

A U.S. Grand Strategy for the Global Digital Economy

ROBERT D. ATKINSON | JANUARY 2021

For America to remain the global leader in IT, the U.S. government must formulate a grand strategy grounded in a new doctrine of “digital realpolitik.” The first priority should be advancing U.S. interests by spreading the U.S. digital innovation policy system and constraining digital adversaries, especially China. This will entail working with allies when possible—and pressuring them when necessary.

- U.S. IT and digital policy needs to be guided by a grand, overall strategy, focused first and foremost on maintaining U.S. global tech leadership.
- The United States faces a risk where much of the world, including the EU, could align against U.S. IT and digital interests, leading to a many-against-one environment, with detrimental consequences.
- In efforts to reestablish closer relations with the EU, the United States should not “give away the store” by allowing the EU to go forward with its increasingly aggressive technology mercantilism.
- The United States must enlist likeminded nations in a variety of ways to support U.S. interests—and it should not be reluctant to exert pressure to encourage these nations to come along.
- The overarching goal of U.S. strategy should be to limit China’s global dominance and manipulation of markets in the IT and digital space.

CONTENTS

- Introduction..... 3
- Why National IT and Digital Leadership Is Important 6
- Where Do Nations Stand?..... 7
 - America Leads..... 7
 - China Responds, Mostly Succeeds, and Is Poised for Further Success..... 10
 - Europe Responds, But Largely Fails 13
 - Japan and the Four Asian Tigers Respond, and Partially Succeed..... 17
- Nation States Still Matter..... 19
- Major Centers of National Power in the Digital World 21
 - The United States: The Major Advocate for and Driver of Global IT and Digital Innovation and Progress..... 21
 - China: Seeking Global Hegemony Through Technology..... 22
 - Europe: Precaution and Protection..... 23
 - The “UNCTAD South”: The Oppressed Seeking “Digital Alms” 25
 - The Unaligned: Going Forward With Heads Down 28
 - The Disruptors: Russia and Other Digital Scofflaws..... 29
- Undesirable Scenarios 29
 - Scenario 1: EU “Regulatory Imperialism” Succeeds, and America Is Isolated..... 29
 - Scenario 2: Anti-tech Forces Turn America Into the EU and China Prevails..... 32
 - Scenario 3: The EU Won’t Budge..... 34
 - Scenario 4: Nations Craft a “Digital WTO” 35
 - Scenario 5: China Wins the Minds (if not the Hearts) of UNCTAD-Nations 37
 - Scenario 6: The Splinternet Emerges 38
 - Scenario 7: The United States Spends Much of Its Political Capital on Promoting the Open Global Internet 38
- An Action Agenda for Desirable Scenarios..... 39
 - Scenario 8: U.S., EU, and Non-aligned Nations Isolate, Punish, and Defend Against “Scofflaws” 40
 - Scenario 9: The United States Forms an Anglo-American (and Friends) Alliance 41
 - Scenario 10: EU, United States, and Non-aligned Nations Cooperate Against China 41
 - Scenario 11: The United States Approach Prevails in Developing Markets..... 44
- Principles for a New Realpolitik Doctrine in U.S. Global Digital Policy 45
 - Principle 1: Unabashedly Support IT and Digital Innovation, Rejecting the Techlash Narrative and Policies..... 45

Principle 2: Embrace IT and Digital “National Developmentalism” (Smart, Active Policies to Support IT Innovation and Adoption) and Bring More Nations Into That Orbit.....	46
Principle 3: Work to Limit China’s IT and Digital Progress, Especially When It Is Based on Innovation Mercantilism	48
Principle 4: Actively Fight Foreign IT and Digital Protectionism	48
Principle 5: Embrace IT and Digital Free Trade, Especially With Like-Minded Nations	48
Principle 6: Resist Authoritarian Influences in the IT and Digital Economy but Remain Focused on Key U.S. Interests.....	48
Principle 7: Defend the Private Sector’s Core Role in IT and Digital Governance.....	49
Principle 8: Defend the Principle That Big Is Not Bad, and Often Is Superior.....	49
Principle 9: Defend Innovation-Oriented Regulation.....	49
Principle 10: Defend the Mostly Open Internet	49
Principle 11: Support a Robust Domestic IT and Digital Policy That Ensures U.S. Global Leadership	50
Conclusion	50
Endnotes.....	52

INTRODUCTION

For the past quarter-millennium, each emerging wave of general-purpose technologies has widened the scope of global economic integration, raising new questions about international governance and national economic competition. The rise of the digital economy over the last two decades has further deepened and widened global integration as the Internet and related technologies have allowed firms to more easily attain global reach, while at the same time linking the world more closely in a web of information. But there is also a large countervailing force: an autocratic, non-democratic country—China—that is threatening to wrest global leadership in these technologies, with attendant social, political, economic, and security implications.¹

Against this backdrop, the key question today is how a world, extremely diverse in income levels, cultures, and types of government, will deal with global technologies and global firms. This is a particularly important question now. For unlike the prior period of globalization—which reached its pinnacle in the summer of 2001 (after China joined the World Trade Organization (WTO) and before 9/11 and the start of the failed WTO Doha round), a time when there was a wishful consensus that most nations would embrace globalization, rules-based open markets, democracy, and cooperation—today’s era is one of nationalization, mercantilism, increased authoritarianism, and tension.

The digital economy entails a degree of overlap—and tension—between economic, social, and political control that is different from traditional 20th century trade in physical goods. The digital world thus is rife with strife: There is conflict over cyberattacks, Internet blocking, and cross-border data flows; over attitudes and policies toward leading information technology and Internet firms; and over technology leadership and competitiveness. Indeed, for many countries and regions, advancement of their own IT and digital firms, sometimes involving active steps to hobble foreign competitors, especially American firms, has become a centerpiece of economic policy. (The Information Technology and Innovation Foundation (ITIF) defines digital economy industries as more than just Internet companies; they include firms involved in the entire “stack” of information technology (IT), including chip design, semiconductors, hardware, software, e-commerce, and Internet services.)

In this world, the United States as the global IT and digital leader has struggled to articulate and advocate for a coherent and strategic response. All too often, U.S. thinking about privacy, tech platforms, national security, and Internet and artificial intelligence (AI) governance is siloed and bifurcated. During the Clinton and second Bush administrations, U.S. policymakers believed that the rest of the world would emulate what was obviously the superior U.S. digital policy system, and they worked toward that end. But China’s unprecedented success in IT and digital industries, coupled with a questioning of the desirability of a U.S.-style light-touch digital regulation and the rise of U.S. “big tech” companies, has meant that the United States can no longer rely principally on persuasion to convince others of the economic and innovation advantages of its approach.

When that reality started to crystalize, the Obama administration made advancing the global “open Internet” one of its top global digital policy goals. Unfortunately, many countries have grown distrustful of the U.S. government, especially after the Snowden revelations showed the degree to which U.S. intelligence agencies were leveraging digital technologies for surveillance. Despite some reforms and engagement by the Obama administration, the last decade has seen

retrenchment rather than advancement of the open Internet globally, open governments, and an open, rules-based global digital economy.

The Trump administration's response to this rising digital competition was grounded in realpolitik and determination to put U.S. interests first, coupled with a reduced presence and advocacy of U.S. interests in international forums. But while the former part of this shift was needed, the reality of the global digital economy is that it is difficult to effectively advance U.S. national interests unilaterally.

This brings us to the present moment. The United States needs to move away from an idealist view of digital international relations to a new doctrine of “digital realpolitik”—focusing more on protecting key U.S. interests rather than acting as a global ambassador of Internet openness. The new doctrine needs to move away from the idealist's dream of a harmonized, values-based global Internet, as this is clearly not going to happen. It also needs to move away from principally unilateral action.

The U.S. government needs to formulate a grand strategy grounded in a doctrine of digital realpolitik that advances U.S. interests first and foremost, recognizing that it should work with allies when it makes sense, and constrain digital adversaries, especially China and Russia.

A realist strategy needs to be based on the central recognition that America must enlist, in a variety of ways, like-minded nations to support U.S. interests, and at the same time not be reluctant to exert pressure to have other nations come along. And given China's directly conflicting approach to the Internet, this needs to include cooperation on the overarching goal of limiting China's global dominance and manipulation of competitive markets in the IT and digital space.

Fears of the Internet fracturing at the root system level into a so-called “splinternet” are overblown. But it is true that global digital politics are likely to be highly contentious for the foreseeable future. Permanent alliances may be difficult to sustain, even against China. More likely, alliances will shift, depending on the issue.²

This means that shaping the global IT and digital economy in ways that are in U.S. interests is one of the most important challenges facing U.S. foreign and economic policy going forward. Getting it wrong could lead to a many-against-one environment wherein U.S. IT and digital firms—and by extension, the United States overall—face a challenging environment with consequences for many aspects of American life.

It is long past due to leave behind the hopeful, but naïve, view that most countries will see the digital economy the way the United States has historically seen it: as a force for progress, innovation, and free speech, wherein market outcomes should generally be allowed to prevail, with a light touch of government only in the few places needed. In the future, needed change will come more from appealing to foreign interests, rather than values and ideas.

The U.S. government needs to formulate a grand strategy grounded in a doctrine of digital realpolitik that advances U.S. interests first and foremost, recognizing that it should work with allies when it makes sense, and constrain digital adversaries, especially China and Russia.

This report first discusses why leadership in IT and digital technology is important. It then discusses where major nations or groups of nations stand vis-à-vis IT and digital technology and their strategies and successes. These include the United States, China, the EU, Japan, the Four Asian Tigers (South Korea, Taiwan, Singapore, and Hong Kong), developing nations generally, and disruptive nations such as Russia. The report then enumerates seven undesirable scenarios and how they may develop:

Scenario 1: EU “regulatory imperialism” succeeds, and America is isolated.

Scenario 2: Anti-tech forces turn America into the EU and China prevails.

Scenario 3: The EU won’t budge.

Scenario 4: Nations craft a “digital WTO.”

Scenario 5: China wins the minds (if not the Hearts) of UNCTAD nations.

Scenario 6: The splinternet emerges.

Scenario 7: The United States spends much of its political capital on promoting the open global Internet.

It then lists four desirable scenarios the achievement of which U.S. policy should seek:

Scenario 8: U.S., EU, and non-aligned nations isolate, punish, and defend against IT and digital “scofflaws,” such as Russia.

Scenario 9: The U.S. forms an Anglo-American (and friends) alliance to push back against Chinese innovation mercantilism.

Scenario 10: The United States, the EU, and non-aligned nations cooperate against China.

Scenario 11: The U.S. approach prevails in developing markets.

Finally, the report lists 11 key principles that should guide U.S. IT and digital policy internationally:

Principle 1: Unabashedly support IT and digital innovation, rejecting the techlash narrative and policies.

Principle 2: Embrace IT and digital “national developmentalism” (smart, active policies to support IT innovation and adoption) and bring more nations into that orbit.

Principle 3: Work to limit China’s IT and digital progress, especially when it based on innovation mercantilism.

Principle 4: Actively fight foreign IT and digital protectionism.

Principle 5: Advance IT and digital free trade, especially with like-minded nations.

Principle 6: Resist authoritarian influences in the IT and digital economy but remain focused on key U.S. interests.

Principle 7: Defend the private sector’s core role in IT and digital governance.

Principle 8: Defend the principle that big is not bad, and often is superior.

Principle 9: Defend light-touch regulation.

Principle 10: Defend the mostly open Internet.

Principle 11: Support and advance a robust domestic IT and digital policy that ensures U.S. global leadership.

WHY NATIONAL IT AND DIGITAL LEADERSHIP IS IMPORTANT

Since the rise of the first industrial revolution in Britain, most nations seeking wealth and power have focused on attaining leadership, or least competencies, in technologies that are emerging, foundational, and propulsive. These technologies change over time as emerging technologies become mature and nations master them. But initially, these technologies are emerging, and most nations seek capabilities. They are foundational in that they apply to many different parts of an economy and society, including to military capabilities. And they are propulsive, in that their growth spurs widespread investment and growth in the overall economy.

For example, when the British led in the development of the railroad, nations around the world sought to also adopt the technology. While the first modern steam locomotive railroad was built in 1830 between Liverpool and Manchester England, it took decades for other nations to attain it. For example, in the United States, rail miles grew from about 32,000 in 1860 to about 180,000 in the mid-1890s. And it was not until 1872 that the first railroad was built in Japan, which the modernizing Meiji government saw as critical to launching Japan into the modern age.³ Likewise, governments have sought to ensure technology capability in every key technology since, including steel, electricity, telephony, aviation, oil, mass production systems, computing, and now digital technologies.

Propulsive industries are almost always characterized by scale and the growth of extremely large firms, in part because only very large firms can assemble the resources to master the complexity of the task at hand.

Technologies such as the railroad and IT and digital today enable “propulsive” industries that generate an economic boom, both through the investment wave generated and the economic benefits they bring. In the late 1860s, about 10 percent of America’s non-farm paid labor and 50 percent of the production of its capital goods industries were involved in railroad construction. During the next major economic transformation in the late 1890s, the steel industry played a similar role. Again, in the early 1950s, the technology systems of chemical processing, electronics, and mass production powered an economic boom, with mass production goods industries such as automobiles and appliances propelling the U.S. economy to new heights.

During their emergent periods, these technologies and industries seem larger than life, capturing the excitement of the entire society. In the boom period of the railroad, it was at the center of the national imagination just as the Internet was from the mid-1990s to the mid-2010s. As one economic historian described it, “Stories about railroad projects, railroad accidents, and railroad speed filled the press, the fascinating subject was taken up in songs, political speeches, and magazine articles.”⁴ In 1880, sociologist Charles Fraser stated that “an agent is at hand to bring everything into harmonious cooperation, triumphing over space and time, to subdue prejudice and unite every part of our land in rapid and friendly communication ... and that great motive

agent is steam.” The rhetoric surrounding IT and digital technology was not all that different, at least until recently. But eventually the excitement dies, and in some cases turns to scorn, as we see with the current “Techlash,” wherein big tech firms and emerging tech generally are accused by many as the source of much that has supposedly gone wrong.⁵

Propulsive industries are almost always characterized by scale and the growth of extremely large firms, in part because only very large firms can assemble the resources to master the complexity of the task at hand. The United States saw this with the railroad industry, which generated America’s first large corporations, an industry many later industrial leaders, such as Andrew Carnegie, got their start in. Similarly, propulsive industries such as oil, aviation, autos, computing, and software were also characterized by the emergence of very large firms, just as we see with today’s large Internet firms. And from their early beginnings, these firms became global.⁶ And like now, populist reactions against these large firms emerged. Despite what the populists might say, scale and global reach is a feature, not a bug.

Once most nations have built out or developed a new foundational technology, it and the industry developing it cease to become central, and are usually relegated to routinized policy interest, just as industries such as rail, steel, oil, and mass production manufacturing are today in most developed nations. The excitement and policy focus shifts to the next emerging technology system.

But while the current IT and digital technology system is similar to prior emerging technologies in multiple ways—it is global, propulsive, foundational, and characterized by very large, global firms—it is different in three key ways:

1. The system is more of a production and consumer technology system than prior periods (e.g., mainframe computers were used by organizations, not consumers; search engines are used by everyone).
2. They are also a communication technology, which means that they impact what people see and hear, and who with and how they communicate, and thus have a broad political and social impact.
3. They have a potentially broader impact on jobs than most prior technology systems.

It is these aspects that add complexity to the global digital system, as it means that the technology systems links nations, firms, and people more closely together, often in ways that conflict with individual country norms and rules.

WHERE DO NATIONS STAND?

As noted, nations have long competed for leadership or at least competence in the propulsive industries of the day. So where do leading nations/regions stand when it comes to IT and digital?

America Leads

Since the development of computing in the 1930s, the United States has led the world in IT, with a succession of leading companies.

The particular nature of the IT innovation system played to U.S. strengths. Unlike some sectors and technologies wherein innovation could be pursued more incrementally by incumbent firms,

the history of the IT industry is one in which older firms committed to older technologies were regularly replaced with new ones embracing fundamentally different technologies. This relentless Darwinian winnowing and survival of the fittest played to America's entrepreneurial strengths. Americans were willing to take risks and start new enterprises, often with the support of robust venture capital pools. Indeed, with the establishment of the American Research and Development Corporation in 1946, the United States pioneered the venture capital industry.

As such, one key to U.S. success was the continuing entry of new IT companies, displacing others as leaders. Once-dominant companies such as Cisco, General Electric, Hewlett Packard, and IBM are now smaller than they were at their peak. And once strong companies such as AOL, DEC, EDS, Lucent, Motorola, Myspace, Netscape, Sperry Rand, Sun Microsystems, Yahoo, and Wang are either out of business or were purchased by other firms. And the top digital companies in the United States—Amazon, Apple, Facebook, Google, and Microsoft—are on average just 31 years old. Some of this evolutionary change came about as technology opened up new opportunities (e.g., the shift from mainframes and mini-computers to personal computers, the rise of the Internet, etc.) wherein incumbents could not adapt effectively, and new entrants emerged and thrived.⁷

This disruptive dynamic played out in the emergence of semiconductors. When Bell Labs pioneered the development of the transistor, it would seem logical for General Electric, America's sixth largest company, to lead in this technology. But it did not. Other new firms such as Texas Instruments did. And after presiding over the development of the transistor at ATT's Bell Labs, William Shockley founded his own semiconductor company in Mountain View, California, in 1957, called Shockley Semiconductor Laboratories. Rebelling against his authoritarian style, eight of the young technicians he had recruited—the “traitorous eight”—quit and formed their own company: Fairchild Semiconductor. When two of the eight, Robert Noyce and Gordon Moore, got frustrated working at Fairchild, they left to start their own firm: Intel. Another of the eight, Eugene Kleiner, cofounded the Silicon Valley venture capital firm Kleiner Perkins Caulfield & Byers, which made early investments in companies including Google, Amazon, AOL, Netscape, and Sun Microsystems.

The United States had another key advantage, one which China enjoys today, and that is scale. As noted business historian Alfred Chandler has written, the large American market enabled U.S. firms to successfully enter new mass production industries, such as chemicals, steel, and meat processing, and later autos, aviation, and electronics.⁴ Because scale mattered so much to innovation and firm competitiveness, U.S. firms such as DuPont, Ford, GE, GM, Kodak, Swift, Standard Oil, and others became global leaders.

Scale mattered even more to IT firms, for which fixed costs were high (writing the code, designing the chip, etc.) and marginal costs significantly lower. This meant that having access to a larger market gave firms key advantages that allowed them to drive down costs and reinvest the profits into the next generation of technology. As David Moschella argued in *Seeing Digital*, in most businesses, as sales grow, “there are initially important economies of scale due to learning and experience, but these eventually flatten out. In economic terms, the marginal cost comes to equal the average cost of adding more human capacity.” Software and network markets are different: “Here, the marginal cost of adding a new user to, say, Google or Facebook is close to zero. This means that average costs keep falling with volume, generating increasing returns to

scale, and a tendency to create highly profitable, winner take-all (or near all) industry structure.”⁸

And because digital industries, especially information (including search engines and social networking) and e-commerce, are characterized by scale and network effects, U.S. firms were able to capitalize on early leads to be the most competitive in the global market.

That contributed to another key success factor: The United States became a talent magnet, particularly for electrical engineering and computer science talent. Andy Grove, Andy Bechtolsheim, Vinod Khosla, Sergei Brin, Elon Musk, and Peter Theil are just a few of the top immigrant entrepreneurs who helped fuel U.S. IT leadership.

Another key advantage was U.S. government policy. With World War II and the subsequent emergence of the Soviet threat, the federal government constructed the world’s greatest innovation system. The massive expenditures on weaponry and research and development (R&D) in WWII positioned the United States as the leader in a host of advanced industries, including electronics. The response to the Soviet threat—exemplified by the satellite Sputnik—helped cement America’s technology leadership. By the early 1960s, the federal government invested more in R&D than every other foreign government and business combined. And that support for research, as well as contracts to provide needed government services and products, provided critical, although usually overlooked, inputs to America’s key technology hubs, including Boston’s Route 128 and Silicon Valley. Indeed, as late as 1990, Silicon Valley’s Santa Clara County received more Department of Defense (DOD) prime contract award dollars per capita than any other county.⁹

Absent major policy changes, it is likely that in the next decade America sees continued relative decline, and with it, increased dependency on other nations’ IT and digital products, including from non-allies.

As IT entered into a new phase in the 1980s and 1990s, with more powerful microprocessors, the emergence of personal, networked computers and easy-to-use software, it became clear to many policymakers that IT was now a key driver of growth and competitiveness, and that effective economic policy mean getting it policy right.

