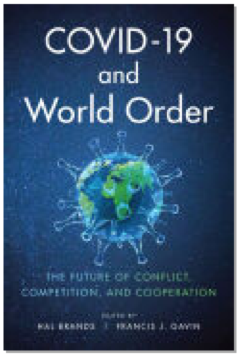
9. Flat No Longer: Technology in the Post-COVID World



Published by

Gavin, Francis J. and Hal Brands.
COVID-19 and World Order: The Future of Conflict, Competition, and Cooperation.
Johns Hopkins University Press, 2020.
Project MUSE. https://doi.org/10.1353/book.77593.

Chapter Nine

Flat No Longer

Technology in the Post-COVID World

Christine Fox and Thayer Scott

Even before the world faced a pandemic crisis, the bloom was already coming off the rose of globalization. Nowhere is this more true than in the high-technology arena—an arena that had been at the forefront of breaking down barriers and transcending the traditional antagonisms between nations. Technology, commerce, and connectivity would move on apace regardless of what governments did or said. Fields such as telecommunications, computing, artificial intelligence (AI), and biotechnology have all benefited from the relatively open exchange of people and products since the Cold War ended.

By the time the COVID-19 pandemic struck, the globalist system of technology commerce and research was already starting to fray. The United States was in the midst of using its semiconductor advantages to slow the spread of Chinese telecommunications infrastructure—efforts that would intensify after the outbreak. The COVID-19 crisis revealed the United States' deep and disturbing dependence on China for key pharmaceuticals and medical equipment, sparking calls for more self-sufficiency and less reliance on foreign suppliers. The kind of globalism extolled by Thomas Friedman and others after the Cold War now looks much less inevitable—and attractive—in the wake of COVID-19.[1]

Christine Fox is assistant director for policy and analysis at the Johns Hopkins University Applied Physics Laboratory. Thayer Scott is a public policy writer and consultant.

The authors are grateful for the contributions of Melissa Terlaje and Jessica Dymond to this essay.

China has moved quickly and opportunistically to further upend a liberal world order that had been conducive to technology innovation—and to American interests. For example, the Chinese government is leveraging its existing Belt and Road Initiative (BRI) relationships and transport hubs to provide medical equipment, supplies, and treatment to many of the same countries as part of a new "Health Silk Road." China is also aggressively deploying its own 5G telecommunications systems and enabling electronic surveillance in ways that are appealing to authoritarian governments within the BRI and elsewhere. Where the United States has withdrawn—through a combination of hostility and indifference—from global institutions, most notably the World Health Organization (WHO), China has jumped in to fill the gap. This dynamic extends to international bodies that set standards for the next generation of technology. Recently, China's president, Xi Jinping, presented China as an exemplar nation, promoting a "community of common destiny for mankind."[2] The United States appears to be entering a period of retrenchment, on course to unravel supply chains for medical equipment, computing, telecommunications, and more.

Retrenchment and disentanglement pose significant risks, as the United States could end up with less access to international technology talent, innovation, and markets. Before the pandemic, the Chinese government had set ambitious plans and made significant investments in critical technologies—efforts redoubled in the wake of COVID-19.[3] China is poised to expand its influence by more widely deploying its telecommunications infrastructure, encouraging the de facto splintering of what had been a World Wide Web, and reaping the fruits of massive investments in domestic research and development and manufacturing. China's aggressive engagement with international standards setting could further advance and validate its authoritarian model in much of the world.

Many important technology products and discoveries trace their origins to when the US government, in the context of the Cold War, played a much larger role in funding and research. In recent decades, the commercial sector has been the driving force behind technology innovation. American technology leaders often cite the relatively light, or absent, hand of national governments as a key to success. But the past couple of years have also shown the limits of laissez-faire—for telecom and pharmaceuticals especially. To mitigate some of these dependencies in a way that minimizes negative economic and scientific impacts, the US government will need to play a more active and more competent role in ensuring reliable sourcing on everything from 5G to antibiotics. Attempting to do so unilaterally will almost certainly fail and leave us worse off. Without trying to replicate an inefficient and centralized Chinese model, the governments of advanced democracies must collaborate more—with each other and between each country's public and private sectors.

