter, "What Will Really Determine The Winner Of The U.S.-China Rivalry Over A.I.?," *Slate*, March 12, 2019, https://slate.com/technology/2019/03/united-states-china-rivalry-artificial-intelligence.html.
[83] Lee, *AI Superpowers: China, Silicon Valley, And The New World Order*, 16-17.
[84] Samm Sacks and Jim Lindsay, "The Global Artificial Intelligence Race With Samm Stacks," February 19, 2019, in *The President's Inbox*, produced by the Council on Foreign Relations (CFR), podcast, MP3 audio, 23:44, accessed February 22, 2019, https://www.cfr.org/podcasts/global-artificial-intelligence-race-samm-sacks.
[85] Lee, *AI Superpowers: China, Silicon Valley, And The New World Order*, 136-138.
[86] Ibid., 111-112.
[87] Ibid., 124-128.
[88] Ibid., 96-97.
[89] Ryan Hass and Zach Balin, "US-China Relations In The Age Of Artificial Intelligence," *Brookings*, January 10, 2019, https://www.brookings.edu/research/us-china-relations-in-the-age-of-artificial-intelligence/.
[90] As argued by Thompson and Bremmer: Refer to Nicholas Thompson and Ian Bremmer, *The AI Cold War That Threatens Us All: Nicholas Thompson and Ian Bremmer Discuss The Risks*, YouTube Video, 23:38, November 1, 2018, https://www.youtube.com/watch?v=W7hkFpS5HhY.
[91] Alluded to by Kai-Fu Lee, Speaker, moderated by Deven J. Parekh, *The Artificial Intelligence Race And The New World Order*, YouTube Video, 58:49, October 5, 2018, https://www.youtube.com/watch?v=bh0TXtB0NxU.
[92] For more on European AI ethics, refer to "High-Level Expert Group On Artificial Intelligence: Ethics Guidelines For Trustworthy AI," *European Commission*, April 8, 2019, https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai.
[93] Klint Finley, "The Wired Guide To 5G," *Wired*, December 13, 2018, https://www.wired.com/story/wired-guide-5g/.
[94] "What Is 5G?" *Government of Canada*, last modified July 20, 2017, accessed May 15, 2019, http://www.crc.gc.ca/eic/site/069.nsf/eng/00077.html.
[95] Finley, "The Wired Guide To 5G."
[96] Ibid.
[97] James Andrew Lewis, "5G: To Ban Or Not To Ban? It's Not Black Or White," *Center for Strategic and International Studies (CSIS)*, April 24, 2019, https://www.csis.org/analysis/5g-ban-or-not-ban-its-not-black-or-white.
[98] James A. Lewis, "How 5G Will Shape Innovation And Security: A Primer," *Center for Strategic and International Studies (CSIS)* (December 2018): 9, https://csis-prod.s3.amazonaws.com/s3fs-public/publication/181206_Lewis_5GPrimer_WEB.pdf.
[99] Elizabeth Woyke, "China Is Racing Ahead In 5G. Here's What That Means," *MIT Technology Review*, December 18, 2018, https://www.technologyreview.com/s/612617/china-is-racing-ahead-in-5g-heres-what-it-means/.
[100] Ibid.
[101] James A. Lewis, "How 5G Will Shape Innovation And Security: A Primer," 5.
[102] Akito Tanaka, "China In Pole Position For 5G Era With A Third of Key Patents," *Nikkei Asian Review*, May 3, 2019, https://asia.nikkei.com/Spotlight/5G-networks/China-in-pole-position-for-5G-era-with-a-third-of-key-patents.
[103] Mark Scott, "Telcogeopolitics: West vs. China In 5G Race," *Politico*, last modified April, 19, 2019, accessed May 15, 2019, https://www.politico.eu/article/5g-telecommunications-infrastructure-china-us-eu-qualcomm-nokia-ericsson-huawei/.
[104] Tanaka, "China In Pole Position For 5G Era With A Third of Key Patents."

[105] Lewis, "How 5G Will Shape Innovation And Security: A Primer," 5.
[106] Ibid., 6.
[107] *Trump Says U.S. "Wants To Be The Leader" in 5G Deployment*, YouTube Video, 28:31, April 12, 2019, https://www.youtube.com/watch?v=o_Gakw0dPvE.
[108] Refer to Ibid.
[109] "The FCC's 5G FAST Plan," *Federal Communications Commission (FCC)*, September 28, 2018, https://docs.fcc.gov/public/attachments/DOC-354326A1.pdf.
[110] Trump and Pai, Trump Says U.S. "Wants To Be The Leader" in 5G Deployment."
[111] James A. Lewis, "How 5G Will Shape Innovation And Security: A Primer," 5.
[112] Mark Scott, "Mobile World Congress To Show Why Europe Is The World's 5G Laggard," *Politico*, last modified February 27, 2018, accessed April 5, 2019, https://www.politico.eu/article/mobile-world-congress-mwc-5g-europe-china-us-telecommunications-network/.