Successive administrations, supported by bipartisan agreement in Congress, took a number of steps to spur IT and digital innovation, including deregulating broadband telecommunications (as most American homes had access to at least two broadband “pipes”— cable and DSL), freeing up radio spectrum for wireless communications, and taking a light touch with respect to regulating online privacy, establishing Section 230 of the Communications Decency Act to protect Internet intermediaries from liability for content on their systems, opening up the GPS satellite system for commercial use, and using IT to transform government itself. Finally, at least until recently, the prevailing attitude toward IT and digital’s impact on jobs and the economy was positive, with few policymakers wanting to slow down transformation, even if it led to productivity growth and some employment disruption.

While the United States still leads in many areas of IT, its lead is shrinking and, in some cases, such as in telecom equipment to China, has been lost.¹⁰ And absent major policy changes, it is

likely that in the next decade America sees continued relative decline, and with it, increased dependency on other nations' IT and digital products, including from non-allies.

China Responds, Mostly Succeeds, and Is Poised for Further Success

In the early 1980s, when China sought to gain advantage in the IT industry, it was significantly behind Europe and the Four Asian Tigers. But it has arguably made the most progress, and succeeded in creating many viable competitors for leading American IT and digital companies, and in the case of telecom equipment, destroying the competition.¹¹

As a result, China's IT economy is massive. Around 30 percent of Chinese exports are in the IT sector.¹² However, much of this output and exports is by foreign multinationals that produce in China. But China has developed some leading multinationals of its own, including Huawei, Lenovo, and ZTE. In addition, its BAT companies (Baidu, Alibaba, and Tencent) have used their protected home market to grow and become dominant in China, before using it as a base to expand into foreign markets around the world.¹³

China has adopted some technologies at a rapid pace. For example, in 2019, there were an estimated \$1.5 trillion of online retail transactions, 25 percent of the nation's total retail transactions—more than twice both the volume and proportion of e-commerce in the United States.¹⁴ This is even more impressive given China's Internet penetration rate remains low at only 60 percent, and 99 percent of its Internet users have mobile Internet (with 70 percent using mobile payments).¹⁵

As in virtually all technology sectors, China's game plan is the same: first copy foreign technology (often through forced joint ventures, intellectual property (IP) theft, or reverse engineering); then limit access to the Chinese market of foreign firms while supporting domestic firms with a panoply of support, including grants, low-cost and preferential financial loans, tax breaks, discriminatory government procurement and other tools; and finally, supporting "going out" to gain market share outside of China.

China made arguably the most important digital strategy decision in the history of the IT industry. It decided it would not let the giant U.S. dot-coms—especially Google, Facebook, and Amazon—just set up shop and dominate the Chinese market.

China's first step was to attract foreign investment. In the early 1980s, when Deng Xiaoping opened up the Chinese economy to foreign investment, its main economic development strategy sought principally to induce foreign multinationals to shift relatively low- and moderate-value production to China.¹⁶

China's second step was to attempt to learn from foreign companies, in part by having them train Chinese executives, scientists, and engineers, and also by forcing them to transfer technology as a condition of market entry. Since roughly 2000, when China joined the WTO, it has deployed an array of unfair and often WTO-illegal tactics, including currency manipulation, massive subsidies, and limits on imports in order to both attract foreign establishments and support domestic manufacturers, especially in the IT sector.

The third step was to support Chinese companies in their efforts to copy and incorporate foreign technology while building up domestic capabilities. One important marker for the transition from

stage two to stage three was the publication in 2006 of “National Medium- and Long-Term Program for Science and Technology Development (2006–2020),” which calls on China to master 402 core technologies—including a host of IT sectors such as integrated circuits and high-performance computers. China moved to a “China Inc.” development model of indigenous innovation, which focused on helping Chinese firms, especially those in IT and digital industries.

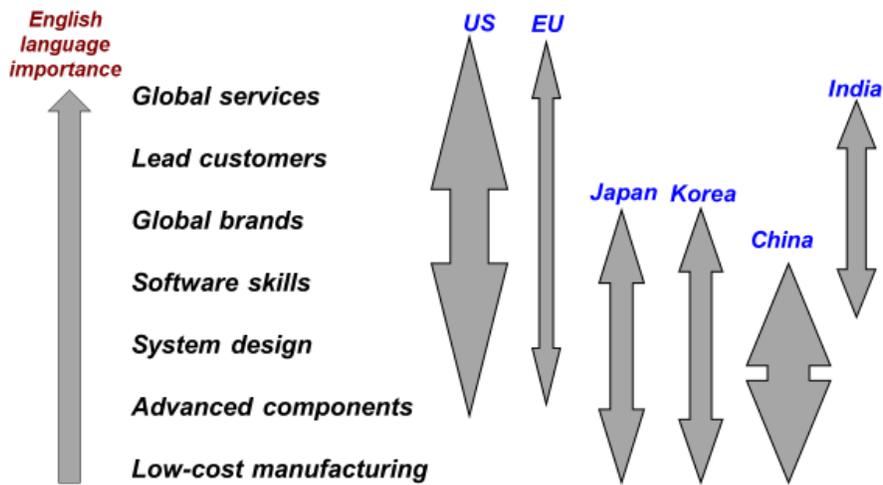
This is how China’s digital economy became dominated by domestic firms. The Chinese government banned international competitors, such as Facebook and Twitter, in 2009, and Dropbox and Google in 2010.¹⁷ Indeed, China made arguably the most important digital strategy decision in the history of the IT industry when it decided it would not let the giant U.S. dot-coms—especially Google, Facebook, and Amazon—just set up shop and dominate the Chinese market the way they were doing in so many other nations. Instead, it significantly limited the role of or banned U.S. firms, creating time for its own firms—especially Baidu, Alibaba, and Tencent—to build similar services, or at least initially copies of U.S. services. This means that a generation of Chinese consumers has grown up without knowing that their Internet and consumer experience is completely different than what is available in most other countries. And this happened during a critical, formative period of digital growth in China. While it is not possible to calculate an exact figure, ITIF has conservatively estimated (based on market-share comparisons) that Google, which withdrew from the Chinese market in 2010, subsequently lost \$32.5 billion in search revenue from 2013 to 2019, while Amazon and Microsoft’s cloud services (IaaS, which is restricted in China) lost a combined \$1.6 billion over the two-year period from 2017 to 2018.¹⁸

While this type of protectionism was unfair and even illegal under WTO rules, there is no doubt this “China First” strategy was wildly successful and led directly to China’s now highly diverse and dynamic mobile and Internet services industries. Its apparent success is what attracts many other large developing countries, such as India and Indonesia, in trying to replicate China’s success in developing an advanced IT and digital sector.

The fourth and final step was to enable Chinese firms to be independent innovators—as Japan, Singapore, South Korea, and Taiwan have all become. China is attempting to do this through an array of plans and policies: “13th Five-Year Plan for Science and Technology,” “13th Five-Year Plan for National Informatization,” “The National Cybersecurity Strategy,” and, of course, “Made in China 2025 Strategy.” For instance, with regard to information and communications technology (ICT)-enabled manufacturing, the strategy calls for 80 percent domestic market share of high-end computer numeric-controlled machines by 2025; 70 percent for robots and robot core components; 60 percent for big data; 60 percent for IT for smart manufacturing; and 50 percent for industrial software.¹⁹ Transitioning from “fast follower” to “global leader” in innovation is extremely difficult. And while China is among the leaders in some areas such as telecommunications equipment, it is farther away in others such as semiconductors—but is closing the gap. (See figure 1.)

Figure 1: National IT and digital strengths²⁰

National IT strategies mostly focus on distinct value chain layers



This is important because too many experts, pundits, and policymakers in the United States persist in believing that China can never catch up technologically and as such never be a technological threat to the United States. They believe that because they hold that there is only one “recipe” for innovation success, and that this is the Washington Consensus model of free markets, IP rights, and limited government. This is why Zachary Karabell wrote in *The Washington Post*, “Chinese firms excel at copying but not yet at creating. As a result, smart foreign companies realize that the lasting solution is innovation, not courts and lawyers.”²¹ Kerry Brown, a professor at Kings College London, wrote,

The Chinese government under Xi can pour all the money they want into vast research and development parks, churning out any number of world class engineers and computer programmers. Even with all of this effort, however, China is likely to produce few world class innovative companies. The fundamental structural problem is that the role of the state and government in China is still very strong ... The system that China currently has still rewards conformity.²²

Self-congratulatory assumptions on the part of U.S. commentators about China’s inability to innovate are not only wrong, but dangerous.

Officials and experts in China love to send this message to Americans. They pretend to bemoan the fact that that government is bad at “picking winners” and that China would be better off without such policies, but alas, the government hasn’t yet seen the light. The not-so-subtle subtext is don’t worry about us, we can’t challenge you technologically.

Such self-congratulatory assumptions on the part of U.S. commentators about China’s inability to innovate are not only wrong, but dangerous. As Gregory C. Allen, a fellow at the Center for a New American Security, wrote, China’s dominance in AI technology and its military applications are not only credible, but likely, in the absence of a massive shift in U.S. policy. The reality is that China can innovate, even if it is not always “first to the world,” and that has, does, and will

challenge U.S. IT and digital leadership.²³ It will also innovate in very different areas, prioritizing those valued by the state, such as facial recognition, social credit, traceable financial transactions, and the like. Overall, China is the most serious competition America has ever faced.

Europe Responds, But Largely Fails

Europe has responded to America's digital leadership with concern, even alarm. Many EU policymakers regularly call out U.S. technology "colonization" and call for "digital sovereignty" against (U.S.) "dominant platforms."²⁴ The French Minister for Economic Affairs went so far as to call U.S. "big tech" companies an "adversary of the state"²⁵

These reactions are not new. Since the 1960s, Europe has viewed U.S. IT leadership with alarm. As French economic journalist Jean Jacques Servan-Schreiber wrote in his 1968 bestseller, *The American Challenge*, "One by one, U.S. corporations capture those sectors of the economy most technologically advanced, most adaptable to change, and with the highest growth rates."²⁶ Like today, Europeans characterized the challenge in dire terms: "a seizure of power," "invasion," "domination," "counterattack," and "industrial helotry."

Also like today, it was not just European politicians sounding the alarm, it was European business. The major business trade association of Europe (UNICE) complained that U.S. firms actually had the audacity to cut prices, writing in a report to government:

A joint study of production costs has allowed us to set rules which, while safeguarding competition, prove beneficial to all. We must not allow the American firms from lack of knowledge of our methods, to provoke a price war that would cause serious difficulties in the market.²⁷

In other words, American firms refused to participate in price cartels and instead focused on providing EU consumers with lower prices, and this should be stopped.

Servan-Schreiber called for Europe to get its house in order: Build a single market, fund advanced technology R&D, and expand university enrollment, particularly in STEM (science, technology, engineering, and math). He eschewed any talk of punishing or rejecting U.S. investment. In fact, he wrote, "Nothing would be more absurd than to treat the American investor as 'guilty' and to respond by some form of repression."²⁸

As both a cause and effect, in response to the current "invasion" by U.S. digital firms, Europe has embraced the kind of "repression" Servan-Schreiber counseled against.

Despite fretting about the U.S. "invasion" for over half a century, and the success of such firms as Arm, SAP, Skype, and Spotify, Europe largely failed to generate global-leading IT and digital firms. In fact, Europe has lost global market share, especially to China.²⁹ As figure 1 shows, compared with nations such as South Korea and Taiwan—and especially the United States—the EU has broader technology capabilities across value chains, but has much shallower capabilities in each area.

As both a cause and effect, in response to the current "invasion" by U.S. digital firms, Europe has embraced the kind of "repression" Servan-Schreiber counseled against. The EU has deployed a wide array of mercantilist tools to protect itself in the hope of hobbling, Gulliver-like,

the American giants so that that the EU “Lilliputians” can grow. This takes the form of aggressive antitrust enforcement; limitations on the export of data; taxes on U.S. digital companies’ sales (digital services taxes); geo-blocking prohibitions; regulating video platforms as traditional audiovisual providers; government funding of technology alternatives (e.g., the Quaero search engine, the GAIA-X cloud project); establishing EU-approved “data intermediaries” as an alternative to U.S. tech firms; mandates for paying newspapers to list their articles in search results; limits on price discounts by e-commerce retailers; requirements to take down information from the web (“right to be forgotten”); charging foreign firms more for access to EU government data; massive fines for privacy, content, and other digital violations; onerous regulatory restrictions on the use of data; and many others.³⁰

There are multiple reasons for Europe lagging behind in IT and digital, especially in developing EU-headquartered firms (most U.S. tech firms actually invest significantly in EU operations, including R&D). One is its approach to antitrust. With the Sherman Act, the United States banned trusts and cartels, which led American firms to merge and get big, significantly boosting their global competitiveness.³¹ In contrast, Europe was more permissive toward cartels and other cooperative arrangements (as noted by the previously mentioned UNICE statement), which meant that on average EU firms remained smaller. For example, in 1966, the United States had 134 corporations with annual revenues of more than \$500 million, while Europe had just 41. In the IT sector, wherein scale is everything, this was a serious drawback. Europe’s continued veneration of small businesses continues to hold back its digital leadership, as it leads to a reinforcing cycle of attacking large U.S. IT firms while at the same time continuing to provide small EU firms with a host of preferences, which are tied to them being small and just ensure they remain small.³²

Europe also has a long history of throwing money at second-rate “national champions,” usually in an attempt to win “the last war.” For every Airbus or Ariane, there are many more failures.³³ Europe did that with mainframe computing in a quixotic campaign to challenge IBM, funding companies such as Bull and Olivetti, before the weakened firms were bought up by General Electric—which in turn also failed at computing. And Europe failed in the Eureka project to create a digital television industry. It failed to build the next so-called “Google killer” with Quaero, and the next cloud giant with Cloudwatt or Numergy.³⁴ And now the French government wants to inject public money into creating the next Airbnb.³⁵ In this case, they fail to effectively predict the future, as noted by a 2006 European Commission report on national champions, which does not even mention the Internet.³⁶

EU policymakers never understood, and still largely don’t, that the way to compete with American tech giants is not to take them on directly, but to rely on Schumpeterian competition. As Joseph Schumpeter wrote:

[C]ompetition from the new commodity, the new technology, the new source of supply, the new organization ... competition which commands a decisive cost or quality advantage and which strikes not at the margins of the profits and the outputs of the existing firms but at their foundations and their very lives.³⁷

Europe consistently strikes at the margins—by taxing, regulating, and fining American tech giants—when it should strike at foundations, by supporting disruptive technologies in which U.S. (or Chinese) firms are not yet established. They continue to fight the last war, with their focus on

cloud computing, search, and social networks; all relatively mature technologies wherein new entrants will have a difficult time penetrating because current offerings are so good and because scale economies and network advantages make entry difficult. The United Kingdom has performed a bit better, with a rich history of at least inventing, if not exploiting, IT (for example, Deep Mind).

Structurally, the EU continues to suffer from a number of challenges, including limited venture capital funding, a relatively weak higher education system for computer science, and too many small firms that do not scale.³⁸ In addition, even though the EU has made considerable progress since 1992 in establishing a single market, and more recently, a “digital single market,” it still has not completed the task. And even with that, language differences make it harder for firms to scale quickly across Europe, leading them to lag behind Chinese and U.S. competitors.³⁹

Because of a lack of synchronized layers of laws and regulations (in other words, regulatory fragmentation) across member states, and a digital single market that remains more theory than reality, the EU has been unable to nurture data-driven business models through a large domestic market. There are still divergences in IP rules, licensing arrangements, and regulatory enforcement, as well as obstacles to the efficient delivery of online goods. Fragmentation prevents scale for companies—in a digital economy in which successful players are those that can harness network effects.

Europe also lagged because its firms did not embrace the IT “ecosystem-based” business models. For example, in 2006, Nokia was the leading cell phone maker in the world. Within just a few years, Apple was dominant and Nokia’s cell phone business was dead. This was in large part because Apple was able to leverage technology to create a unique customer experience through a product-service, ecosystem-based business model. In addition, the EU generally put an emphasis on mechanical engineering at the expense of software capabilities, even as Marc Andreessen famously stated that “software is eating the world.”⁴⁰

In addition, Europe has not been able to generate an environment in which enough new firms emerge and then reach global scale. In 2000, for example, there were 30 major IT companies started since 1950 and still strong in the United States, compared with just 3 in Europe.⁴¹

Europe has even convinced itself that its array of heavy-handed, precautionary-based digital economy regulations, rather than being a drag on innovation, are actually a spur to it.

The kinds of disruptive change needed to succeed in the digital economy goes against the nature of Europe. America was settled principally by Europeans who wanted out from under the yoke of feudal hierarchy and limitations. The ones that remained were less entrepreneurial and more committed to the status quo. As Servan-Schreiber wrote, “Behind the success of American industry lies the talent for accepting and mastering change.”⁴² It appears no different today, with 41 percent of Americans strongly agreeing that in general they are willing to take risks, compared with 8 percent in Spain and 10 percent in Germany.⁴³

As Servan-Schreiber alluded, behind the success of the American tech economy lies the embrace of change and innovation. In contrast, the EU has embraced the “precautionary principle” wherein virtually every new innovation is approached from a “glass half empty” view, with the

urgent need to form a commission of experts—largely academics and “civil society” representatives with little connection to actual commerce—to study the innovation and identify the sundry and various ways it could go bad, especially in the hands of the profit-hungry, U.S.-cowboy capitalists.⁴⁴

Europe has even convinced itself that its array of heavy-handed, precautionary-based digital economy regulations, rather than being a drag on innovation, are actually a spur to it. The dominant narrative in Brussels and most EU states is that the strict regulation of privacy, AI, and other emerging technologies is required in order to boost consumer trust, which in turn will give EU firms a leg up because, unlike the United States, EU consumers will more readily adopt these technologies. However, the fact is they do not. The scholarly evidence is quite clear that these kinds of restrictive regulations (as opposed to balanced regulations) not only deter innovation but fail to spur more digital adoption.⁴⁵ Moreover, they believe that since EU firms will already be in compliance with what will soon become global regulatory standards, they will gain competitive advantage.

At times, it's even worse, with European elites being actively hostile to technology and capitalism. Simone de Beauvoir, a leading French intellectual, wrote in 1966:

In every country of the world, socialist or capitalist, man is crushed by technology, alienated from his work, enslaved and brutalized. This has happened because man has multiplied his needs rather than constraining them.... When did this downfall begin? The day we began to prefer science to wisdom and utility to beauty.

In other words, the peasants should be happy with immiseration, looking at the beautiful sunsets after a long day of backbreaking labor with scythes and rakes.⁴⁶ Similar statements today about emerging technologies such as AI abound. For example, **Loubna Bouarfa**, a member of the European Commission's Artificial Intelligence High Level Experts Group, embraces resistance to AI, writing, “I find that this resistance has great potential. We must embrace it as a wake-up call; treating it not as a direct cause of alarm, but as a valuable societal warning sign.”⁴⁷

Strict and stifling digital regulations don't just come from a deep-seated commitment to the precautionary principle; they come from the fact that Europe remains a social-democratic society wherein markets, businesses (especially large and U.S. businesses), and technologies are suspect, government is privileged, and so-called “civil society” groups are presumed to represent the public interest. Moreover, these regulations come from a long-standing concern in Europe over employment, where job loss is something to be avoided, and policymakers have struggled to bring unemployment rates down to U.S. levels, in large part because unemployment benefits and other income support systems are so generous that many people choose to stay out of the labor market longer than they otherwise would and many firms are virtually prohibited from dismissing workers.

None of this, of course, is to say that the correct alternative is libertarianism, despite the fact that some EU officials believe this is the overriding U.S. governing philosophy. It is to say that the only way a nation or region has any chance of succeeded globally in the digital economy is to adopt a balanced approach to regulation that privileges both innovation and social protection. This means recognizing that no one right or interest (such as privacy) should define a

government's approach to innovation, but that like any public policy issue, there are going to be multiple rights and interests to balance.

Japan and the Four Asian Tigers Respond, and Partially Succeed

Japan and the Four Asian Tigers were the miracle economies of the 1970s and 1980s. The Japan challenge to U.S. technology leadership in the 1980s was particularly significant, with a host of books being written about it.⁴⁸

To be sure, all five countries or territories have made significant progress in technology, most of it fueled by a burning desire to develop and catch up, especially in technology industries. All five relied on explicit government industrial policies, with their strategies following particular phases. As Linsu Kim wrote in his definitive history of Korean-innovation upgrading, *Imitation to Innovation: The Dynamics of Korea's Technological Learning*, there are several distinct stages these nations took to try catching up to the leaders in innovation. The first stage involved the transfer of foreign technology to that nation—sometimes by foreign direct investment, sometimes by licensing, and to some extent, although vastly less than with China, by theft.⁴⁹ This was supplemented by intensive education in technical fields; supported by rigorous screening, testing, and promotion (something few other developing nations did).

This painstaking process of doing the work hard on the low end of commodity IT markets first, and then working their way up was based on humility, patience and hunger (something Europe lacks).