[113] Ibid.
[114] "Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions – 5G for Europe: An Action Plan," *European Commission* (2016): 4-10, https://ec.europa.eu/digital-single-market/en/news/communication-5g-europe-action-plan-and-accompanying-staff-working-document.
[115] Arjun Kharpal, "Here's Which Leading Countries Have Barred, And Welcomed, Huawei's 5G Technology," *CNBC*, April 25, 2019, https://www.cnbc.com/2019/04/26/huawei-5g-how-countries-view-the-chinese-tech-giant.html.
[116] "H.R.5515 – John S. McCain National Defense Authorization Act For Fiscal Year 2019," *Congress.Gov*, accessed May 8, 2019, https://www.congress.gov/bill/115th-congress/house-bill/5515/text.
[117] "Chinese Telecommunications Conglomerate Huawei And Huawei CFO Wanzhou Meng Charged With Financial Fraud," *United States Department of Justice – The United States Attorney's Office Eastern District of New York*, Monday January 28, 2019, https://www.justice.gov/usao-edny/pr/chinese-telecommunications-conglomerate-huawei-and-huawei-cfo-wanzhou-meng-charged.
[118] "Executive Order Reimposing Certain Sanctions With Respect To Iran," *The White House*, August 6, 2018, https://www.whitehouse.gov/presidential-actions/executive-order-reimposing-certain-sanctions-respect-iran/.
[119] "Huawei's Meng Wanzhou Sues Canada Authorities Over Arrest," *BBC News*, March 4, 2019, https://www.bbc.com/news/world-us-canada-47436497.
[120] "Chinese Telecommunications Conglomerate Huawei And Huawei CFO Wanzhou Meng Charged With Financial Fraud," *United States Department of Justice – The United States Attorney's Office Eastern District of New York*.
[121] Refer to Ben Blanchard and David Ljunggren, "China Warns Of Severe Consequences If Canada Does Not Release Huawei CFO," *Global News*, last modified December 8, 2018, accessed June 10, 2019, https://globalnews.ca/news/4743451/china-consequences-canada-release-huawei-cfo/.
[122] Refer to Jason Proctor, "'Poor Canada': Will Meng Wanzhou Extradition Hearing Threaten National Interest?" *CBC News*, last modified May 3, 2019, accessed June 10, 2019, https://www.cbc.ca/news/canada/british-columbia/meng-wanzhou-extradition-chinese-huawei-1.5089840.
[123] Saša Petricic, "Canadian Canola Spat Shows China Has 'Ways Of Hurting' Trade Partners For Political Ends," *CBC News*, last modified April 12, 2019, accessed May 13, 2019, https://www.cbc.ca/news/world/canadian-canola-spat-shows-china-has-ways-of-hurting-trade-partners-for-political-ends-1.5095600.
[124] Peter Zimonjic, "U.S. Senate Passes Resolution Commending Canada For Its Actions In Huawei Case," *CBC News*, last modified May 8, 2019, accessed May 13, 2019, https://www.cbc.ca/news/politics/meng-senate-resolution-charter-1.5128399.
[125] Robert Williams, "Is Huawei A Pawn In The Trade War?: The Politics Of The Global Tech Race," *Foreign Affairs*, January 30, 2019, https://www.foreignaffairs.com/articles/china/2019-01-30/huawei-pawn-trade-war.
[126] Elizabeth C. Economy, "China's New Revolution: The Reign Of Xi Jinping," *Foreign Affairs*, May/June 2018, https://www.foreignaffairs.com/articles/china/2018-04-17/chinas-new-revolution.
[127] Elizabeth C. Economy, "The Problem With Xi's China Model: Why Its Successes Are Becoming Liabilities," *Foreign Affairs*, March 6, 2019, https://www.foreignaffairs.com/articles/china/2019-03-06/problem-xis-china-model.
[128] Creemers, Triolo and Webster, "Translation: Cybersecurity Law Of The People's Republic Of China [Effective June 1 2017]."

[129] Williams, "Is Huawei A Pawn In The Trade War?: The Politics Of The Global Tech Race."
[130] Arjun Kharpal, "Huawei CEO: No Matter My Communist Party Ties, I'll 'Definitely' Refuse If Beijing Wants Our Customers' Data," *CNBC*, last modified January 16, 2019, accessed May 6, 2019, https://www.cnbc.com/2019/01/15/huawei-ceo-we-would-refuse-a-chinese-government-request-for-user-data.html.
[131] Arjun Kharpal, "Huawei Says It Would Never Hand Data To China's Government. Experts Say It Wouldn't Have A Choice," *CNBC*, last modified March 5, 2019, accessed May 6, 2019, https://www.cnbc.com/2019/03/05/huawei-would-have-to-give-data-to-china-government-if-asked-experts.html.
[132] Kharpal, "Here's Which Leading Countries Have Barred, And Welcomed, Huawei's 5G Technology."
[133] "U.S. Won't Partner With Countries That Use Huawei Systems: Pompeo," *Reuters*, February 21, 2019, https://www.reuters.com/article/us-huawei-tech-usa-pompeo/us-wont-partner-with-countries-that-use-huawei-systems-pompeo-idUSKCN1QA1O6.
[134] By translation, refer to Ren Zhengfei, *Huawei Founder: 'America Doesn't Represent The World'*, YouTube Video, 2:50, February 19, 2019, https://www.youtube.com/watch?v=ju1epxXUPkQ.
[135] Yuan Yang, "Huawei Reports Record Profits Despite US Battle Over Chinese Spying Claims," *FT Weekend (US Edition)*, March 30/31 2019.
[136] Fred Kempe, "The Battle Over 5G And Huawei Is The Biggest Test Yet For Trump's Approach For China," *CNBC*, last modified February 23, 2019, accessed May 1, 2019, https://www.cnbc.com/2019/02/23/fred-kempe-battle-over-5g-huawei-is-the-biggest-test-yet-for-trumps-approach-for-china.html.
[137] Sherisse Pham, "The US Is Stepping Up Pressure On Europe To Ditch Huawei," *CNN Business*, last modified February 12, 2019, accessed May 5, 2019, https://www.cnn.com/2019/02/11/tech/huawei-mike-pompeo-hungary/index.html.
[138] Tracy Withers, "New Zealand Says China's Huawei Hasn't Been Ruled Out of 5G," *Bloomberg*, last modified February 18, 2019, accessed May 1, 2019, https://www.bloomberg.com/news/articles/2019-02-18/new-zealand-says-china-s-huawei-hasn-t-been-ruled-out-of-5g-role.
[139] Tobias Buck, "German Regulator Says Huawei Can Stay In 5G Race," *Financial Times*, April 14, 2019, https://www.ft.com/content/a7f5eba4-5d02-11e9-9dde-7aedca0a081a.
[140] James Andrew Lewis, "5G: To Ban Or Not To Ban? It's Not Black Or White."
[141] Josh Wingrove, "Canada Said To Put Huawei 5G Decision On Back Burner With Allies Split," *BNN Bloomberg*, May 8, 2019, https://www.bnnbloomberg.ca/canada-puts-huawei-5g-decision-on-back-burner-with-allies-split-1.1255833.
[142] James A. Lewis, "How 5G Will Shape Innovation And Security: A Primer," 10.
[143] Amy Webb, "Yes, The Splinternet Is A Thing. Here's Why You Should Care," *Inc.*, July/August 2018, https://www.inc.com/magazine/201808/amy-webb/splinternet-pitfalls.html.
[144] Scott Miller, William Alan Reinsch, Victoria Espinel and H. Andrew Schwartz, "Digital Trade With Victoria Espinel Of BSA l The Software Alliance," April 18, 2019, in *The Trade Guys*, produced by the Centre for Strategic and International Studies (CSIS), podcast, MP_3 audio, 37:52, accessed April 18, 2019, https://www.csis.org/podcasts/trade-guys.
[145] David Tweed, "What Could Go Wrong In 2019? Eurasia Group Outlines The Risks," *BNN Bloomberg*, January 7, 2019, https://www.bnnbloomberg.ca/what-could-go-wrong-in-2019-eurasia-group-outlines-the-risks-1.1194200.
[146] Jonathan Masters and James McBride, "Foreign Investment And U.S. National Security," *Council on Foreign Relations (CFR)*, last modified August 28, 2018, accessed May 8, 2019, https://www.cfr.org/backgrounder/foreign-investment-and-us-national-security.
[147] Patricia Zengerle and Matt Spetalnick, "Exclusive: Fearing Espionage, U.S. Weighs Tighter Rules On Chinese Students," *Reuters*, November 29, 2018, https://www.reuters.com/article/us-usa-china-students-exclusive/exclusive-fearing-espionage-us-weighs-tighter-rules-on-chinese-students-idUSKCN1NY1HE.
[148] "EU To Scrutinise Foreign Direct Investment More Closely," *European Parliament*, February 14, 2019, http://www.europarl.europa.eu/news/en/press-room/20190207IPR25209/eu-to-scrutinise-foreign-direct-investment-more-closely.
[149] Elizabeth C. Economy, *The Third Revolution: Xi Jinping and the New Chinese State* (Oxford, UK and New York: Oxford University Press, 2018), 232.

[150] Refer to Dongwoo Kim and Isaac Lo, "What Is China's New Foreign Investment Law And What Does It Mean For Canada And The Global Economy?" *Asia Pacific Foundation of Canada*, April 9, 2019, https://www.asiapacific.ca/blog/what-chinas-new-foreign-investment-law-and-what-does-it-mean.