The second stage involved “the effective diffusion of imported technology within an industry and across industries.” The third stage:

involved local efforts to assimilate, adapt, and improve imported technology and eventually to develop one's own technology. These efforts are crucial to augmenting technology transfer and expediting the acquisition of technological capability. Technology may be transferred to a firm from abroad or through local diffusion, but the ability to use it effectively cannot. This ability can only be acquired through indigenous technological effort.⁵⁰

This painstaking process of doing the work hard on the low end of commodity IT markets first, and then working their way up, was based on humility, patience, and hunger (something Europe lacks today).

The final stage is to become global innovation leaders, with all four (leaving aside Hong Kong) regions working to achieve. As Lim wrote:

Firms in catching-up countries that have successfully acquired, assimilated, and sometimes improved mature foreign technologies may aim to repeat the process with higher-level technologies in the transition stage in advanced countries. Many industries in the first tier of catching-up countries (e.g., Taiwan and Korea) have arrived at this stage. If successful, they may eventually accumulate indigenous technological capability to generate emerging technologies in the fluid stage and challenge firms in the advanced countries.⁵¹

These places, especially Singapore, Taiwan, Japan, and South Korea, focused on IT hardware, including semiconductors, computers, consumer electronics (e.g., TVs), and more recently smartphones. For example, computers, telecommunications equipment, and the manufacture of electronic components/circuit boards account for close to 90 percent of the value added by Japan's ICT sector.

As figure 1 shows, these Asian nations have specialized and competed mostly in hardware and components.⁵² Taiwan is home to a world-leading semiconductor foundry, TSMC, as well as a host of component and hardware makers. South Korea is home to two world-leading semiconductor producers, Samsung and SK Hynix, and electronics firms such as LG. In Japan, long-standing electronics firms such as Hitachi, NEC, and Mitsubishi Electric have all moved into ICT production, and Softbank is a world-leading holding company for advanced IT and software firms.

These nations took a different approach from Europe. First, they initially relied on low wages to gain market share at the lower end of the value chain in many IT segments. And they were willing to accept lower margins, something most U.S. technology companies were not, and often were supported financially by the state. As a result, many U.S. technology companies ceded the low end of many markets to these regions, hoping to retain the more profitable, higher ends. However, these nations were not content with staying at the lower end, and used that entry to gain knowhow and experience, and then reinvest into the next generation of technology, gradually working their way up the value chain, often taking U.S. market share.⁵³

At the same time, each country provided valuable government support in the form of industrial and technology policy.⁵⁴ In Taiwan for example, the public-private Industrial Technology Research Institute (an entity established in part by the U.S. government in the 1960s), played a key role in helping Taiwanese technology firms.⁵⁵ Singapore invested significantly in government R&D targeted to the technology industry, supported universities to do research and train engineers and computer scientists, and actively recruited leading IT firms from around the world.⁵⁶

Despite these policies, and their success, for the most part these nations did not fully capitalize on the Internet and digital era, especially in Internet services. In Japan's case, one reason was it initially did not embrace the Internet-era global, interoperable standards, preferring to develop its own standards. In what has been termed the "Galapagos Island Syndrome," Japanese enterprises developed quite advanced IT products that were nevertheless isolated from global markets. Japan's development and adoption of unique standards for second- and third-generation (2G and 3G) mobile networks contributed to Japan's leading mobile-phone manufacturers, including NEC, Panasonic, and Sharp, dominating domestic markets with innovative mobile technologies and products. Indeed, in the early 2000s, many American commentators visiting Japan praised Japanese cell phone makers for being more innovative than American ones. But because they adopted Japan-only standards, these Japanese technology firms had difficulty exporting to foreign markets and gaining needed scale.⁵⁷ And these early leaders were soon left behind firms that chose to use global standards.

And like Europe, by the time many firms in these countries got around to focusing on key Internet technologies, such as search and social media, U.S. firms had already made considerable progress, and because of network effects, essentially locked in the market. In

addition, some of these nations, particularly Japan and Korea, had a much less well-developed entrepreneurial ecosystem, with many workers preferring to work for large, well-established companies. On top of that, there was more resistance to disruptive innovation, with entrenched interest groups fighting new entrants.⁵⁸ Finally, it is hard to overstate how much of a factor the English language was in limiting global Internet opportunities for these nations.

However, the governments of Japan, Singapore, South Korea, and Taiwan have succeeded in newly emerging digital technologies, such as the Internet of things, AI, and robotics—a key focus of their technology policies. Singapore has well-developed AI policies.⁵⁹ South Korea has formed a presidential commission on the Fourth Industrial Revolution.⁶⁰ And Japan has developed a national AI initiative.⁶¹

NATION STATES STILL MATTER

Even if their products are sometimes virtual, IT and digital firms have physical presences in actual countries, and their products and services are sold to actual people and organizations. Countries seek advantage in these industries, and many do so by designing policies that hurt foreign competitors. For this reason alone, the concept of the nation state and national interests continues to matter.

However, the rise of the Internet has led some to argue that it leads to new and unprecedented global structures and functions, and that concepts such as national power are now anachronistic. In his classic 1996 Internet manifesto, cyber guru John Perry Barlow waxed poetically about some special place called cyberspace:

The Internet has no elected government, nor is it likely to have one, but this does not mean it is not governed. The Internet is ruled, as are all technologies, not only by the norms and beliefs of its users, but also by the laws and values of the societies in which they live,... We do not want an Internet controlled by the nations of the world, but neither do we want an Internet divorced from government. We seek a balance that recognizes both the rights of the individual and the benefits to the community of well-ordered systems.... We reject your declaration of independence and take up a new call for interdependence among sovereign nations and peoples. We will work together in common cause so that no one can arrest our progress.⁶²

People could be excused for falling for this kind of philosophizing in 1996 when few even used the Internet. But there is no reason why anyone should today. Yet many still do. *The Economist* recently wrote:

To make sense of all of this, it helps to see the political world as one in which technology is beginning to look every more like geography ... where a state's territory stood in respect to such geographical facts of lie told it what is should fear and what it might aspire to, whose interests conflicted with its own and whose might align with them. In other words, geography was destiny. The units of analysis for today's nascent technopolitics are platforms."⁶³

Former State Department official Anne-Marie Slaughter, agrees, writing in *Foreign Affairs*:

Think of a standard map of the world, showing the borders and capitals of the world's 190-odd countries. That is the chessboard view. Now think of a map of the world at night, with

the lit-up bursts of cities and the dark swaths of wilderness. Those corridors of light mark roads, cars, houses, and offices; they mark the networks of human relationships, where families and workers and travelers come together. That is the web view. It is a map not of separation, marking off boundaries of sovereign power, but of connection.⁶⁴

As does NYU's Jeff Jarvis:

We also see globalization not only in commerce—affecting jobs and economies—but also in social interaction. Thus, borders are challenged and so are nations. Is this challenge a reason why we see the rise of nationalism? We see now that wars can be fought with data and without national armies or weapons. We see that virtual currencies can challenge the monetary power of nations. Will the nation-state as we know it survive intact?⁶⁵

In this notion, competing nation states are not the problem and in fact are structurally weakened in the digital age. Rather, the challenge is from amorphous networked systems. This is fanciful to say the least. The telegraph and telephone no more did away with the need for a Westphalian view than the Internet does now. Notwithstanding some individuals who commit cybercrime, it is still governments that take or support actions that most directly impact U.S. national interests, and it will continue to be. When a nation state truly wants to affect change on the Internet, it can do so. The question at the heart of this report is how nation states such as the United States go about articulating and advocating for their preferred approach to Internet governance—not whether they should be trying at all.

The telegraph and telephone no more did away with the need for a Westphalian view than the Internet does now.

An associated branch of this Internet exceptionalist view is that the United States and other democracies should be focused on challenging the so-called authoritarian Internet: the use of digital technologies to limit freedom. For example, Cohen and Fontaine warned, “In Zimbabwe, for instance, the Chinese AI company CloudWalk is helping develop a national facial recognition system, giving the local government a powerful new tool for political control.”⁶⁶

But the Internet and associated technologies such as AI and facial recognition are no more authoritarian than technologies such as the guns and mainframe computers the Nazis used. Facial recognition systems, for example, can be bought in every nation, and most governments will eventually install them widely because of their significant benefits. The issue is not that some technologies are authoritarian. The issue is the rules under which they are used. Authoritarian nations will use technology for authoritarian purposes. Democratic nations will use them for legitimate and civil-liberty-protecting purposes. Moreover, history has shown that short of overthrowing these governments and installing democratic ones, the best that can be hoped for is diplomatic pressure to limit abuses. Telling an authoritarian dictator that Internet openness, as desirable as it is, is better for them is like telling a dictator that his nation is better off with democratic elections. And banning U.S. exports of technologies that might be misused does little or nothing to limit techno-authoritarianism, and hurts U.S. economic interests.⁶⁷

MAJOR CENTERS OF NATIONAL POWER IN THE DIGITAL WORLD

It has become common to argue that the Internet is splintering into multiple different Internets. One report stated that “several Internets are currently coexisting uneasily.”⁶⁸ In fact, this is quite misleading. There is only one Internet. Siberia and South Carolina both use the same Internet, even if for the most part they don’t view the same Internet pages. While there is still one Internet (in terms of the technical architecture), there are multiple Internet policy regimes.

Idealistic notions of a unified global Internet community living in love and harmony, above craven and corrupt governments and bureaucrats, is now thankfully mostly assigned to the dust bin of history. But there is a risk that this simple-minded framework will be replaced by another one: that the overarching issue in digital governance is the fight between open democracies versus closed autocracies. Jared Cohen and Richard Fontaine wrote:

Almost in parallel, the United States and its allies have stepped away from their tradition of collaboration. Instead of working together on issues of common interest, they have been pulled apart by diverging national interests and have responded incoherently to autocratic states’ co-optation of new technologies. Although officials in most democratic capitals now acknowledge the profound ways in which new technologies are shaping the world, they remain strangely disconnected from one another when it comes to managing them.⁶⁹

While this is no doubt true and problematic, it assumes that there is just one major axis of conflict: between open democracies and closed authoritarian regimes.

Even if all countries had an open Internet, the United States would still face significant global digital policy challenges and conflicts.

But this is too simple. Even if all countries had an open Internet, the United States would still face significant global digital policy challenges and conflicts. To fully understand global digital policy conflicts, it is useful to formulate a framework comprising six major groups of nations. To be sure, any such typology risks oversimplification, in part because some nations can be aligned with more than one camp, depending on the issue. But this formulation hopefully provides a useful guide for how the U.S. government should constitute a grand digital strategy.

Tensions between these groups of nations play out over three main clusters of issues: 1) issues of criminal or other malign activity, such as Internet piracy and cyber-attacks; 2) social and economic regulation, including of AI and other emerging technologies, privacy, Internet, and telecom standards; and 3) issues related to national technology competitiveness and national security, including cross-border data flows, taxation, IT and digital competitiveness policies, encryption and law enforcement access to data, and export controls. Nations have different views on these issues for a variety of reasons.

The United States: The Major Advocate for and Driver of Global IT and Digital Innovation and Progress

The first group is the United States. Because the United States is home to global-leading IT firms, it seeks a deeply globally integrated market, including with data flows and Internet openness, so that its firms can fully benefit from expanded markets. But the motivation goes beyond commercial. The United States has also pushed for this, and the policies that go along

with it, because most U.S. policymakers believe that technological innovation is critical to global gross domestic product (GDP) growth and societal progress, and democratic values, norms, and processes are critical to human fulfillment. And they rightly see U.S. policies, practices, and firms as maximizing these.

Because of this, U.S. policymakers push for limiting unfair and protectionist foreign IT policies, not only because they threaten U.S. interests, but because they harm global IT innovation.⁷⁰ At the same time, the United States has pushed for a governance approach to the Internet and IT standards generally that is based on a voluntary, industry- and stakeholder-led, bottom-up standards process, rightly pushing back against some government efforts to dictate standards. It has also pushed for an open Internet wherein all or most legal content is available to citizens, because of the belief in the democratizing and empowering force of information. And from the Clinton administration, Internet governance principles crafted by Ira Magaziner to efforts by the Trump White House supporting a light-touch approach to AI regulation, the United States has generally avoided innovation-harming regulatory regimes and sought to convince other nations of the wisdom of this approach.⁷¹

More recently, the United States has tried, albeit haphazardly, to lead a global coalition to push back against Chinese IT and digital dominance, including in the telecom equipment and AI spaces. There are three main motivations for such actions: 1) concerns about cybersecurity and Chinese government access to foreign networks; 2) concerns about Chinese Internet values, including censorship and government surveillance, spreading globally; and 3) concerns about the damaging effects of Chinese predatory “innovation mercantilism” practices on U.S. competitiveness and global innovation.

China: Seeking Global Hegemony Through Technology

China is not a “normal” country when it comes to trade and globalization, especially in the IT and digital field. Even Asia Tigers who sought to build up their key industries through heavy-handed industrial policy never embraced autarky in all key sectors. China does. There is no IT sector, perhaps with the exception of IT consulting, in which China does not seek global leadership, if not dominance. That alone makes China the most important threat in the IT and digital space to virtually every country hoping to grow or maintain its IT and digital industry.

China has worked tirelessly to increase its influence on important international bodies related to IT and digital technologies, such as the ITU, in order to shield it from global scrutiny and help ensure its approach to IT and digital policy is widely adopted.

It would be one thing if China were simply a supercharged Taiwan or South Korea. The threat would be only loss of key industries and the jobs associated with them. But China is not just another Asian Tiger; it is a Leninist dictatorship that rejects Western values of free speech, an open press, democratic elections, and the rule of law. Indeed, under Xi Jinping, all party apparatuses are to “guide the broad masses of teachers and students to be strong believers” in Marxist theories and socialist core values.⁷² Indeed, the famous Document 9, an internal communique from the party in 2013, warned all cadres to stop universities and media from discussing seven topics: “Western constitutional democracy, universal values, civil society,

neoliberalism, the Western concept of press freedom, historical nihilism, and questioning whether China's system is truly socialist."⁷³

It is one thing for another country with different cultural values than those of the United States to seek to preserve those values. It is quite another for a country such as China to reject core values grounded in respect for human rights and freedom.

Finally, as an aspiring global hegemon, China uses a combination of carrots and sticks to bribe and bully other nations into submission, including its "digital silk road."⁷⁴ Moreover, it has worked tirelessly to increase its influence on important international bodies related to IT and digital technologies, such as the ITU, in order to shield it from global scrutiny and help ensure its approach to IT and digital policy is widely adopted.⁷⁵

Europe: Precaution and Protection

As noted, the European Union is characterized by two key foci, both of which put it at odds with the United States.

The first is a desire to impose a precautionary-principle-based regulatory framework on the digital ecosystem, not only in Europe but in virtually every nation in the world, outside of nations such as China and North Korea. Achieving this framework globally would not only be detrimental to global innovation, it would harm U.S. technology interests. One reason is EU techno pessimism—AI and robots kill jobs, AI is biased, virtual reality is addicting, e-commerce hurts small firms, big tech breeds inequality, big firms should be chopped down to size, Internet companies practice "surveillance capitalism," and on and on—not only dampen excitement for and interest in digital technology innovation, they generate anti-innovation policies.

Europe is talking out of both sides of its mouth, promoting free trade so it can get access to foreign markets for its goods, while also protecting its markets when it comes to some sectors and technologies in which it is weaker.

The second is the growing and increasingly naked EU protectionism, which takes the form of an array of attacks on U.S. technology companies, limits to EU markets, and policies to unfairly prop up EU competitors. Until recently, much of the EU's focus was on spurring its own domestic innovation, including by trying to establish a digital single market. But under the new commission, that has changed. Now, with stronger Franco-German leadership, its focus is much more about protectionism.

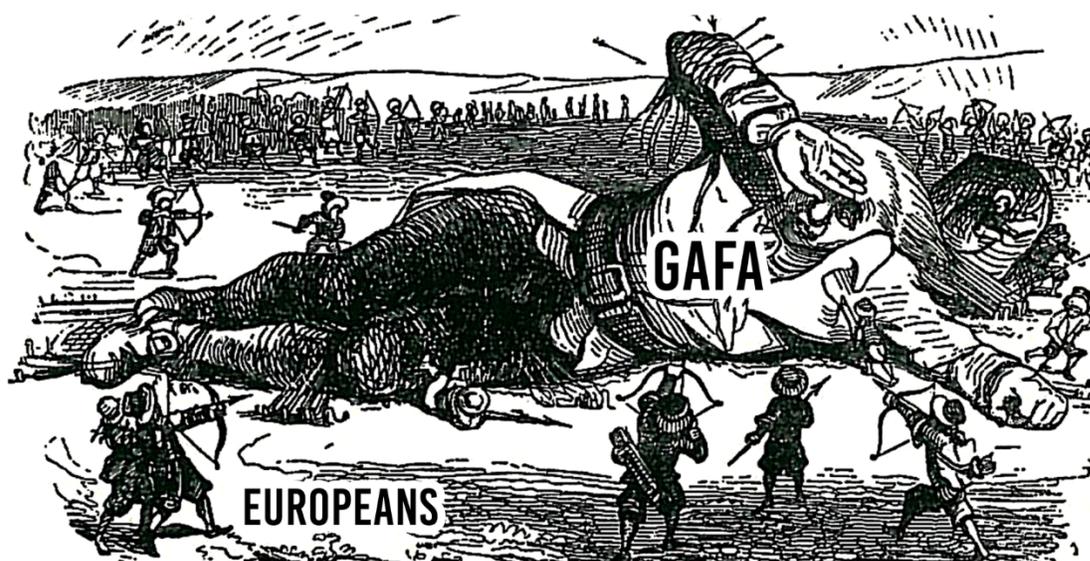
EU officials now frame much of this agenda around the importance of small businesses, which, in their narrative, are victimized by big tech and need an array of special privileges and government handouts in order to thrive.⁷⁶ They argue, without evidence, that small business is the driver of innovation and all good things, and that digital policy must be not only biased toward "little tech" but biased against "big tech," especially U.S. big tech. This is the only way to give "little tech" a fair and fighting chance.

Without a Gulliver-like tying down of U.S. big tech, including through antitrust, onerous privacy rules, mandated data sharing, algorithmic audits, and public data banks (where small companies get free access), discriminatory taxation targeting U.S. tech companies, asymmetric rules regarding platforms, and other measures, coupled with subsidies and other favors for EU "little

tech,” the latter supposedly will have no chance. For example, the proposed EU Digital Services Act is quite clear of the intent: “Asymmetric rules will ensure that smaller emerging competitors are boosted, helping competitiveness, innovation and investment in digital services, while targeting specific harms emerging from large platforms.”⁷⁷ The proposed Digital Markets Act just by happenstance appears to include only foreign (mostly U.S. companies). Rather than focusing on boosting their own framework conditions, and celebrating their overwhelming export success with the United States, they focus instead on raising U.S. tech firms’ costs. Finally, Europe’s forthcoming rules on foreign subsidies could give it the power to unilaterally shut out U.S. products from the EU marketplace, without having to go through the WTO.⁷⁸

Leaving aside the clear violations of the spirit, if not the letter, of the WTO—which EU officials proudly tout their allegiance to—such policies will do little to help grow the EU digital economy—but they will harm the U.S. tech economy.

Figure 2: EU Lilliputians “tying down” the U.S. tech Gulliver



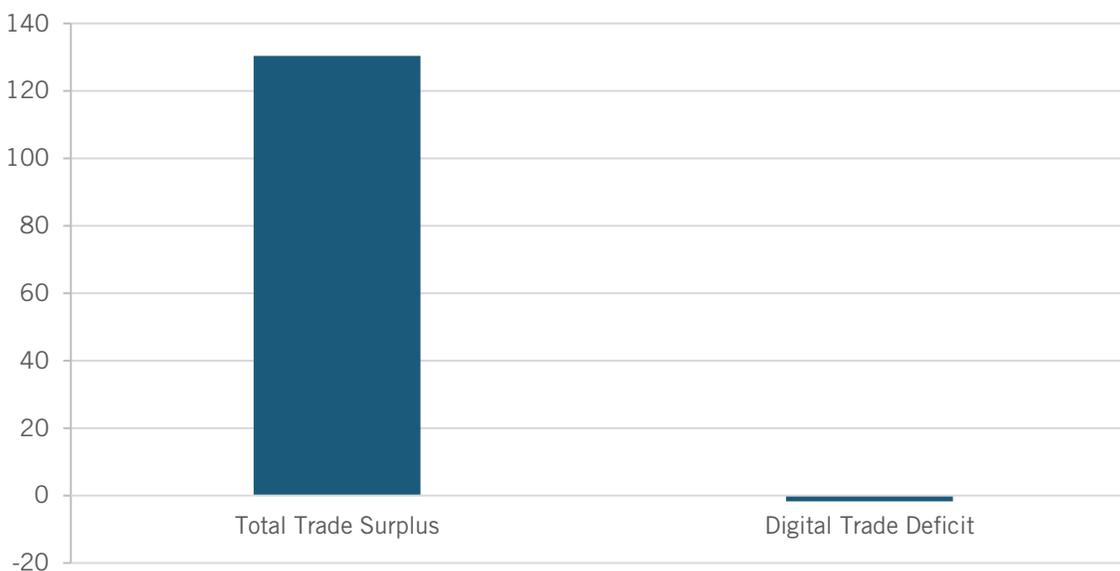
Many European officials actually believe that the digital threat from America is greater than the threat from China, and many believe that the condition for cooperation depends on the United States embracing the EU digital regulatory system.

The EU is convinced that it needs to, in the words of EU President Ursula von der Leyen, “achieve technological sovereignty in some critical technology areas.”⁷⁹ Thierry Breton, the EU Commissioner for Internal Market, argued that “European data should be stored and processed in Europe because they belong in Europe.”⁸⁰ Yet, these messages directly contradict the message from DG Trade, which states, “Trade allows countries to procure the best products and services for its citizens internationally. This means government and local authorities can spend less public money on the products and services they purchase,” and “[t]rade makes it easier to exchange innovative or high-technology products.”⁸¹ Clearly Europe is talking out of both sides of

its mouth, promoting free trade so it can get access to foreign markets for its goods, while also protecting its markets when it comes to some sectors and technologies in which it is weaker.

It is even more galling that the EU is going in this direction given the very large trade surpluses it runs with the United States on virtually every manufactured product. As seen in figure 3, the EU runs significant trade surpluses with the United States on pharmaceuticals and medical devices, motor vehicles and parts, chemicals, electrical goods, and instruments. In 2019, the EU ran a trade surplus of \$153 billion with the United States, but a small trade deficit of around \$1.8 billion in the information/Internet services sector.

Figure 3: EU trade balance with the United States (\$billions)



Many have acknowledged the divergence between EU and U.S. digital policy interests, but usually without a fully accurate description of the source of the differences. EU officials like to cloak their precaution and protection in higher values. Marietje Schaake, a former MEP, called the EU digital policy system “values based” as opposed to the U.S. system, which many in the EU see as based on crass commercial interests and “radical individualism.”⁸² But this is misleading. It is not that the EU system is based on values and the U.S. system is based on greed. The U.S. system is deeply based on values: the values of innovation, progress, and growth. In contrast, the EU system is based on the values of stability and protection of incumbent interests.

As such, achieving a strong, working alliance with the EU against China is easier said than done. Many European officials actually believe that the digital threat from America is greater than the threat from China, and many believe that the condition for cooperation depends on the United States embracing the EU digital regulatory system.

The “UNCTAD South”: The Oppressed Seeking “Digital Alms”

While the United States and at least some in Europe see the central digital conflict between China and the West, many developing nations see the conflict as between “North and South,” with China part of the developing “South.” In this view, the North (developed nations in North America, Europe and Asia) have all the advantages and use them, including in digital

technologies, to hold back and exploit the less developed “South.” This is the updating of classic development dependency theory which held that the periphery South was being exploited and drained by the Center (North).⁸³ (This was certainly true when most of the nations were colonies; it is no longer true today.)

Many in the developing world, and the advocacy communities that support them, frame most digital issues, including data flows and use, through the lens of imperialism and even feudalism. In this narrative, these nations are helpless victims being exploited by digital imperialists. This is why the United Nations Commission on Trade and Development (UNCTAD) stated, “The only way for developing countries to exercise effective economic ‘ownership’ of and control over the data generated in their territories may be to restrict cross-border flows of important personal and community data.”⁸⁴ It went on to state, “With data becoming an increasingly valuable resource in the digital economy, there are questions about the wisdom of allowing foreign firms to extract data without restraint.”⁸⁵ *The Economist* agreed, writing that countries such as India want to “make sure that they do not risk becom[ing] mere sources of data, while having to pay for the digital intelligence produced.”⁸⁶ Renata Avilia, head of the Web Foundation wrote that “the world’s offline populations are the disputed territory of tech empires, because whoever gets them locked into their digital feudalism, holds the key to the future.”⁸⁷ Yale’s Michael Kwet warned, “Digital colonialism is threatening the Global South. It’s time to talk about Silicon Valley as an imperial force and what has to be done to resist its power.”⁸⁸

In fact, the opposite is true. Citizens of these nations receive the same free digital services as citizens in high-income nations, but their data is worth significantly less because their consumer spending is significantly less. Rather than being exploited, these nations are being cross-subsidized.

This North-South narrative is one of predatory imperialist digital juggernauts that scan the world to exploit underdeveloped nations. Case in point: UCNTADS’ claim that “Amazon... is set to provide Chile with cloud computing for local businesses, for the government, and for Chile’s world-leading telescopes. In return, it will receive not only a rent, but also access to key data that could be used to further improve AI and create new services.”⁸⁹ This is simply wrong. Neither Amazon nor other major cloud service providers get access to the data on their servers, and no one is forcing Chile to sign a contract with Amazon or any other U.S. company.⁹⁰

Indeed, this gives voice to many of these views in articulating a protectionist-based “digital industrial strategy” that essentially seeks to apply tried-and-failed import substitution policies to the digital economy. UNCTAD acts a “trade association” for developing nations to press their supposed grievances against developed nations, seeking whatever favors, concessions, and handouts they can get. For them, the lion’s share of IT and digital policy issues is framed in terms of inequality and the global digital divide. To be clear, the North, especially the United States, should do much more to help the South develop more effectively through IT and digital technologies, but not by supporting or turning a blind eye to South policies that harm growth and competitiveness in the North.

Perhaps of all the countries in the UNCTAD orbit, India is the most important when it comes to digital policy, simply because of its sheer size. India has embraced an array of policies that harm U.S. and global IT and digital interests. It introduced a forced localization scheme whereby companies that want to sell IT into India must produce locally. It has limited cross-border data

flows.⁹¹ It has limited access to Indian markets of foreign e-commerce firms. And it has proposed limiting foreign over-the-top video services.⁹² But at the same time, U.S. and Indian IT and digital firms are deeply interlinked, making cooperation between the two nations critical.

When it comes to digital technologies, many developing nations in addition to India want to structure markets and digital policies in ways that limit technological disruption and growth and distort trade. These include weakening IP rights, forced localization in exchange for market access, limiting cross-border data flows, and designing regulations to harm foreign IT and digital firms.

Policymakers in many developing countries are seduced by the misguided and costly fallacy that it is the location of data that matters (i.e., countries can best serve their economic interests by forcing firms to store data locally, a concept known as “data localization”) instead of focusing on the fundamentals of ICT adoption, education, digital infrastructure, and data governance policies, which are necessary to maximize the economic and societal benefits of data and digital technologies.⁹³ Data localization and other policies are often used to address the “digital divide”: the social and economic disadvantages that may result from a lack of access to technology. But a digital development strategy based on data localization and other restrictions will not help. In fact, such an approach is not only wrong, but harmful to a country’s economy and ability to support innovation, since it is likely to affect the price, availability, and range of ICT services. What should matter most for digital development is encouraging the widest possible adoption of digital technologies in an economy, the benefits of which far outweigh the much more limited gains from actually producing these technologies.

This North-South narrative is one of predatory imperialist digital juggernauts that scan the world to exploit underdeveloped nations.

These nations also prioritize small and medium-sized enterprises (SMEs) s, including micro-businesses and small illegal firms (“informal” firms), in part because they have few large firms, and because they believe that if they can convince policymakers of the importance of their SMEs, they can extract concessions from richer nations. They also stress local content requirements. For example, UNCTAD wrote: “Local content can be linked, for example to the domestic production of software in developing countries.”⁹⁴ And many side with their domestic telecommunications providers, often state-owned, to limit access to over-the-top Internet services such as Netflix and Skype, even though they’re not part of sectors that are actually central to global tech leadership (e.g., semiconductors). It’s simply because they’re providing competition to domestic firms.

Many also push for open source software, arguing that it is inherently superior to closed source. There is nothing wrong with using open source, but these decisions should be made by organizations involved, decided on the best value for money—not on United Nations (UN) or government dictates—and based on an unwillingness to pay for imports. Most also oppose IP protection, seeing it as solely designed to keep these countries from getting IP without paying, which they see as unfair, since these countries have lower incomes.

Unlike nations such as the Four Asian tigers and Europe that could advance even more in the digital economy with strong domestic policies to support innovation, this is much harder for most

emerging economies because they lack requisite skills, entrepreneurial talent, research universities, and digital infrastructures. As such, it is easier for them to blame the North and proffer a narrative of victimization and inequality. Rather than ask how new technologies can spur growth, UNCTAD's digital economy report asks, "How will the latest frontier technologies affect inequalities for developing countries?"⁹⁵ UNCTAD also advocates that large "Northern" firms are hobbled, writing, "Competition policies will need to be updated—and broadened to consider issues such as consumer privacy, personal data protection, consumer choice, market structure, switching costs and gender, between countries, race, income, class, patents."⁹⁶

The Unaligned: Going Forward With Heads Down

Many nations don't fall into these four groups. These are mostly middle- and upper-income countries that are too developed to be in the UNCTAD orbit and are not in the EU.

These include the Commonwealth nations of Australia, Canada, New Zealand, and the United Kingdom. These nations are for the most part not protectionist and seek to gain IT competitive advantage through legitimate means.⁹⁷ And of course, they are democracies. These countries should naturally align with the United States on most digital economy issues, especially digital governance, and may be willing to join with the United States to push back against China digital expansionism. These countries advocate IT and digital economic and trade policy that is generally driven by the recognition that they need to build economies of scale through an open and rules-based global digital economy (they do not have the internal market size of China or the United States). However, occasionally these nations emulate Europe in their own drive to push back against U.S. digital firms, often because of domestic political pressures from business interests that dislike foreign competition. For example, Australia has proposed legislation to require Internet providers to pay Australian news providers for linking to their sites.⁹⁸ Canada has proposed draconian privacy legislation that would subject firms to massive fines for even inadvertently not following the new rules.

Included in this group is also a set of Latin American countries. While some countries such as Venezuela are more in the authoritarian camp and others such as Brazil often align with the UNCTAD camp, many LatAM nations, particularly ones with more market-oriented policies such as Chile, Columbia, Costa Rica, Mexico and Peru, have started to build their own digital trade and economic framework (via the Pacific Alliance), which is similar to the U.S. approach.⁹⁹ However, more broadly, they remain unaligned, as many countries (such as Colombia) emulate European data privacy policies. Thus, the United States, the EU, and China are all engaged in trying to get them into their respective orbit.

None of the unaligned want to be attacked by China's aggressive "wolf warrior diplomacy" and aggressive trade and other economic sanctions. And they all want to keep being able to sell as much as possible to China and attract whatever state-directed investments that suit their interests.

Most countries in Africa, and the region via initiatives at the African Union, are at an early stage in enacting data protection, economic and trade, and other policies to account for the growing importance of data-driven innovation and trade. South Africa, Nigeria, and Kenya are home to emerging tech hubs. Policymakers in the latter two countries recognize the opportunity of embracing digital technologies, developing and attracting tech investment and talent, and

playing a part in global debates around data, including at the WTO.¹⁰⁰ However, many countries in Africa—most often led by South Africa—are in the UNCTAD camp and oppose efforts to negotiate new rules at the WTO on e-commerce and want to enact duties on digital transmissions. Many countries have also enacted restrictive measures.¹⁰¹ Regional discussions about building a digital economy agreement are therefore fractured by debates about what approach to take and whether to adapt policies from the U.S., EU, or China models.

Finally, there is a set of Asian nations that see China as a threat and are on an independent development path or are already developed. These include such nations as Indonesia, Japan, Malaysia, Philippines, South Korea, Taiwan, and Vietnam. None of these nations have an interest in seeing China become the sole power in the region. And all are threatened by Chinese IT and digital mercantilism. But at the same time, they have to live with China given how deeply intertwined they are economically, which leads to their legitimate fears of being singled out for retribution from Beijing.

Indeed, none of the unaligned want to be attacked by China’s aggressive “wolf warrior diplomacy” and aggressive trade and other economic sanctions. And they all want to keep being able to sell as much as possible to China and attract whatever state-directed investments that suit their interests. At the same time, they do not want to be too much in the orbit of China and risk becoming a client state, and in so doing lose the support of the United States. So most keep their head down and focus on domestic reforms and programs (often taking in foreign investment and assistance along the way), with the hope that both China and the United States do not force them to choose sides.

The Disruptors: Russia and Other Digital Scofflaws

Finally, there is a small group of nations, most importantly Russia, but also countries such as Turkey, Iran, North Korea, and Ukraine, that pose no real threat to U.S. technology leadership but do pose threats as systematic bad actors, sponsoring cyber-attacks, manipulating U.S. media and elections, hosting and distributing illegal digital content, and engaging in ransomware attacks or other financial crimes.¹⁰² This is not to say that other countries such as Brazil, Indonesia, and Vietnam do not also engage in malignant digital activity, or that China is not a widespread perpetrator of digital content theft.¹⁰³ Rather, it is to say that the main challenge from the disruptors is crime, rather than spreading their policy system around the world or taking global market share from firms in the United States.

UNDESIRABLE SCENARIOS

Rather than consider the U.S global digital strategy as binary—United States vs China—policymakers should recognize and act on its multifaceted nature. Before discussing the scenarios the U.S. government should work to achieve, this report first discusses scenarios that would be adverse to U.S. interests.

Scenario 1: EU “Regulatory Imperialism” Succeeds, and America Is Isolated

In this scenario, the United States either by commission or omission allows the EU model of digital governance to prevail in most parts of the world, other than China and digital bad-actor nations. By commission, the United States would support the right of the EU to enact stifling regulations and encourage companies around the world to adopt them, so they become the de facto rules. By omission, the United States does little to actively work with other nations to

educate and pressure them to adopt the U.S. innovation-based model of digital regulation. Either way, the United States is isolated, and its firms face a global digital economy—one that isn't based on open, rules-based competition and innovation, but rather on who can best manage multiple conflicting compliance regimes.

All nations want a globally competitive domestic economy. That is why most try to structure their regulatory systems in ways that protect key societal interests, such as public health, privacy, and the environment, but also that limit regulatory compliance costs. As noted, that is not the case in Europe. This is partly because powerful civil society groups exert disproportionate influence on policymakers, and also because Europe embraces the “precautionary principle.” The resulting regulatory system makes Europe's IT and digital industry less globally competitive.

The EU wants rules-based globalization so that it can have its cake and eat it too: restrictive, precautionary principle-based regulations and reasonably competitive industries.

To limit that relative disadvantage, Europe tries to get other nations to adopt its regulatory regime. To be sure, the European Union mostly uses the velvet glove of persuasion, including portraying themselves as the reasonable alternative to Chinese authoritarianism and U.S. “surveillance capitalism.” But it is not above using the iron fist of coercion by threatening trade restrictions as punishment. In other words, the EU wants rules-based globalization so that it can have its cake and eat it too: restrictive, precautionary principle-based regulations and reasonably competitive industries.

Big, powerful nations such as the United States and China can usually resist such pressure. But many other states are often faced with a stark choice: adopt EU-style regulations or face the risk of being shut out of the EU market. This is particularly problematic for nations that have fewer resources to invest in costly regulatory systems that are designed for advanced economies and have less economic leverage to push back against Europe. As one author noted:

The differences in power, wealth, capacity, interests and priorities between rules-exporting and -importing states globally are much starker than those dividing different EU member states ... the scattered and embryonic nature of the law and institutions of global risk governance gives far less protection to the relative losers of rules globalization.¹⁰⁴

European “regulatory imperialism” plays out in many digital technology regulatory areas, especially privacy. Europe's General Data Protection Regulation (GDPR) saddles its companies with strict privacy rules, making them less competitive.¹⁰⁵ For example, the right to explanation could reduce AI accuracy, the right to data erasure would harm AI systems, and the prohibition on repurposing data will limit AI innovation.

To compensate for these self-imposed limitations, the EU, in the words of former European Commissioner for Justice Věra Jourová, wants “to set the global [privacy] standard.” One way is to get other countries to adopt Convention 108, a Council of Europe treaty on privacy. The EU sees this as a stepping-stone for countries to commit to before getting closer to their own GDPR-style regulations. Non-Council of Europe states Argentina, Cabo Verde, Mauritius, Mexico, Morocco, Senegal, Tunisia, and Uruguay have already acceded to the treaty.

The EU's more direct means of conversion and coercion involve "adequacy" determinations. It negotiates with other countries about changes they need to make to their privacy regimes so they can be deemed compliant with the terms of Europe's GDPR and thus worthy of managing EU personal data. Over the course of 20-plus years, the European Commission has only granted adequacy to a small and disparate collection of 12 countries (mainly former colonies) that have achieved such adequacy determinations. But most nations have not. Without this, the EU forces firms to use other legal tools, which makes transfers of EU personal data much harder and costlier.¹⁰⁶

Using the same strategy and under the veil of the so-called "technological or digital sovereignty" as a cornerstone narrative, the European Commission is planning to roll out more regulatory frameworks in the next years to regulate technology companies and emerging technologies, including with rules specifically targeting the development and use of AI, the implementation of "European common data spaces" to increase control over industrial and personal data, and the business models of large technology companies.

Europe uses several strategies to export its regulatory systems to economic competitors. One is by relying on the so-called "California effect." This refers to the dynamic in the United States wherein California, the largest U.S. state (economically), often becomes the de facto regulatory standard setter because national companies find it easier to comply with just one regulatory framework—in this case California's. The EU relies on this dynamic on a global scale. It has been called "the Brussels effect" because it is the largest trading block in the world—when it sets stringent regulatory requirements, global companies often capitulate and design their products or processes to meet EU standards.

The EU also works actively with other nations on regulatory schemes. For example, the EU made the case in Colombia for a GDPR-style privacy bill. Exporting its regulatory standards clearly allows Europe to make up for the competitive deficiencies it has imposed on itself, but it couches its agenda in terms of human values, arguing that if countries truly care about their people, they should adopt the EU approach. A variant of this argument is that the EU is the civilized alternative to lawless American "cowboy capitalism." It also taps into underlying anti-American sentiments in many countries. Who wants to emulate the Yankees?

European leaders also argue other nations should emulate their regulatory system because it will make their economies more competitive. For example, when it comes to the GDPR, the EU sells a narrative that strong privacy rules are a source of **competitive advantage**. The reality is that by limiting the use of data, including for AI, the GDPR has actually hurt EU competitiveness, especially through high compliance costs and unnecessary restrictions on how firms can use data to drive innovation.¹⁰⁷ This is especially the case for small and medium-sized firms.

Finally, left-wing academics and civil society groups around the world press their case that the United States is a failed state that allows its companies to engage in rapacious behavior, and that the only globally just system is one based on EU social democratic values and regulations. In this narrative, any different or lesser regulatory protections for less-developed nations, at least in the digital space, are exploitative, if not racist. Often underlying their positions is broader, underlying anti-American sentiments.

So, in this scenario, Europe successfully convinces many nations to adopt its digital regulatory regime, including aggressive antitrust and digital service tax provisions. Not only does this increasingly isolate the United States—as when President Trump pulled out of the Paris Climate Accord—making it harder to prevail in global and regional forums; it weakens U.S. technology firms as they must face a much more restrictive regulatory and tax regime around the world.

Scenario 2: Anti-tech Forces Turn America Into the EU and China Prevails

In this scenario, the United States voluntarily adopts the EU approach to digital governance and loses IT and digital competitiveness, with the requisite implications for U.S. competitiveness and national security, and Chinese firms becoming dominant globally.

While the EU has doubled down on the precautionary principle and protectionism backed by a disdain of GAFA (Google, Amazon, Facebook, and Apple), the United States has rightly resisted going down that path because it would significantly reduce U.S. digital innovation and competitiveness.¹⁰⁸

But recently an elite-based “techlash” has led to growing calls for the United States to emulate Europe. Indeed, the techlash manifests itself not only as calls for precautionary-based tech policies, but active antipathy toward technological innovation and big tech firms.¹⁰⁹ We see this with calls to break up big tech companies, require “big tech” to pay users for their data, eliminate Section 230 protections, impose strict privacy regulations, heavily regulate or even ban emerging technologies, tax IT technologies, and move to government provision of broadband services.¹¹⁰

Indeed, a growing chorus of anti-tech voices pound the drum for becoming Europe, rejecting concerns that this could weaken the United States vis-à-vis China. Indeed, across the political spectrum, these critics sound shrill alarms of gloom and doom. Liberal icon Robert Reich has said big tech has become “way too powerful.”¹¹¹ Robert VerBruggen, writing for the conservative *National Review*, called Google, Facebook, and Amazon, “Our Digital Overlords.”¹¹² And the bipartisan pairing of Bill Galston, a center-left thinker who helped shape President Clinton’s domestic agenda, and Bill Kristol, the center-right thinker and veteran of the first Bush administration, formed a new group with a reform platform that includes “Challenging the Tech Titans.”¹¹³

Such views are increasingly mainstream, especially on the left. Dan Gillmor, cofounder of the News Co/Lab at Arizona State University, commented, “Governments (and their corporate partners) are broadly using technology to create a surveillance state, and what amounts to law by unaccountable black-box algorithm, far beyond anything Orwell imagined.”¹¹⁴ Andrew Nachison, of the National Community Reinvestment Coalition, said that the “[d]ominance of digital overlords is devastating to journalism, small businesses, and governance.”¹¹⁵ Internet critic Shoshana Zuboff warned:

Right now we have two versions of the Internet—a market-led capitalist version based on surveillance, which is exploitative; and an authoritarian version also based on surveillance... The question is: will Europe and North America pull together to construct the legal and technological frameworks for a democratic alternative?¹¹⁶

Robert Kuttner, a liberal economic commentator who during the Japan challenge of the 1980s advocated for a strong U.S. economy, including in advanced technology, now argues for embracing the EU model:

Will Amazon, Google, and Facebook, the most powerful global corporations in the history of the world, continue to have their way with us, using trade law as a means of constraining domestic regulation? Or will the U.S. and the EU join forces to add some rules on privacy, transparency, competition, and some liability for abuses?¹¹⁷

Indeed, it is now almost a requirement of membership in elite circles, particularly left-of-center, to disdain technology and technology companies, ascribing to them a host of wrongs from climate change to joblessness to democratic deficits to low wage growth and excess profits.

And virtually no claim about the malevolence of tech companies or the injury being caused by tech is now too outlandish to generate considerable attention—from killer AI that will enslave the human race, as Elon Musk has asserted, to maps on smartphones leading to early onset of Alzheimer's.¹¹⁸ Virtually any and all negative claims are now routinely asserted and then widely circulated as truth, repeated at TED talks, online, and elsewhere, much like other urban myths have spread.

It is now almost a requirement of membership in elite circles, particularly left-of-center, to disdain technology and technology companies, ascribing to them a host of wrongs from climate change to joblessness to democratic deficits to low wage growth and excess profits.

And these voices are reinforced by tens of thousands of academics, activists, pundits, civil society groups, media figures, and public officials throughout much of the world. For them, these issues are no longer even up for debate, for “we all know x” (e.g., AI is biased, tech kills jobs, privacy is a fundamental human right, etc.). And these ideas often prevail because they are framed in value-based terms that appeal to people’s emotions (human rights, autonomy, privacy, fairness, etc.) and where the alternative is about corporate profits and corrupt government actors, not broad-based innovation.

But it’s not just that these voices seek to limit innovation, they seek to both limit market-based economics and develop alternatives. In this growing narrative from the left, it is the very nature of capitalism that generates these harms: racial injustice, gender bias, environmental degradation, steep inequality, job loss from technology, crass materialism, lack of privacy, concentrated political power, and more. In this framing, it is markets and businesses (especially large ones) themselves that are the problem, and solutions should respond to that, embracing at least soft forms of socialism.

It is easy to dismiss these claims as the rants of a few out-of-control TED talkers, but in fact, ideas matter. In this case, this overarching anti-innovation, anti-tech, and even anti-capitalist narrative is influencing legislation at all levels of U.S. government.

Moreover, an additional force that could move the United States in this direction is the view that the China challenge is so paramount that the United States must do anything to get Europe on its side, including emulating European digital governance. For example, *The Economist* called for the United States to “recognize European privacy and other regulatory concerns as well as

demands that the tech titans be property taxed.”¹¹⁹ In exchange, the EU would then supposedly help the United States with China. *Financial Times* columnist Rana Foroohar argued that a stronger EU-U.S. alliance is critical, and that the Biden administration adopt EU tax, regulatory, and anti-trust approaches to the tech sector so that the EU will cooperate with America.¹²⁰ Indeed, there will be considerable pressure on the Biden administration to “give away the store” to Europe under the motto of “America is back.” But adopting the EU model lock, stock, and barrel would significantly weaken the U.S. tech economy. Moreover, there is no evidence that the EU would then live up to its side of the bargain.

There will be considerable pressure on the Biden administration to “give away the store” to Europe under the motto of “America is back.” But adopting the EU model would significantly weaken the U.S. tech economy.

This is not to say that the United States should not move somewhat closer to the EU position on some issues. But this should be step by step, a careful weighing up of the pros and cons of each potential policy proposal (considering *all* rights and interests, not just privacy); not a headlong rush to copy and paste whatever the EU does. For example, Congress should pass a national privacy bill, but not one based on the GDPR. The administration should continue to ensure that antitrust authorities monitor and prosecute anticompetitive behavior (as opposed to focusing on industry structure) while maintaining a commitment to the consumer welfare standard. And it should support international tax reform to limit tax havens.¹²¹

Scenario 3: The EU Won't Budge

Ideally, the United States and EU would recognize they share more in common than they often care to admit—even when it involves contentious issues—and their shared values stand in stark contrast to Chinese innovation mercantilism and digital authoritarianism. Thus, they realize the best approach is to cooperate in a pragmatic and cooperative manner in order to establish a shared approach to China, while also each giving a little in order to cooperate in establishing global digital norms. But in this scenario the EU is unwilling to make reasonable compromises. Its political leaders have put themselves out on a limb of “digital sovereignty” they cannot crawl back from. Anti-American and anti-tech forces, including in government, business, and “civil society,” are too strong. And the lure of hefty yuan profits from China is too high for EU businesses not to pressure their governments to capitulate.

If this scenario prevails, the United States will need to play hardball. If the EU will not allow data flows to the United States because they don't trust our law enforcement and intelligence services, then the United States should make it clear that it will limit intelligence sharing, as well as prohibit EU firms in America from moving data on American persons to Europe. If it insists on imposing digital services taxes on U.S. firms, the United States should make it clear that it will retaliate, by either imposing similar taxes on EU firms doing business in the United States or levying tariffs on imports from the EU. It should also make it clear to the EU that it's America's defense spending that lets EU nations spend relatively little on defense themselves, and that this support comes with the price of reasonable cooperation: not attacking U.S. tech firms and cooperating to push back against unfair Chinese technology practices.

Scenario 4: Nations Craft a “Digital WTO”

Often, international cooperation and governance regimes don’t emerge until several decades after the initial commercialization of a technology. Samuel Morse electrically transmitted his famous message, "What hath God wrought?" from Washington, D.C., to Baltimore on May 24, 1844, but it was not until 1865 that the First International Telegraphy Conference was held in Paris that led to the signing of the first International Telegraph Convention establishing the basic principle of cross-border telegraphy.¹²² Sometimes the process is faster. Marconi first broadcast his radio signal across the English Channel in 1899, and the First Radiotelegraph Convention was held in Berlin in 1906.¹²³ And after Russia launched Sputnik in 1957, a UN space treaty had been signed by 1967.

Today, after the Internet was developed in the 1960s and reached commercial application by the mid-1990s, we still don’t have an equivalent global Internet treaty. But this is largely because unlike prior technologies wherein government was much more directly involved (in many nations, governments ran the communications networks), the Internet is more decentralized (a network of networks governed by technical protocols) and managed by bottom-up, industry-led consensus bodies such as the ICANN and the Internet Governance Forum.

Nonetheless, an increasingly popular solution to cross-border digital policy conflicts and tensions is to create some kind of supra-national body to address international digital policy issues. In this scenario, the United States spends its scarce political capital to help establish such an organization.

These supranational proposals take a variety of forms. For example, Ian Bremmer wrote that the United States should support the creation of a “World Data Organization” akin to a WTO. In this proposal:

A secretariat would be established to help member states create a universal set of digital norms that can be adopted by the group (with a particular focus on artificial intelligence, privacy, intellectual property, citizens' rights, and data) alongside an enforcement mechanism to help mediate any potential disagreements between parties.¹²⁴

Others have made vaguer calls for some kind of global governance of digital technologies, particularly AI. AI scientist Andrew Murray stated:

We need international cooperation on the standards of regulation. We need a UN body—an international telecommunications union for AI or a body similar to that. We need a global standard-setting body. Otherwise, what will happen is that in the commercial battlefield, the US and China will get involved in a battle to become the world market leader in AI. If we don’t have international standards, governments will develop the standard that is most beneficial to their industry sector and not most beneficial to us.¹²⁵

Others support international agreements on the use of particular technologies. Cohen and Fontaine wrote, “The leading democracies have yet to agree on rules for using **facial recognition technology**, including its proper role in the criminal justice system, or the protocols that should govern data collection.”¹²⁶

There are multiple problems with these proposed governance frameworks. First, to the extent that digital policy issues involve trade (either “at the border” or “behind the border” issues), we

already have the WTO. It makes no sense to create a new separate organization just for IT and digital issues. Where needed, countries should use the WTO to develop rules to better address e-commerce and digital issues.¹²⁷ China and Russia are 2 of the 70-plus countries taking part in ongoing WTO e-commerce negotiations; however, they do not necessarily need to be there at the end. In fact, if an ambitious outcome is possible, the United States should actively push them out if they refuse to take on the same ambitious outcomes as everyone else, especially on cross-border data flows.¹²⁸

Second, any global organization that lets China in would no longer be able to advance many commonly accepted values, such as rule of law, but any organization without China would not be global.

Third, many IT and digital policy issues reflect deeply held views and values of particular nations. The EU, for instance, does not have the same commitment to freedom of speech as the United States does. For example, online access to *Mein Kampf* is blocked in Germany but not in the United States. If there are global rules, which rules apply to such speech?¹²⁹

A global governance body, especially one tied to the UN, would be even more problematic than the EU model becoming dominant because it might tie the United States to agreements that are neither in its nor the world's best interest.

Moreover, there is no reason why nations should not have different regulatory regimes for digital issues, as long as they are not de facto trade barriers. After all, Europe and the United States are unlikely to agree on a privacy framework or how to regulate AI. And if nations are worried that digital imports won't reflect their domestic regulatory framework, they can block them at the border, as the WTO allows (as long as the restrictions are not hidden protectionism). In other words, the idea that without a global agreement, that bad, rapacious AI would flood into nations is nonsense. Bad, rapacious, unsafe cars don't flood into Europe now because EU enforces product standards on imports. It can do the same thing on digital technologies, as long as they are not de facto trade barriers.

In addition, countries already regulate technologies differently. There is no reason why digital technologies should be any different. For example, there is nothing special about facial recognition technologies that suggests governance should be elevated to the international level. In some nations, local and regional governments will regulate it. In others, it will be regulated at the national level. Some nations may ban it. Others may encourage its use, but with appropriate guidelines and protections. Still other governments will abuse the technology. There is no need, or ability, for a global solution to this kind of issue.

A global governance body, especially one tied to the UN, would be even more problematic than the EU model becoming dominant because it might tie the United States to agreements that are neither in its nor the world's best interest, such as banning AI-enabled autonomous weapons systems.¹³⁰ Such a body could easily fall into the standard reflexive thinking that privacy is a fundamental human right, large companies are bad, AI is inherently biased, people have a right to own their data, and so on. Indeed, as a report from the Stanford Cyber Policy Institutes states:

A large and globally-based democratic coalition could offer a meaningful alternative to the two existing models of technology governance—the privatized corporate model and the authoritarian state model. This effort should involve countries that meet democratic standards, and could include an ambitious mandate for the governance of powerful technology behemoths.¹³¹

This kind of scenario is decidedly against both U.S. and global interests in expanding innovation.

Scenario 5: China Wins the Minds (if not the Hearts) of UNCTAD-Nations

In this scenario, China brings a large share of the developing world into its orbit, gaining market share at the expense of the United States, and increasingly isolating the United States internationally.

In the Cold War, the United States competed with the Soviet Union for influence in the “third world.” A similar competition is raging today, but with a much more challenging adversary. China has provided large amounts of money for its Belt and Road Initiative, including to UNCTAD and EU-10 nations, tying it to mandated purchases from Chinese technology companies and the use of Chinese technology applications, such as Baidu, Alibaba, and Tencent. Recently, China has ratcheted up its efforts to train foreign politicians to emulate China’s approach, which Xi Jinping has called a “new option” for these countries, and that the “Chinese approach” would address major global challenges.¹³²

China also keeps countries in line by visibly and forcefully punishing nations for taking actions to side with the West, including by cutting off their imports to China. China’s punitive blocking of Australian imports is indicative of how it is happy to use trade as a weapon against countries it sees as acting against its political interests.¹³³ This sends a clear message to developing nations that while displeasing the United States might result in a diplomatic memo, displeasing China results in real pain.

If American capitalism can be defined as the problem, then Chinese authoritarian communism doesn’t look so bad.

In addition, the United States continues to withdraw from its role internationally, including continuing to underinvest in foreign assistance and instead investing in antiquated technology (not in IT and digital tech, backed by clear and effective digital aid strategies). In addition, left-wing academics and civil society groups from around the world continue to press the narrative that it is capitalism, and the United States and its “big tech” companies in particular, that are the real threat to developing nations—and that they should adopt policies to limit U.S. market access. If American capitalism can be defined as the problem, then Chinese authoritarian communism doesn’t look so bad.

As such, in this scenario, a large share of developing and moderate-income nations not only are tied into the China trade and economic orbit, but they also essentially become Chinese client states at international bodies such as the WTO, the World Intellectual Property Organization (WIPO), and the International Telecommunication Union (ITU), doing China’s bidding to the detriment of the United States and its allies.

Scenario 6: The Splinternet Emerges

In this scenario, Russia or China decides to splinter the Internet at both the policy and technical architecture level. In other words, one of them takes radical steps to separate its Internet from the global Internet. This is a scenario that is widely touted as not only possible, but even already in progress.¹³⁴ In it, nations either wall off the outside Internet through blocking, or design a separate Internet architecture that doesn't interoperate with their current global ones. For example, some have described China's Internet as being similar to a gigantic intranet, such that China-to-China Internet traffic never leaves the country, never mind the fact that it has a few (state-controlled) connection points to the global Internet.¹³⁵ This has long been a fear of cyber-exceptionalists who deny any role of government in "cyberspace."¹³⁶

While such a scenario would be bad for U.S. interests, it would be worse for the nations practicing it. No nation can function without access to the global Internet. Any nation that tried would very quickly find out the costs. This is one reason why it is not likely to happen, at least not on a wide scale.¹³⁷ Most of the warnings refer to the practice of some countries of blocking certain websites for political reasons. This is quite different than a splintered or separate Internet architecture or widespread Internet blocking.

Moreover, by cyber-exceptionalist standards, every country embraces the Splinternet because every country makes some Internet content, such as child pornography and pirated copyright materials, illegal. The practice of authoritarian nations to limit access to certain websites and web pages does not constitute the breaking of the Internet. Nor does all website blocking constitute a threat to the open Internet.

Scenario 7: The United States Spends Much of Its Political Capital on Promoting the Open Global Internet

In this scenario, the United States focuses most of its political capital on ensuring an "open Internet." This is a popular position among many left-of-center globalists. In 2016, former State Department official Anne-Marie Slaughter wrote:

The next U.S. president should adopt a grand strategy of building and maintaining an open international order based on three pillars: open societies, open governments, and an open international system. The essential fault line of the digital age is not between capitalism and communism or democracy and autocracy but between open and closed. Alec Ross, a technology expert and former State Department official, lines up countries on an "open-closed axis." As he argues, "the societies that embrace openness will be those that compete and succeed most effectively."¹³⁸

These views are grounded in an ideology that generates a simplistic mantra: open, good; closed, bad.¹³⁹ In fact, closed systems can succeed, as we see with China. And in many cases, for example in the Apple ecosystem, more closed systems can provide great value for consumers.

The principal problem with openness as the central organizing principle for U.S. global digital policy is that it puts the United States in a position of sacrificing key national interests in exchange for promoting the global good. Yes, a globally open Internet would be good for the world. But why is it the United States' responsibility to convince other nations of that, especially if by doing so it ignores or downplays other foreign actions that harm key U.S. interests?

Case in point is the Obama administration's Open Government Partnership (OGP), which started with seven other countries: Brazil, Indonesia, Mexico, Norway, the Philippines, South Africa, and the United Kingdom, and has grown to 78 nations.¹⁴⁰ According to Slaughter, "[A]ll participants must sign the Open Government Declaration, a set of principles that they pledge to implement through a national action plan."¹⁴¹ But the Obama administration did not require membership in this agreement to mean eschewing digital policies harmful to global trade and U.S. interests. Case in point: OGP member Indonesia, which enacted both a broad, vague, and discriminatory regulatory framework for OTT Internet-based services, including forcing firms to set up a local office, hire local staff, produce local annual reports, and store data locally and changes that allow it to enact tariffs on imports of digital products, such as downloads of movies, e-books, and software.¹⁴² As long as they don't block some websites, presumably a country can be in OGP, regardless of how harmful its other policies are to U.S. and global IT and digital interests.

The principal problem with openness as the central organizing principle for U.S. global digital policy is that it puts the United States in a position of sacrificing key national interests in exchange for promoting the global good.

Moreover, the globalist view is often accompanied with the opposite view when it comes to industrial policies. As long as governments have an open Internet, the view goes, it's okay for them to seek economic protectionist-based autonomy. As Slaughter wrote, "Washington should of course recognize its allies' desire for autonomy ... Paradoxically, strengthening Asian and European competitors in American-dominated industries will advance long-term U.S. interests."¹⁴³ There is no paradox here because this view is incorrect. Strengthening American competitors weakens U.S. industry, U.S. workers, and U.S. national interests.

Another problem with the "openness" agenda is that it moves the U.S. system toward an EU one, as its advocates largely support a host of anti-innovation policies such breaking up large technology companies; embracing restrictive digital regulations, including mandating that companies pay people for their data (which would mean the end of free digital services for lower-income consumers); and encouraging government provision of what are now mostly private-sector-provided IT and digital services.¹⁴⁴ To the extent the U.S. government focuses on the Internet's freedom, it should be as part of an overall human rights and free speech strategy, not the defining lens it uses to engage in IT and digital issues.

AN ACTION AGENDA FOR DESIRABLE SCENARIOS

These scenarios are all ones the U.S. government should either actively work against or avoid supporting. However, that does not mean incrementalism and "fighting fires" is the proper alternative response. It is time for the U.S. government to develop and implement a grand strategy for the global IT and digital economy that is realistic and pragmatic in recognizing how countries enact digital policies and is most likely to appeal to a broad and diverse range of countries—while putting U.S. national interests at the forefront. Failure to do so will risk having the United States surrounded by a host of technology competitors, and in some cases, such as with China and Russia, adversaries, which will lead to diminished U.S. technological, economic, political, and military leadership.

For too long, the United States has either had abstract, ideological strategies such as promoting an open global Internet, or responded piecemeal, fighting each fire as it breaks out. And in both kinds of engagement, it has worked to change hearts and minds by trying to persuade other nations of the superiority of the U.S. system. That might have had some purchase in the 1990s and 2000s when the United States was the early leader in the digital revolution and before the rise of large, global U.S. tech firms. But education and persuasion, while needed, are no longer enough. EU officials, for example, mostly understand the arguments U.S. officials make—they just either don't agree with them or their politics won't allow them to act on them. This is even more true in China, where for years the U.S. approach was to “educate” Chinese officials on the merits of the U.S. system. China didn't need education. They fully knew they were “cheating” and what the United States did not like. It needed pressure and pain.

It is time for the U.S. government to develop and implement a grand strategy for the global IT and digital economy that is realistic and pragmatic in recognizing how countries enact digital policies and is most likely to appeal to a broad and diverse range of countries—while putting U.S. national interests at the forefront.

As such, the U.S. government needs to understand that the major global IT and digital challenges it faces stem not from ignorance, but from ideology and interests. As such, here are four scenarios the U.S. government should work to achieve in the immediate and moderate term.

Scenario 8: U.S., EU, and Non-aligned Nations Isolate, Punish, and Defend Against “Scofflaws”

In this scenario, the United States, EU, most non-aligned nations, and some developing nations work together to respond to digital scofflaws such as Russia. Currently, nations that are havens for or active participants in cyber-attacks, cybercrime, digital piracy, counterfeiting, and other digital misbehavior face few consequences globally. In many cases, law-abiding nations not only turn a blind eye, but actually reward these nations. For example, in 2020, Algeria, Indonesia, and Ukraine were not only the United States Trade Representative (USTR) Special 301 Priority Watch List for IP violations, but they also enjoyed tariff-free access to U.S. markets on the Generalized System of Preferences program.¹⁴⁵ Australia, Japan, New Zealand, and Switzerland also provide Algeria and Saudi Arabia (on the 301 list) with Generalized System of Preferences (GSP) benefits.¹⁴⁶ The EU provides GSP benefits to India and Indonesia, both of which are on the 301 watch list.

In this scenario, the United States, EU, and allies would agree on which nations qualify as digital scofflaws and use a variety of means to impose consequences until their behavior changes, including ending state-sponsored attacks and taking meaningful action to crack down on private sector digital crime, including digital piracy. These steps would include not only cutting off tariff-free access but imposing additional tariffs on certain classes of final goods (tariffs on intermediate goods can hurt domestic producers). In addition, these nations would cooperate more on cyber-deterrence, identifying and limiting cyber-attacks, and agreeing on when cyber-retaliation is allowed.

Scenario 9: The United States Forms an Anglo-American (and Friends) Alliance

In this scenario, the United States and the EU cannot come to a compromise over digital policy because the EU wants to persist in its IT and digital protectionism and “have its cake and eat it too” when it comes to China (e.g., wanting the United States to engage in the hard and painful work of pushing back against Chinese mercantilism, while the EU enjoys even better access to Chinese markets).

However, Commonwealth nations, especially the United Kingdom and Australia, become increasingly concerned with and frustrated over China and its IT and digital mercantilism and “wolf warrior” diplomacy. In this scenario, the benefits of the United Kingdom leaving the EU outweigh the negatives (less UK influence in the EU to temper its regulatory and anti-U.S. excesses), as it is now free to move closer to the more innovation-inducing U.S. system. In such an alliance, the United States, United Kingdom, Australia, and other members of the “five eyes” intelligence partnership formally add a digital trade component to their cooperation. They formalize an agreement to enable unrestricted cross-border data flows within the group, eschew digital services taxes, fight piracy, and limit other innovation-damaging regulatory actions. In addition, they work more cooperatively on a joint advanced technology strategy to help support advanced tech firms competing against Chinese champions backed unfairly by the Chinese government. As this alliance is established and strengthened, members jointly and selectively invite in new members. It will be particularly important to strengthen relations with selected Northeast (e.g., Japan and Taiwan) and Southeast Asian nations (e.g., Singapore) which tend to place more focus on driving digital innovation and competitiveness, which makes them more skeptical of embracing the EU-style precautionary principles approach.

Scenario 10: EU, United States, and Non-aligned Nations Cooperate Against China

The United States is faced with three possible areas of actions vis-à-vis China: cooperation, resistance, and confrontation.

Many Washington thought leaders stress cooperation. They argue that the United States will need to increasingly cooperate on issues such as climate and health. This is a dangerous view as doing so would divert U.S. actions away from confronting China on IT and digital issues (and overall economic issues). The United States should not go hat in hand to Beijing for help on climate change for two reasons. First, China has a much higher stake in addressing climate change than does the United States, and has every motivation to address it. Second, it fundamentally doesn't matter what any nation does to control climate change; what matters is how fast clean energy innovation progresses so that every nation, firm, and consumer voluntarily wants to adopt it. And on this measure, Chinese innovation mercantilist policies have harmed clean energy product innovation in areas such as solar panels and, likely, batteries.¹⁴⁷

In the resistance scenario, the United States invests political capital to fight for human rights and democracy in China. To be sure, these issues are extremely problematic, but are fundamentally not U.S. issues alone.¹⁴⁸ First, it will be extremely difficult to change Chinese policies in this area. What is most likely is diplomatic relations with Beijing will deteriorate, but little else will happen. Second, if pressing China on human rights involves limiting U.S. exports to China in order to “punish” China for its behavior, the only result will be to hurt U.S. firms while helping Chinese firms. China is not a small dependent nation that cannot afford to alienate

the United States. Third, to the extent U.S. policymakers focus on human rights in China, it will weaken U.S. ability to advance its core technology and economic interests vis-à-vis China.¹⁴⁹

Many argue that the United States will need to cooperate with China on issues such as climate and health. This is a dangerous view as doing so would divert U.S. actions away from confronting China on IT and digital issues.

This gets us to confrontation. If the EU and United States are willing to compromise on key IT and digital policy issues, and if the EU is willing to join the United States in standing up against Chinese economic predation, then ideally the United States, EU, Commonwealth nations, and other non-aligned nations would formally cooperate against Chinese economic predation with the goal of limiting damage to their interests, while at the same time slowing Chinese technological advance.

This is the optimal solution that many support. For example, Cohen and Fontaine wrote:

This new grouping of leading “techno-democracies”—call it the T-12, given the logical list of members—would help democracies regain the initiative in global technology competition. It would allow them to promote their preferred norms and values around the use of emerging technologies and preserve their competitive advantage in key areas. Above all, it would help coordinate a unified response to a chief threat to the global order.¹⁵⁰

Council on Foreign Relations scholar Robert Knake proposed something similar, writing that we need a digital trade zone that, if it “grows strong enough, China might see more benefit to cooperative engagement than continued disruptive behavior.”¹⁵¹

However, there should be no illusion that this is simply some kind of free-trading club that China will make some modest compromises to join. Even if the United States led such an agreement, with China’s own Regional Comprehensive Economic Partnership (RCEP), it hardly needs to be inside U.S.-led agreements. In addition, such an alliance would require imposition of real consequences for Chinese IT and digital mercantilism.

In addition, it will require some EU nations, especially Germany, to look beyond their short-term interests of having access to the Chinese market, especially in cars. Europe needs to understand that the market access its companies salivate over now is only likely short term in nature. In autos, for example, it is only a matter of time before Chinese car makers dominate the Chinese market and China shuts out foreign producers and starts to expand overseas. Embracing docility in hopes of Chinese favors is not only selfish, as it harms the rest of the non-Chinese world, it is shortsighted. The EU claims to be working for all of humanity when it makes sacrifices for climate change; but when it comes to working for all of humanity to support freedom, democracy, and global innovation by working to push back against Chinese innovation mercantilism, Europe looks to its pocketbook and commercial advantage over the United States.

Such an agreement would also mean the United States and the EU both complying with the WTO ruling on Airbus and Boeing. And it would mean the United States ending EU steel tariffs. In addition, both parties would seek to establish real substantive transatlantic digital dialogues. As part of this, EU officials would dial back its “digital autonomy” talk, which only fans the flames of IT and digital protectionism, and roll back its “war on U.S. big tech.”

Under such an alliance, the countries would cooperate in a host of areas both related to China and for broader IT and digital policy cooperation. For the former, this should include 5G equipment and systems, Chinese investment screening, joint WTO cases against China, cooperation on cyber-hacking and other IP theft, supply-chain cooperation, reciprocal advanced technology strategy and program cooperation, joint blocking of Chinese imports when massive subsidies or IP theft or coercion are involved, cooperative export controls, and cooperation in international forums related to the digital economy.

For the latter, it could include cooperation on a shared and common approach to AI-based data mining, principles and procedures for government access to personal data (including that there be an independent judiciary involved), commitments to cross-border data flows, and others areas.

In addition, these nations should formally agree to come to each other's economic aid against China by forming the Democratically Allied Trade Organization (DATO). This organization would be governed by a council of participating countries, and if any member were threatened or attacked unjustly with trade measures that inflict economic harm, DATO would quickly convene and consider whether to take joint action to defend the member nation. DATO nations should cooperate to deter individual episodes of Chinese economic aggression against individual members and provide a mutual defense umbrella against broad Chinese policies that harm all nations—particularly mercantilist policies such as the “Made in China 2025” initiative.¹⁵²

The U.S. government should seek multilateralism that advances U.S. interests (and the interests of global IT and digital innovation). This is not easily accomplished and should be pursued thoughtfully.

However, the key is for the United States to “not give away the store” just to get other nations to cooperate. Indeed, some argue that the only way to form such an alliance is for the United States to compromise with Europe on a whole set of digital policy issues, such as the right to be forgotten, digital service taxes, antitrust, privacy, and AI regulation. As *The Economist* wrote, “A connected America cemented into the rest of the world by means of a grand techno-political bargain could be the hub of something truly unsurpassable.”¹⁵³ This way, Europe would support the United States in other forums, such as standard-setting bodies, and would help push back against China.

But the risk is that the United States compromises so much that it reverts to scenario 2 wherein the U.S. system no longer effectively supports digital innovation. Multilateralism for multilateralism's sake risks being a diversion from advancing U.S. national interests. Rather, the U.S. government should seek multilateralism that advances U.S. interests (and the interests of global IT and digital innovation). This is not easily accomplished and should be pursued thoughtfully.

Fortunately, it appears the EU may be leaning toward a reasonable compromise solution. The European Commission and the EU foreign affairs services have released a joint statement proposing an EU-U.S. agenda, calling for more cooperation on cybersecurity and digital trade, a push for democratic values in the online world, and unified positions on issues such as digital taxation, “Big Tech,” and the protection of critical technologies.¹⁵⁴ The EU's intent is also to reinforce regulatory ties with the United States, including by creating an EU-U.S. Trade and

Technology Council (TTC) that would coordinate common positions and foster transatlantic trade, in addition to a Transatlantic AI Alliance.

If American policymakers expect the EU to compromise, it is only reasonable that the United States does as well. This could start with Congress passing a privacy bill. Such a bill would give consumers reasonable privacy rights, and would also preempt state and local regulations, ban private rights of action, and give consumers an opt-out—not opt-in—right.¹⁵⁵ On digital tax issues, the administration should continue to work with the Organization for Economic Cooperation and Development (OECD) to ensure all companies pay reasonable taxes and cannot unreasonably shelter income in tax havens. But that does not mean that just because a company sells services in a nation, even digital services, that country should be able to receive taxes from the company. There is no logical basis for having digital profits go to where customers live any more than there is to say that an automobile company's profits should go to the jurisdictions wherein car customers live. Both should also agree to encourage responsible AI without harmful bias.

Finally, the U.S. government should ensure that when it supports international organizations and outside policy groups, these organizations largely embrace the U.S. approach to digital policy and governance, rather than the EU and Internet regulatory approach. Unfortunately, the U.S. government has not always done that, in essence funding organizations that weaken, rather than strengthen, U.S. interests.¹⁵⁶

Scenario 11: The United States Approach Prevails in Developing Markets

Over the next several decades, the fastest growing digital markets will be in developing economies.¹⁵⁷ It is of vital U.S. interest that these nations adopt an open, rules-based digital economy (as many countries have done at the WTO for physical goods), integrate more closely with U.S. firms and technologies, and adopt attitudes and policies toward the digital economy more aligned with the United States than with China (or the EU, for that matter).

In this scenario, a growing number of nations become fed up with China's bullying, negative-sum approach to trade and predatory lending deals. They also begin to think twice about adopting the EU digital regulatory system as they see the negative impacts on countries that embrace that model. Furthermore, given the compromises by both the EU and United States, some points of conflict have been resolved, thus reducing the clear competition between the two models.

A strong IT and digital partnership between India and the United States will be a powerful tool to ensure democracies stay ahead of China.

At the same time, the United States significantly ramps up its efforts to be engaged with developing markets, including by expanding digital-technology-oriented aid through bodies such as US Agency for International Development and the Millennium Challenge Corporation. Congress also expands funding for the International Finance Development Corporation and funding for state and Commerce Department engagement with developing nations, including expanding the digital attachés program.¹⁵⁸ Equally importantly, U.S. aid and other support, including through organizations such as the World Bank and InterAmerican Development Bank, should be contingent on nations limiting their digital protectionist policies and programs, such as data export restrictions, IP theft, and forced localization of production.

The U.S. government should place a particular focus on Latin America as many LatAM nations are focusing on how to grow their economies through digital technologies, and many LatAM economies are already deeply integrated with the U.S. economy and U.S. technology firms. In addition, India should be a key priority. While the conventional wisdom holds that India and China are adversaries, it would pose a massive risk if they became collaborators, for India has key strengths in software and IT services, while China has growing strengths in hardware. Together, that could be an unbeatable combination. The reverse is also true. A strong IT and digital partnership between India and the United States will be a powerful tool to ensure democracies stay ahead of China.

PRINCIPLES FOR A NEW REALPOLITIK DOCTRINE IN U.S. GLOBAL DIGITAL POLICY

For the past decade or so, a major part of the U.S. challenge in discussing, advocating, and negotiating internationally in this area is U.S. officials do not have an easy-to-translate model of digital governance and associated set of talking points. What does the United States want (besides everything), and what are its major priorities—open markets, human rights, the freedom to innovate, privacy, national security, jobs, a more economically integrated world, a more peaceful world?

For many years, U.S. officials believed in and advocated for open markets, international trade, less regulation, greater economic integration, and the rule of law because they thought those would benefit both the United States and the world. That basic framing may have worked before China became a systemic competitor/adversary, Russia and several other states became systemic bad actors, and the EU and many developing states embraced digital protectionism.

As such, going forward, the United States needs a revised and clear set of principles that together articulate a new doctrine of digital realpolitik to orient its global digital policy. These are both at the same time principles for guiding U.S. action and talking points to communicate to allies and non-aligned nations.

Principle 1: Unabashedly Support IT and Digital Innovation, Rejecting the Techlash Narrative and Policies

This may seem obvious, but it is anything but. China's goal is not innovation; it is global power. Europe's goal is not principally innovation; it is ensuring that IT and digital technologies serve such goals as privacy, racial and gender justice, income redistribution, limiting the role of government in areas such as law enforcement, expanding the role in other areas such as broadband, supporting small business and undermining large, and protecting incumbent businesses. Many UNCTAD nations' goals are digital protectionism and redistribution from the North. It is this core lack of agreement on goals that makes achieving policy agreement so difficult.

Policymakers today need to reaffirm that commitment and make it clear in dealing with other nations that the United States will support policies that spur global IT and digital innovation and oppose those that needlessly harm that.

Since the formation of the republic, the United States has stood for growth and progress, including technological. Policymakers today, from both parties, need to reaffirm that

commitment and make it clear in dealing with other nations that the United States will support policies that spur global IT and digital innovation and oppose those that needlessly harm that. As such, all discussions and narratives about digital technologies need to start with why the technology is a force for progress.

Principle 2: Embrace IT and Digital “National Developmentalism” (Smart, Active Policies to Support IT Innovation and Adoption) and Bring More Nations Into That Orbit

In the Cold War, there were two major camps: the democratic, market-based West and the authoritarian Communist East. It was clear what the goal of U.S. foreign policy was: keep nations from aligning with the Soviets and the Chinese, and encourage them to align with the United States.

Now there are five major political economy approaches to the digital economy.

The first is the neo-liberal “**Washington consensus**.” This is the traditional market-based approach that advocates for open markets, international trade, less regulation, the rule of law, and a minimal role for government. There are two problems with this approach. First, it always undervalues the key role of government in supporting innovation. Historically, the federal government played a key role in helping enable many key digital technologies, including the Internet, semiconductors, computing, GPS, and others. The second is that when the U.S. government advocates a principally free-market, hands-off approach to government, it fails to provide an acceptable alternative to China’s state-directed model. This not only means the United States has less influence in most nations seeking to grow their digital economy, it also leads many nations to become closer to China, and follow what appears to be a successful government-led model of technology catch up.

The second is **social democratic regulation**. As noted, this is the dominant doctrine in the EU (and among most on the left in the United States). In this approach, the key role of government is to regulate technology and technology companies so they achieve social democratic values of equality. This is increasingly bolstered by identity politics wherein activists routinely assert, usually without evidence or by cherry-picking evidence that supports their preconceptions, that digital technologies are inherently biased and harmful. It is a short step to the view that capitalism itself is inherently biased, oppressive, imperialist, and exploitative.

There are two problems with this approach. The first is that embracing it means less digital innovation and, by definition, slower per capita income growth, something many social democrats reject anyway, since they believe people already consume too much and for the sake of the planet should “live simple.” It also means less innovation in key areas such as health care, transportation, and education. The second problem is this approach lends support to an anti-business agenda, especially toward big business, and as such, leads to a weaker U.S. economy, since the United States on average has larger (and more efficient) firms than other nations.¹⁵⁹ It also lends itself to anti-Americanism and the false third-way narrative between Chinese authoritarianism, American capitalism, and idealistic, harmonious, and sustainable EU social democracy.

The third approach is **protectionism**: This is the view that sees limiting foreign IT and digital market access as the key way to grow a digital economy. Nations such as India and Indonesia exemplify this approach. Digital protectionism usually doesn’t work, in part because it often

drives up the costs of digital technologies, thereby limiting their use domestically, and because it also is against U.S. interests.

Washington has long and rightly argued against digital protectionism, although all too often it has spoken loudly but “carried a small stick.” In other words, digital protectionists have seldom been punished, and in some cases, continue to be rewarded.

The fourth is **authoritarian statism**. This is the state-directed approach that Chinese and other authoritarian governments engage in. While China is protectionist, it is more than that. It is also authoritarian, and its policies don’t just seek to protect domestic markets, they seek to harm foreign competitors.

There are two key problems with this approach. The first is while it can generate income growth and digital industry growth, it often comes at the expense of strong total factor productivity growth because so many resources are wasted.¹⁶⁰ The second is it harms global IT and digital innovation because China’s massive subsidies, IP theft, and coerced transfer take market share away from more innovative firms in other nations.¹⁶¹ The third is China does not embrace freedom, human rights, civil liberties, or democracy, and the lack of those values is often reflected in both their companies and their advocacy in global forums.

The fifth approach is **national developmentalism**, which holds that government should be a coach, helping firms within its borders to compete globally, innovate, and boost productivity.¹⁶² It supports innovation, markets, and business—including big business. But it also recognizes that the state should play a key role in supporting digital innovation, including by defending its firms from unfair foreign competition. Some nations have moved toward or have fully embraced the national developmentalism model, including Scandinavian nations; increasingly the United Kingdom, as conservatives move beyond their Thatcherite traditions; Israel, Singapore, Taiwan, and others. In addition, some U.S. policymakers on both sides of the aisle have moved in this direction.

The United States should fully embrace national developmentalism and actively work to bring as many countries as possible into the U.S. national developmentalism orbit, “selling” it as a compelling and effective alternative to social democratic regulation, protectionism, and authoritarian statism.

While this doctrine presents a more realistic picture of the world, for it recognizes that nations seek competitive advantage in IT and digital industries, it also counsels a “race-to-the-top” wherein nations support digital innovation with policies related to R&D, skills development, and digital infrastructures, as well as the right regulatory and tax policies, coupled with government use of the technologies themselves.

U.S. policymakers are moving more toward a national developmentalism view as they recognize the significant challenge that is China. As such, the United States should fully embrace national developmentalism and actively work to bring as many countries as possible into the U.S. national developmentalism orbit, “selling” it as a compelling and effective alternative to social democratic regulation, protectionism, and authoritarian statism.

Principle 3: Work to Limit China’s IT and Digital Progress, Especially When It Is Based on Innovation Mercantilism

While U.S. policy should foster a broad community of nations embracing IT and digital national developmentalism and a free and mostly open Internet, it should also work to limit Chinese progress, in part by working with allies and other nations that see China as a threat. To be clear, the motivation here is based not only on resisting China’s efforts to become a global hegemon, but on the fact that much of China’s technological success comes from illegitimate, unfair, predatory, and often illegal policies and practices.

While changing Chinese behavior (e.g., reducing their innovation mercantilist behaviors) is important, it should not be the principal goal, as that can be quite difficult. China has shown little willingness to pare its innovation mercantilist arsenal.

Rather, the goal should be to limit both Chinese progress and Chinese harm to U.S. technology and economic interests. As long as China seeks to gain global dominance in IT and digital sectors (as opposed to comparative advantage) by using “innovation mercantilist” tools that violate the spirit, if not the letter, of the WTO, and seeks to repress freedom, U.S. policy should work to limit Chinese IT and digital progress. But this must be done in ways that do not at the same time “shoot ourselves in the foot,” such as through unilateral export controls of technology products that for the most part China can obtain elsewhere.

Principle 4: Actively Fight Foreign IT and Digital Protectionism

As noted, many nations and regions, including Europe and many UNCTAD nations support digital protectionism (including limiting cross-border data flows), wrongly seeing it as a fast track to growth. If for no other reason than this hurts U.S. firms in their global competition with Chinese firms, U.S. policy should more actively resist foreign digital protectionism, and engage more effectively in multinational agencies, such as the World Bank and UNCTAD, that reward and encourage such protectionist policies.

Principle 5: Embrace IT and Digital Free Trade, Especially With Like-Minded Nations

The converse to principle four is that the United States should support IT and digital free trade. Concretely, for example, this means supporting the free flow of data; continued expansion of the Information Technology Agreement (ITA), including an ITA-3 that brings products covered up to date; and negotiating an ambitious WTO e-commerce agreement.¹⁶³ However, the United States should be strategic about which nations it encourages to participate in such agreements. For example, while it is in the United States’ interests for China to remain in the ITA agreement, the United States should negotiate the WTO e-commerce agreement without China, only letting China in after the agreement is concluded. Failure to do that is likely to lead to a significantly weakened agreement.¹⁶⁴

Principle 6: Resist Authoritarian Influences in the IT and Digital Economy but Remain Focused on Key U.S. Interests

Just as the United States rightly resists authoritarianism around the world because it violates core human rights, as well as often threatening core U.S. national interests, it should do the same when it comes to these nations’ actions and influences on the digital economy. But this should not mean weakening key national interests (e.g., IT and digital competitiveness) to push for more openness in authoritarian nations. And, to the extent the U.S. government pushes back

against Chinese censorship, especially unilaterally, it should include a focus on how it hurts U.S. competitiveness.¹⁶⁵

Principle 7: Defend the Private Sector’s Core Role in IT and Digital Governance

When it comes to IT and digital standards, global innovation is maximized if the private sector plays the key role not influenced by government. When authoritarian governments get involved, the motivation is to limit Internet freedom or support technology protectionism. As such, U.S. policy should continue its affirmative stance for a strong non-governmental role, but at the same time, should get more engaged in stopping China from distorting the global standards system for its own advantage, including by forcing Chinese companies to “toe the party line.”

Principle 8: Defend the Principle That Big Is Not Bad, and Often Is Superior

It is all too easy for policymakers, even in the United States, to get swept up in the anti-Big Tech rhetoric coming out of other nations seeking to take U.S. tech companies down a peg or two. Large companies, including tech companies, are mostly a force for good—helping drive growth, innovation, and competitiveness.¹⁶⁶ As such, U.S. policy should defend the concept of bigness and not aid and abet other nations that seek to attack large U.S. firms.

Principle 9: Defend Innovation-Oriented Regulation

To the extent the United States embraces Internet-libertarianism, it is helping other nations by making it easier for them to adopt an anti-American narrative and policies. However, the alternative should not be EU-style regulation, which limits innovation. Indeed, if the United States embraces a social-democratic approach to Internet regulation, it will mean less progress and growth both domestically and around the world. As such, the United States needs to embrace innovation-based IT and digital regulation (as opposed to precautionary principles-based) at home and abroad. At home, for example, this means enacting national privacy legislation and rules around the use of such technologies as facial recognition. Abroad, this means actively assisting other nations on how to craft innovation-enhancing regulatory systems that also meet key social policy concerns.

Principle 10: Defend the Mostly Open Internet

When the United States pursues an absolutist open Internet agenda (virtually everything should be open), it not only alienates other nations that don’t share U.S. values or have the same approach to free speech, it also diverts U.S. efforts from defending the U.S. digital economy. This is not to say, however, that an open Internet is not a force for progress or that the United States should not encourage nations to move in this direction. But if the U.S. narrative is tone-deaf to cultural differences (e.g., some nations do not want their citizens to access Internet pornography; others want to limit access to hate speech, etc.) the United States will be tuned out not just on this issue but on more important ones. In addition, the narrative of the absolutely open Internet makes it harder for the United States to call for measures to limit digital piracy, since many Internet exceptionalists and progressives wrongly decry any efforts to fight digital piracy as violating the open Internet.¹⁶⁷

Principle 11: Support a Robust Domestic IT and Digital Policy That Ensures U.S. Global Leadership

Foreign policy only goes so far. The United States will not effectively defend its IT and digital interests, nor effectively promote the superior U.S. approach around the world, unless Congress and the Biden administration put in place a robust, national developmentalism-based IT and digital strategy.¹⁶⁸ One key problem is that while the holders of the Washington Consensus rightly support a light touch approach to digital regulation, they are ambiguous toward a robust national advanced technology strategy.¹⁶⁹ And in turn progressives seek a strategy that advances social policy goals, not competitiveness and innovation goals.¹⁷⁰

Absent such a strategy, the risk of the United States falling behind China grows significantly. Helping IT and digital firms in the United States continue to build products that are so good consumers all around the free world will insist on using them is good insurance, both against Chinese innovation mercantilism and IT and digital protectionism more broadly. This means the government enabling and supporting major advances in digital health care, education, financial services, public services, transportation, and other areas, as well as the talent needed to develop them.

CONCLUSION

This decade will likely prove decisive in how the global digital economy, and the U.S. IT and digital economy in particular, evolve. We can move to a world dominated by EU innovation-limiting regulations and Chinese technology predation and authoritarianism, with the attendant harms to U.S. and global innovation. Or, with decisive U.S. leadership under a new doctrine of digital realpolitik, we can move to a world wherein appropriate technology and regulatory policies enable IT and digital innovation to flourish, with all the attendant benefits, including continued U.S. leadership.

Acknowledgments

The author wishes to thank Dan Caprio (The Providence Group), Daniel Castro and Nigel Cory (ITIF), David Moschella (Leading Edge Forum) for helpful comments on prior drafts, and MacKenzie Wardwell for editorial assistance. Any errors or omissions are the author's alone.

About the Author

Robert D. Atkinson (@RobAtkinsonITIF) is the founder and president of ITIF. Atkinson's books include *Big Is Beautiful: Debunking the Myth of Small Business* (MIT, 2018), *Innovation Economics: The Race for Global Advantage* (Yale, 2012), *Supply-Side Follies: Why Conservative Economics Fails, Liberal Economics Falts, and Innovation Economics is the Answer* (Rowman Littlefield, 2007) and *The Past and Future of America's Economy: Long Waves of Innovation That Power Cycles of Growth* (Edward Elgar, 2005). Atkinson holds a Ph.D. in city and regional planning from the University of North Carolina, Chapel Hill.

About ITIF

The Information Technology and Innovation Foundation (ITIF) is a nonprofit, nonpartisan research and educational institute focusing on the intersection of technological innovation and public policy. Recognized as the world's leading science and technology think tank, ITIF's mission is to formulate and promote policy solutions that accelerate innovation and boost productivity to spur growth, opportunity, and progress.

For more information, visit us at www.itif.org.

ENDNOTES

1. See Albert Hirschman, *National Power and the Structure of Foreign Trade* (Los Angeles, CA: University of California Press, 1945).
2. Countries such as China and increasingly Russia have the ability to split off from the global Internet, but they largely do not have the motivation to. Catalin Cimpanu, “Oracle: China's Internet is designed more like an intranet,” *ZDNet*, July 23, 2019, <https://www.zdnet.com/article/oracle-chinas-internet-is-designed-more-like-an-intranet/>.
3. “History of rail transport in Japan,” Wikipedia, https://en.wikipedia.org/wiki/History_of_rail_transport_in_Japan#:~:text=On%20September%2012%2C%201872%2C%20the,for%20a%20modern%20electric%20train.
4. Robert L. Heilbroner, *Do Machines Make History?* in Merritt Roe Smith and Leo Marx (eds), *Does Technology Drive History?* (Cambridge, MA: MIT Press, 1996), 52.
5. Robert D. Atkinson et al., “A Policymaker’s Guide to the ‘Techlash’—What It Is and Why It’s a Threat to Growth and Progress” (ITIF, October 2019), <https://itif.org/publications/2019/10/28/policymakers-guide-techlash.>
6. Ford Motor Company was incorporated in 1903, and its first Canadian plant was built one year later in 1904.
7. David Moschella, *Waves of Power: The Dynamics of Global Technology Leadership, 1964–2010* (New York: AMACOM, 1997).
8. David Moschella, *Seeing Digital: A Visual Guide to the Industries, Organizations, & Careers of the 2020s* (Virginia: DXC Technology), 177.
9. United States Congress Office of Technology Assessment, *After the Cold War: Living with Lower Defense Spending* (1992).
10. Robert Atkinson, “Who Lost Lucent?: The Decline of America’s Telecom Equipment Industry,” *American Affairs Journal*, vol IV, no. 3 (2020). <https://americanaffairsjournal.org/2020/08/who-lost-lucent-the-decline-of-americas-telecom-equipment-industry/>.
11. Atkinson, “Who Lost Lucent?”
12. “China Information technology exports,” TheGlobalEconomy.com, https://www.theglobaleconomy.com/China/information_technology_exports/.
13. Chinese Competitiveness in the International Digital Economy, ITIF, <https://itif.org/publications/2020/11/23/chinese-competitiveness-international-digital-economy.>
14. Lambert Bu et al., “China digital consumer trends 2019” (McKinsey Digital, September 2019), <https://www.mckinsey.com/featured-insights/china/china-digital-consumer-trends-in-2019#>.
15. Ibid.
16. Robert D. Atkinson, *Enough is Enough: Confronting Chinese Innovation Mercantilism* (Information Technology and Innovation Foundation, February 2012), <https://itif.org/publications/2012/02/28/enough-enough-confronting-chinese-innovation-mercantilism.>
17. Paige Leskin, “Here are all the major US tech companies blocked behind China’s ‘Great Firewall,’” *Business Insider*, October 10, 2019, <https://www.businessinsider.com/major-us-tech-companies-blocked-from-operating-in-china-2019-5>.
18. *Testimony to the U.S. Senate Subcommittee on Trade Regarding Censorship as a Non-Tariff Barrier to Trade* (2020) (statement of Nigel Cory, Associate Director of Trade Policy, ITIF), <https://itif.org/publications/2020/06/30/testimony-us-senate-subcommittee-trade-regarding-censorship-non-tariff.censorship-non-tariff.>

19. Joseph Nahm, "China's Specialization in Innovative Manufacturing" (PowerPoint, National Academies of Sciences Innovation Policy Forum, Washington, D.C., May 23, 2017).
20. Figure used with permission. David Moschella, *Seeing Digital: a Visual Guide to Industries, Organizations, & Careers of 2020* (Tysons, VA: DXC Technology, 2018).
21. Zachary Karabell, "Obama and Chinese President Meeting Should Cover New Topics," *The Washington Post*, November 8, 2009, <http://www.washingtonpost.com/wpdyn/content/article/2009/11/06/AR2009110601904.html>; Kerry Brown, "Why China Can't Innovate," *The Diplomat*, August 19, 2014, <https://thediplomat.com/2014/08/why-china-cant-innovate>.
22. Kerry Brown, "Why China Can't Innovate,"
23. Robert D. Atkinson, "Is China Catching Up to the United States in Innovation?" (ITIF, 2019), <http://www2.itif.org/2019-china-catching-up-innovation.pdf>.
24. Laura Kayali, "Brussels' plan to rein in Big Tech takes shape," *Politico*, September 30, 2020, <https://www.politico.eu/article/digital-services-act-brussels-plan-to-rein-in-big-tech-takes-shape-thierry-breton-margrethe-vestager/>.
25. Béatrice Mouedine, "Bruno Le Maire: Les Gafa sont «aussi puissants que des états»," *Radio Classique*, April 11, 2020, <https://www.radioclassique.fr/magazine/articles/donald-trump-ou-joe-biden-cela-ne-changera-pas-grand-chose-a-nos-interets-commerciaux-assure-bruno-le-maire/?xtor=CS1-3050>.
26. Jean Jacques Servan-Schreiber, *The American Challenge* (New York: Atheneum, 1968), 12.
27. *Ibid*, 23.
28. *Ibid*, 26.
29. Alicia Garcia-Herrero and David Martinez Turegano, "Europe is losing competitiveness in global value chains while China surge," *Bruegel*, November 27, 2020, <https://www.bruegel.org/2020/11/europe-is-losing-competitiveness-in-global-value-chains-while-china-surges/>.
30. Javier Espinoza, "EU to tell Big Tech to police Internet or face large fines," *Financial Times*, December 9, 2020, <https://www.ft.com/content/72371610-4820-44c0-a955-4a19e430d343>.
31. Robert D. Atkinson and Michael Lind, "The Myth of the Roosevelt 'Trustbusters,'" *The New Republic*, May 4, 2018, <https://newrepublic.com/article/148239/myth-roosevelt-trustbusters>.
32. *Ibid*.
33. Directorate-General for Enterprise and Industry, *A Policy for Industrial Champions* (European Commission, 2006), <https://op.europa.eu/en/publication-detail/-/publication/768c3d1a-ae43-479c-b2cb-460248d9f910>.
34. Eline Chivot, "EU Is More Than A Decade Late In Its Plan To Be A Global Cloud Superpower" (Center for Data Innovation, December 2019), <https://datainnovation.org/2019/12/eu-is-more-than-a-decade-late-in-its-plan-to-be-a-global-cloud-superpower/>.
35. Eline Chivot, "France's Airbnb Is Poised To Be Its Next Big Fail" (CDI, June 2020), <https://datainnovation.org/2020/06/frances-airbnb-the-next-big-fail/>.
36. *Ibid*.
37. "Joseph Alois Schumpeter," The Library of Economics and Liberty, <https://www.econlib.org/library/Enc/bios/Schumpeter.html>.
38. From 1995 to 2010, the United States invested \$321 billion more in venture capital in young, innovative entrepreneurial companies than EU nations did, with the United States investing \$478.4 billion, versus the EU's \$157.2 billion. OECD, "OECD Science, Technology, and Industry Scoreboard 2013" (OECD, 2013), <http://www.oecd.org/sti/scoreboard-2013.pdf>.

39. I recently visited a very dynamic French government sponsored tech “accelerator” in Paris and spoke to a software entrepreneur. I asked him what his biggest challenge was and he said that even though his firm’s technology was on par with his main U.S. competitor (also a start-up), the U.S. company was able to scale up much faster on the basis of the large, integrated U.S. market and, because of that, plough revenues back into next generations of improved software, further expanding their lead over their French competitor.
40. Richard Cuthbertson, Peder Inge Furseth, and Stephen Ezell, *Innovating in a Service-Driven Economy: Insights, Application, and Practice* (London: Palgrave MacMillan, 2015). As then-Nokia CEO Stephen Elop acknowledged in his now-famous Burning Platform Memo of February 2011, “The battle of devices has now become a war of ecosystems, where ecosystems include not only the hardware and software of the device, but developers, applications, e-commerce, advertising, search, social applications, location-based services, unified communications and many other things. Our competitors aren’t taking our market share with devices; they are taking our market share with an entire ecosystem.” See Sam Gustin, “Nokia Standing on a ‘Burning Platform,’ CEO Tells Employees,” *Wired*, February 9, 2011, <http://www.wired.com/business/2011/02/nokia-burning-platform/all/>; Marc Andreessen, “Why Software Is Eating the World,” *The Wallstreet Journal*, August 20, 2011, <https://a16z.com/2011/08/20/why-software-is-eating-the-world/>.
41. Directorate-General for Enterprise and Industry, *A Policy for Industrial Champions*, 33, <https://op.europa.eu/en/publication-detail/-/publication/768c3d1a-ae43-479c-b2cb-460248d9f910>.
42. *Ibid*, 67.
43. Flash Eurobarometer 283: Entrepreneurship in the EU and beyond - A survey in the EU, EFTA countries, Croatia, Turkey, the US, Japan, South Korea and China, European Union Open Data Portal, 283. https://data.europa.eu/euodp/en/data/dataset/S765_283.
44. Mauritz Kop, “Quantum Technology and the Law,” *Futurium*, November 16, 2020, <https://futurium.ec.europa.eu/en/european-ai-alliance/document/quantum-technology-and-law>.
45. Alan McQuinn and Daniel Castro, “Why Stronger Privacy Regulations Do Not Spur Increased Internet Use” (ITIF, July 2018), <https://futurium.ec.europa.eu/en/european-ai-alliance/document/quantum-technology-and-law>.
46. Simone de Beauvoir, *Les Belles Images* (Paris: Gallimard, 1966) quoted in Servan-Schreiber, *The American Challenge*, 258.
47. Loubna Bouarfa, “AI and the anti-technology movement - why cultural resistance is a blessing in disguise,” European Commission, September 24, 2018, <https://futurium.ec.europa.eu/en/european-ai-alliance/document/quantum-technology-and-law>.
48. Chalmers A. Johnson, *MITI and the Japanese Miracle: The Growth of Industrial Policy, 1925–1975*, (Stanford: Stanford University Press, 1982).
49. Linsu Kim, *Imitation to Innovation: The Dynamics of Korea’s Technological Learning* (Boston: Harvard Business School Press, 1997), 23.
50. *Ibid*.
51. *Ibid*, 90.
52. Stephen J. Ezell and Caleb Foote, “Global Trade Interdependence: U.S. Trade Linkages with Korea, Mexico, and Taiwan” (ITIF, June 2019), <http://www2.itif.org/2019-global-trade-interdependence.pdf>.
53. Clayton Christensen and Shih Chintay, “Disruptive Innovation—How Taiwan Can Win,” *CommonWealth*, June 24, 2010, <https://english.cw.com.tw/article/article.action?id=996>.

54. United Nations ESCAP, *Evolution of Science, Technology and Innovation Policies for Sustainable Development: The Experiences of China, Japan, the Republic of Korea and Singapore*, https://www.unescap.org/sites/default/files/publications/UN_STI_Policy_Report_2018.pdf.
55. Fareeha Yasmin Iqbal, "The role of large-scale government-supported research institutions in development : lessons from Taiwan's Industrial Technology Research Institute (ITRI) for developing countries" (MIT, 2003), <https://dspace.mit.edu/handle/1721.1/30025>.
56. Goh Chor Boon, *From Traders to Innovators: Science and Technology in Singapore since 1965* (Singapore, ISEAS Publishing, 2016).
57. Stephen J. Ezell and Robert D. Atkinson, "The Middle Kingdom Galapagos Island Syndrome: The Cul-De-Sac of Chinese Technology Standards" (ITIF, December 2014), <http://www2.itif.org/2014-galapagos-chinese-ict.pdf>.
58. David D. Lee, "In South Korea, ride-hailing apps face off against powerful taxi unions and transport laws | South China Morning Post," *South China Morning Post*, March 22, 2020, <https://www.scmp.com/week-asia/economics/article/3076144/south-korea-ride-hailing-apps-face-against-powerful-taxi-unions>.
59. Hodan Omaar, "U.S. States Can Succeed in AI by Looking at Singapore," *U.S. News*, November 27, 2020, <https://itif.org/publications/2020/11/27/us-states-can-succeed-ai-looking-singapore>.
60. "About PCFIR," Presidential Committee on the Fourth Industrial Revolution, <https://www.4th-ir.go.kr/home/en>.
61. "AI Strategies and Policies in Japan," OECD, <https://oecd.ai/dashboards/countries/Japan>.
62. ITIF, "On Anniversary of Barlow's Cyberspace 'Declaration of Independence,' ITIF Renews Alternate Call for Interdependence in Governing Internet" news release, February 5, 2016, <https://itif.org/publications/2016/02/05/anniversary-barlow%E2%80%99s-cyberspace-%E2%80%98declaration-independence%E2%80%99-itif-renews>.
63. "The Grand New Bargain," *The Economist*, November 21, 2020, 20.
64. Anne-Marie Slaughter, "How to Succeed in the Networked World," *Foreign Affairs*, November/December 2016, <https://www.foreignaffairs.com/articles/world/2016-10-04/how-succeed-networked-world>.
65. Janna Anderson and Lee Rainie, "2. Broader thoughts from key experts on the future of democracy at a time of digital disruption" (Pew Research Center, February 2020), <https://www.pewresearch.org/Internet/2020/02/21/broader-thoughts-from-key-experts-on-the-future-of-democracy-at-a-time-of-digital-disruption/>.
66. Jared Cohen and Richard Fontaine, "Uniting the Techno-Democracies," *Foreign Affairs*, November/December 2020, <https://www.foreignaffairs.com/articles/united-states/2020-10-13/uniting-techno-democracies>.
67. Daniel Castro and Alan McQuinn, "Comments to the U.S. State Department on Draft Guidance for the Export of Surveillance Technology" (ITIF, October 2, 2019), <https://itif.org/publications/2019/10/02/comments-us-state-department-draft-guidance-export-surveillance-technology>.
68. Kieron O'Hara and Wendy Hall, "Four Internets: The Geopolitics of Digital Governance," CIGI Papers No. 206, December 12, 2018, <https://www.cigionline.org/sites/default/files/documents/Paper%20no.206web.pdf>.
69. Jared Cohen and Richard Fontaine, "Uniting the Techno-Democracies How to Build Digital Cooperation," *Foreign Affairs*, November/December 2020, <https://www.foreignaffairs.com/print/node/1126499#author-info>.
70. Robert D. Atkinson, "How China's Policies Have Stifled Global Innovation" (ITIF, January 2020), <https://itif.org/publications/2020/01/14/how-chinas-policies-have-stifled-global-innovation>.

71. Adam Thierer, "15 Years On, President Clinton's 5 Principles for Internet Policy Remain the Perfect Paradigm," *Forbes*, February 12, 2020, <https://www.forbes.com/sites/adamthierer/2012/02/12/15-years-on-president-clintons-5-principles-for-Internet-policy-remain-the-perfect-paradigm/?sh=67e9e43d7170>.
72. Eric Fish, "Why's Beijing So Worried About Western Values Infecting China's Youth?" ChinaFile, February 4, 2017, <https://www.chinafile.com/features/whys-beijing-so-worried-about-western-values-infecting-chinas-youth>.
73. Ibid.
74. "The digital side of the Belt and Road Initiative is growing" *The Economist*, February 2020, <https://www.economist.com/special-report/2020/02/06/the-digital-side-of-the-belt-and-road-initiative-is-growing>.
75. Yaroslav Trofimov, Drew Hinshaw, and Kate O'Keeffe, "How China Is Taking Over International Organizations, One Vote at a Time," *The Wall Street Journal*, September 29, 2020, <https://www.wsj.com/articles/how-china-is-taking-over-international-organizations-one-vote-at-a-time-11601397208>.
76. Proposals raised have included mandating big tech companies provide their data for free to small companies; subsidizing small companies' access to cloud computing, including on government-established cloud computing companies; and mandating disclosure of big-company algorithms.
77. Javier Espinoza, "Brussels looks to impose two-tier Big Tech regulation," *Financial Times*, December 4, 2020, <https://www.ft.com/content/bb681171-3673-46e5-a243-9c18d97e22d5>.
78. Robert D. Atkinson, "Comments on the European Commission's White Paper on Foreign Subsidies" (ITIF, September 2020), <https://itif.org/publications/2020/09/02/comments-european-commissions-white-paper-foreign-subsidies>.
79. Mark Scott, "What's driving Europe's new aggressive stance on tech," *Politico*, October 28, 2019, <https://www.politico.com/news/2019/10/28/europe-technology-silicon-valley-059988>.
80. Vincent Manancourt and Melissa Heikkila, "EU eyes tighter grip on data in 'tech sovereignty' push," *Politico*, October 29, 2020, <https://www.politico.eu/article/in-small-steps-europe-looks-to-tighten-grip-on-data/>.
81. "10 Benefits of Trade," https://trade.ec.europa.eu/doclib/docs/2010/november/tradoc_146935.pdf.
82. Marietje Schaake, "How democracies can claim back power in the digital world," *MIT Technology Review*, September 29, 2020, <https://www.technologyreview.com/2020/09/29/1009088/democracies-power-digital-social-media-governance-tech-companies-opinion/>.
83. Jill Hills, "Dependency Theory and Its Relevance Today: International Institutions in Telecommunications and Structural Power," *Review of International Studies*, vol. 20, no. 2 (April 1994), <https://www.jstor.org/stable/20097366?seq=1>.
84. *Digital Economy Report 2019*, United Nations (Geneva, 2019), 89, https://unctad.org/system/files/official-document/der2019_en.pdf.
85. Ibid, 91.
86. Ibid, 21.
87. Renata Avila Pinto, "Digital Sovereignty or Digital Colonialism?" *SUR*, vol. 15, no. 27 (2018), <https://sur.conectas.org/wp-content/uploads/2018/07/sur-27-ingles-renata-avila-pinto.pdf>.
88. Michael Kewt, "Digital colonialism is threatening the Global South," *Al Jazeera*, March 13, 2019, <https://www.aljazeera.com/opinions/2019/3/13/digital-colonialism-is-threatening-the-global-south/>.
89. *Digital Economy Report 2019*, United Nations, 94–95.
90. "Data Privacy FAQ," Amazon Web Services, <https://aws.amazon.com/compliance/data-privacy-faq>.

91. Nigel Cory, "Comments on India's Draft National E-Commerce Policy" (ITIF, March 2019), <https://itif.org/publications/2019/03/08/comments-indias-draft-national-e-commerce-policy>.
92. Hannah Ellis-Peterson, "Indian move to regulate digital media raises censorship fears," *The Guardian*, November 11, 2020, <https://www.theguardian.com/world/2020/nov/11/india-to-regulate-netflix-and-amazon-streaming-content>.
93. Nigel Cory, "The False Appeal of Data Nationalism: Why the Value of Data Comes From How It's Used, Not Where It's Stored" (ITIF, April 2019), <https://itif.org/publications/2019/04/01/false-appeal-data-nationalism-why-value-data-comes-how-its-used-not-where>.
94. *Digital Economy Report 2019*, United Nations, 105.
95. Ibid.
96. Ibid.
97. Stephen J. Ezell, *Contributors and Detractors: Ranking Countries' Impact on Global Innovation* (ITIF, January 2016), <http://www2.itif.org/2016-contributors-and-detractors.pdf>.
98. Joseph Stiglitz, "Australia's New Tech Code is a Road Worth Exploring," *Financial Times*, December 2, 2020, <https://on.ft.com/33yMvPC>.
99. Nigel Cory and Daniel Castro, "Crafting an Open and Innovative Digital Trade Agenda for Latin America" (ITIF, November 2018), <https://itif.org/publications/2018/11/26/crafting-open-and-innovative-digital-trade-agenda-latin-america>.
100. Jake Bright, "Diving deep into Africa's blossoming tech scene," *Tech Crunch*, May 31, 2019, <https://techcrunch.com/2019/05/31/diving-deep-into-africas-blossoming-tech-scene/>; Maxime Bayen, "Africa: a look at the 442 active tech hubs of the continent," *GSMA*, March 22, 2018, <https://www.gsma.com/mobilefordevelopment/blog-2/africa-a-look-at-the-442-active-tech-hubs-of-the-continent/>; GTIPA, GTIPA Perspectives: The Importance of E-commerce, Digital Trade, and Maintaining the WTO E-commerce Customs Duty Moratorium (GTIPA, October 2020), http://www2.itif.org/2020-gtipa-e-commerce.pdf?_ga=2.11830397.898919822.1607697750-254668983.1577993982.
101. Nigel Cory, "Comments to the U.S. International Trade Commission Regarding the Digital Economy and Trade in Sub-Saharan Africa" (ITIF, August 2019), <https://itif.org/publications/2019/08/19/comments-us-international-trade-commission-regarding-digital-economy-and>
102. Anas Baig, "Top 5 Countries Where Cyber Attacks Originate," *Security Today*, March 3, 2017, <https://securitytoday.com/Articles/2017/03/03/Top-5-Countries-Where-Cyber-Attacks-Originate.aspx?Page=2>.
103. Ibid.
104. Veerle Heyvaert, "Globalizing Regulation: Reaching Beyond the Borders of Chemical Safety," *Journal of Law and Society*, vol. 36, no. 1 (March 2009), <https://www.jstor.org/stable/40206881?seq=1>.
105. Nick Wallace and Daniel Castro, "The Impact of the EU's New Data Protection Regulation on AI" (ITIF, March 2018), <https://itif.org/publications/2018/03/26/impact-eu-new-data-protection-regulation-ai>.
106. But nations do not need a GDPR-like framework to protect privacy. Privacy harms are no worse in the United States (which does not have "adequacy") than in Europe, in part because the United States has regulated privacy in ways that enable companies to innovate but also protect individuals from privacy harms.
107. Eline Chivot, "The EU Needs to Reform the GDPR To Remain Competitive in the Algorithmic Economy" (CDI, May 2019), <https://datainnovation.org/2019/05/the-eu-needs-to-reform-the-gdpr-to-remain-competitive-in-the-algorithmic-economy/>.

108. Nick Wallace and Daniel Castro, “The Impact of the EU’s New Data Protection Regulation on AI” (ITIF, March 2018), <https://itif.org/publications/2018/03/26/impact-eu-new-data-protection-regulation-ai>.
109. Robert D. Atkinson et al., “A Policymaker’s Guide to the ‘Techlash’—What It Is and Why It’s a Threat to Growth and Progress.”
110. Robert D. Atkinson, “How MIT’s ‘Work of the Future’ Project Gets It Wrong: Raising Taxes on Machinery and Software Would Kill Jobs and Hamper Wage Growth,” *Innovation Files*, October 5, 2020, <https://itif.org/publications/2020/10/05/how-mits-work-future-project-gets-it-wrong-raising-taxes-machinery-and>.
111. Robert B. Reich, “Big Tech Has Become Way Too Powerful,” *The New York Times*, September 19, 2015, <https://www.nytimes.com/2015/09/20/opinion/is-big-tech-too-powerful-ask-google.html>.
112. Robert VerBruggen, “Google, Facebook, Amazon: Our Digital Overlords,” *National Review*, December 12, 2017, <https://www.nationalreview.com/2017/12/google-facebook-amazon-big-tech-becoming-problem/>.
113. Eleanor Clift, “Bill Galston and Bill Kristol’s New Center Project Takes Aim at the Tech Oligarchs,” *Daily Beast*, September 11, 2017, <https://www.thedailybeast.com/bill-galston-and-bill-kristols-new-center-project-takes-aim-at-the-tech-oligarchs>.
114. Janna Anderson and Lee Raine, “Concerns about democracy in the digital age” (Pew Research Center, February 2020), <https://www.pewresearch.org/Internet/2020/02/21/concerns-about-democracy-in-the-digital-age/>.
115. Janna Anderson and Lee Rainie, “Broader thoughts from key experts on the future of democracy at a time of digital disruption” (PEW Research Center, February 2020), <https://www.pewresearch.org/Internet/2020/02/21/broader-thoughts-from-key-experts-on-the-future-of-democracy-at-a-time-of-digital-disruption/>.
116. Madhumita Murgia and Anna Gross, “Inside China’s controversial mission to reinvent the Internet,” *Financial Times*, March 27, 2020, <https://www.ft.com/content/ba94c2bc-6e27-11ea-9bca-bf503995cd6f>.
117. Robert Kuttner, “Kuttner on TAP: Will Big Tech Take Over Trade Policy,” *American Prospect*, December 4, 2020, <http://americanprospect.activehosted.com/index.php?action=social&chash=c86a7ee3d8ef0b551ed58e354a836f2b.422&s=1acb87ecf9b95b2c95f2308c5b4619f6>.
118. One British author, who it should be noted is not an expert in neurology, claimed—presumably to help promote his book sales—that the increased use of mapping apps, such as Google Maps, would cause a worldwide increase in early onset of Alzheimer’s because we would no longer be adequately exercising our brain as we did when we had to navigate by paper map. (Sarah Knapton, “Google Maps Increases Risk of Developing Alzheimer’s, Expert Warns,” *The Telegraph*, May 29, 2019, <https://www.telegraph.co.uk/science/2019/05/29/google-maps-increases-risk-developingalzheimers-expert-warns/>.) The U.S. Alzheimer’s Association has not made this case and could find no research to support it (email exchange with the Association, September, 2019).
119. “The grand new bargain,” *The Economist*, November 21, 2020, 21.
120. Rana Foroohar, “A transatlantic effort to take on Big Tech,” *Financial Times*, December 6, 2020, <https://www.ft.com/content/09675f3f-189b-4946-8f70-fb55d2ba4471>.
121. Going all the way to embrace the EU approach to digital regulation would only weaken the U.S. digital economy, paving the way for Chinese global dominance.
122. “1 MARCH—17TH MAY 1865: FIRST INTERNATIONAL TELEGRAPH CONFERENCE IN PARIS,” *Geneve Internationale*, <https://www.geneve-int.ch/node/3997>.

123. “International Radiotelegraph Convention (1906),” Wikipedia, [https://en.wikipedia.org/wiki/International_Radiotelegraph_Convention_\(1906\)](https://en.wikipedia.org/wiki/International_Radiotelegraph_Convention_(1906)).
124. Ian Bremmer, “Why we need a World Data Organization. Now.” *GZERO*, November 25, 2019, <https://www.gzeromedia.com/why-we-need-a-world-data-organization-now>.
125. “‘The Time has Come for International Regulation on Artificial Intelligence’—An Interview with Andrew Murray,” *Opinio Juris*, <http://opiniojuris.org/2020/11/25/the-time-has-come-for-international-regulation-on-artificial-intelligence-an-interview-with-andrew-murray/>.
126. Cohen Fontaine, “Uniting the Techno-Democracies.”
127. Nigel Cory, “Why China Should Be Disqualified From Participating in WTO Negotiations on Digital Trade Rules” (ITIF, May 2019), <https://itif.org/publications/2019/05/09/why-china-should-be-disqualified-participating-wto-negotiations-digital>.
128. *Ibid.*
129. Daniel Castro and Robert Atkinson, “Beyond Internet Universalism: A Framework for Addressing Cross-Border Internet Policy” (ITIF, September 2014), www2.itif.org/2014-crossborder-Internet-policy.pdf.
130. “Podcast: The Case for Killer Robots, With Robert Marks,” *Innovation Files*, August 10, 2020, <https://itif.org/publications/2020/08/10/podcast-case-killer-robots-robert-marks>.
131. Marietje Schaake and Rob Reich, “Election 2020: Antitrust and Privacy in the Age of Big Tech,” Stanford University, https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/hai_cyberpolicy_election_6_v1.pdf.
132. “How China’s Communist Party trains foreign politicians,” *The Economist*, December 10, 2020, <https://www.economist.com/china/2020/12/10/how-chinas-communist-party-trains-foreign-politicians>.
133. Jill Disis and Angus Watson, “Australia is out of recession. Now it needs to avoid a trade war with China,” *CNN Business*, December 2, 2020, <https://www.cnn.com/2020/12/02/economy/australia-china-economy-trade-war-intl-hnk/index.html>; Rod Tyers and Yixiao Zhou, “An all-out trade war with China would cost Australia 6% of GDP,” *The Conversation*, <https://theconversation.com/an-all-out-trade-war-with-china-would-cost-australia-6-of-gdp-151070>.
134. Aaron Holmes, “Tech leaders have long predicted a ‘splInternet’ future where the web is divided between the US and China. Trump might make it a reality” *Business Insider*, August 6, 2020, <https://www.businessinsider.com/splInternet-us-china-Internet-trump-pompeo-firewall-2020-8>.
135. Cimpanu, “Oracle: China’s Internet is designed more like an intranet.”
136. “The SplInternet,” *Doc Searls Weblog*, December 16, 2008, <http://blogs.harvard.edu/doc/2008/12/16/the-splInternet/>.
137. It is true that Russia’s Runet is moving in this direction. Fiona M. Maclean and Ksenia Koroleva, “RuNet Law: New Russian Law Could Significantly Impact Telecom and Internet Providers and Social Media Platforms,” *Lexology*, May 22, 2019, <https://www.lexology.com/library/detail.aspx?g=d3649e65-acb5-464b-86dc-98f959aa3af3>.
138. Anne-Marie Slaughter, “How to Succeed in the Networked World,” *Foreign Affairs*, November/December 2016, <https://www.foreignaffairs.com/articles/world/2016-10-04/how-succeed-networked-world>.
139. Peter Schwartz and Peter Leyden, “The Long Boom: A History of the Future, 1980–2020,” *Wired*, July 1, 1997, <https://www.wired.com/1997/07/longboom/>.
140. “Members,” Open Government Partnership, <https://www.opengovpartnership.org/our-members/>.
141. *Ibid.*

142. Nigel Cory, “The Ten Worst Digital Protectionism and Innovation Mercantilist Policies of 2018” (ITIF, January 2019), <https://itif.org/publications/2019/01/28/ten-worst-digital-protectionism-and-innovation-mercantilist-policies-2018>.
143. Slaughter, “How to Succeed in the Networked World.”
144. Ibid.
145. USTR, “USTR Releases Annual Special 301 Report on Intellectual Property Protection and Review of Notorious Markets for Counterfeiting and Piracy,” news release, April 29, 2020, <https://ustr.gov/about-us/policy-offices/press-office/press-releases/2020/april/ustr-releases-annual-special-301-report-intellectual-property-protection-and-review-notorious>; USTR, “GSP in Use—Country Specific Information | United States Trade Representative,” <https://ustr.gov/issue-areas/trade-development/preference-programs/generalized-system-preferences-gsp/gsp-use-%E2%80%93-coun>.
146. UNCTAD, “Generalized System of Preferences: LIST OF BENEFICIARIES,” United Nations, 2018, https://unctad.org/system/files/official-document/itcdtsbmisc62rev7_en.pdf.
147. “China’s Impact on the Solar Industry: Lessons for the Future of Clean Energy,” ITIF event, October 30, 2019, <https://itif.org/events/2019/10/30/chinas-impact-solar-industry-lessons-future-clean-energy>.
148. *Testimony to the U.S. Senate Subcommittee on Trade Regarding Censorship as a Non-Tariff Barrier to Trade (2020)* (statement of Nigel Cory, Associate Director of Trade Policy, ITIF), <https://itif.org/publications/2020/06/30/testimony-us-senate-subcommittee-trade-regarding-censorship-non-tariff>.
149. Bruno Maçães, “Biden on China: A response to Jake Sullivan,” *Foreign Policy*, December 7, 2020, <https://brunomacaes.substack.com/p/biden-thinks-hes-tough-on-china-hes>.
150. Cohen and Fontaine, “Uniting the Techno-Democracies.”
151. Robert K. Knake, “Weaponizing Digital Trade: Creating a Digital Trade Zone to Promote Online Freedom and Cybersecurity” (Council on Foreign Relations, September 2020), <https://www.cfr.org/report/weaponizing-digital-trade>.
152. Robert D. Atkinson and Clyde Prestowitz, “China’s reaction to the pandemic shows why the U.S. and its allies need a NATO for trade,” *The Washington Post*, May 20, 2020, <https://www.washingtonpost.com/opinions/2020/05/20/chinas-reaction-pandemic-shows-why-us-its-allies-need-nato-trade/>.
153. “The Grand New Bargain,” *The Economist*, November 21, 2020, 113.
154. “EU-US: A new transatlantic agenda for global change” news release, December 2, 2020, https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2279.
155. Daniel Castro and Ashley Johnson, “Why Can’t Congress Pass Federal Data Privacy Legislation? Blame California,” *Innovation Files*, December 13, 2019, <https://itif.org/publications/2019/12/13/why-cant-congress-pass-federal-data-privacy-legislation-blame-california>.
156. For a case in point, see Robert D. Atkinson and Michael McLaughlin, “Freedom Is Not Free License: Freedom House’s Flawed Measurement of ‘Internet Freedom’” (ITIF, June 2020), <https://itif.org/publications/2020/06/08/freedom-not-free-license-freedom-houses-flawed-measurement-Internet>.
157. “Global Economic Outlook,” The Conference Board, December 2020, <https://www.conference-board.org/topics/global-economic-outlook>.
158. “The Digital Attache Program,” export.gov, <https://www.export.gov/digital-attache>.
159. Robert D. Atkinson and Michael Lind, *Big is Beautiful: Debunking the Myth of Small Business* (Massachusetts: MIT Press, 2018).

160. John West, “China, a low-productivity superpower,” *The Interpreter*, October 31, 2019, <https://www.lowyinstitute.org/the-interpreter/china-low-productivity-superpower>.
161. Robert D. Atkinson, “Innovation Drag: China’s Economic Impact on Developed Nations” (ITIF, January 2020), <https://itif.org/publications/2020/01/06/innovation-drag-chinas-economic-impact-developed-nations>.
162. Robert D. Atkinson and Michael Lind, “National Developmentalism: From Forgotten Tradition to New Consensus,” *American Affairs*, vol. 3, no. 2, Summer 2019, <https://americanaffairsjournal.org/2019/05/national-developmentalism-from-forgotten-tradition-to-new-consensus/>.
163. Stephen Ezell, “Joining the ITA Spurs Economic Growth in Developing Nations” (ITIF, June 2017), <https://itif.org/publications/2017/06/27/joining-ita-spurs-economic-growth-developing-nations>.
164. Nigel Cory, “Why China Should Be Disqualified From Participating in WTO Negotiations on Digital Trade Rules” (ITIF, May 2019), <https://itif.org/publications/2019/05/09/why-china-should-be-disqualified-participating-wto-negotiations-digital>.
165. *Testimony to the U.S. Senate Subcommittee on Trade Regarding Censorship as a Non-Tariff Barrier to Trade* (2020) (statement of Nigel Cory, Associate Director of Trade Policy, ITIF), <https://itif.org/publications/2020/06/30/testimony-us-senate-subcommittee-trade-regarding-censorship-non-tariff>.
166. Robert Atkinson and Michael Lind, *Big is Beautiful: Debunking the Myth of Small Business* (New Haven: Yale University Press, 2018).
167. *Hearing on “Expanding U.S. Digital Trade and Eliminating Barriers to Digital Exports,” Testimony Before U.S. House Ways and Means Subcommittee on Digital Trade* (2016) (statement of Robert Atkinson, President, ITIF), <https://itif.org/publications/2020/06/30/testimony-us-senate-subcommittee-trade-regarding-censorship-non-tariff>.
168. Robert D. Atkinson, “The Case for a National Industrial Strategy to Counter China’s Technological Rise” (ITIF, April 2020), <https://itif.org/publications/2020/04/13/case-national-industrial-strategy-counter-chinas-technological-rise>.
169. Ibid.
170. Rob Atkinson, “Industrial Policy May Have Finally Arrived: But For What?” *American Compass*, November 16, 2020, <https://americancompass.org/the-commons/industrial-policy-may-have-finally-arrived-but-for-what/>.