These partnerships are needed to hinder Chinese attempts to achieve technology market dominance and, with it, the ability to intimidate and coerce other nations. The approach must be nuanced enough to allow for, and even encourage, research collaborations in fields that benefit the world such as AI and biotech. This strategy will be difficult to design and carry out—it must build up domestic capacity while pursuing global engagement in ways that shape international norms and values. But continuing on this present course will lead to a post-COVID-19 world order that will look considerably different—and much less hospitable—to American needs and aspirations.

This essay explores these challenges—along with recommended government responses—with respect to the potential disintegration of the global internet, the unraveling of global supply chains for semiconductors and telecommunications, and the risks and opportunities posed by biotechnology.

The Coming Splinternet

The internet is a network of independently managed networks—a network of networks—that enables the global sharing of information, communications, and our digital economy. The internet is also at the core of modern disputes over freedom of expression, privacy, transnational crime, internal security, intellectual property, trade, and economic regulation.[4] It has been blamed for the rise of terrorism, the destruction of individual privacy, increased intellectual property theft, and the spread of misinformation. It is also seen as having the potential to sway elections and even topple governments, as evidenced by the Arab Spring.[5] The issues associated with internet governance—technical standards, censorship, privacy, intellectual property—reflect a wider global balkanization. Contravening the internet's origins and ideals, many nations are seeking to impose controls on what populations can see and do online within their borders, in effect fragmenting the internet into different camps with different rules. Eric Schmidt coined the term "splinternet" several years ago, and it stuck.[6] Were this to happen, the World Wide Web that we have grown so accustomed to would be gone, or at least significantly less "world wide." Without a universal internet, national governments would be able to decide what their citizens can access online from inside or outside the country—products, services, information, or ideas. This is not a world that is easy for us to envision today, yet it is a world that we may be heading for.

In some cases, concerns over privacy, health, and safety are creating localized rules and regulations. France, for example, has required Google to remove thousands of search results under a "right to be forgotten" law. France is also leading the European Union (EU) in pushing for new copyright protections that could result in websites banning users from uploading files.[7] But the world's most stringent set of data protection rules comes from the EU's General Data Protection Regulation (GDPR),[8] which went into effect in 2018. These rules place limits on what organizations can do with personal data. And these rules have teeth: the GDPR enables regulators to impose huge fines on businesses for noncompliance.[9] The GDPR is often heralded as a model for personal privacy protections, but it also contributes to segmentation of the internet. It creates a new set of regulatory hurdles and costs for internet transactions. If other countries follow suit, we could end up with an overlapping regulatory environment that puts a damper on international business flow. Smaller businesses in particular would struggle to navigate a complex web of compliance laws.[10]

For other groups of nations, the prime motivation is information control. Russia's "sovereign internet" law of May 2019 mandates that all internet traffic flow through government-controlled choke points, allowing authorities to censor the information before it reaches the Russian people. Russia's internet is not designed technically for this type of choke-point control, however. Hundreds of networks come together in Russia, and many of them are supplied by international network providers.[11] Experts suggest that attempts to employ choke points and block content in this complex network will result in instabilities that will make Russia's internet slower and less reliable.[12] Nonetheless, for the Russian leadership, controlling the internet's content is more important than the quality of internet service received by its people.

China, on the other hand, built its internet from the start on a series of state-run network operators, leading to what is commonly called the Great Firewall of China.[13] It allows the Chinese central government to censor the information available to its citizens more easily than Russian leadership can. China's president, Xi Jinping, does not consider his blatant efforts to control the internet to be a source of embarrassment or something to hide. Rather, he openly discusses this system with pride and sees his vision as a model for other countries,[14] one that advances commerce and innovation without fostering dissent that leads to political change.

Because the existing internet does not align with national borders, governments desiring this kind of internal control must, in effect, build their own internets with their own rules. China is working on a new root name server—a mechanism for translating domain names into numeric internet protocol (IP) addresses—and a corresponding operating organization. Currently there are at least a dozen virtual root name servers based in the United States, Europe, and Japan—but none in China.[15] Control of root name servers translates into control of the distribution of IP addresses and domain names.[16] In a December 2019 statement announcing this effort by the China Academy of Information and Communications Technology (CAICT), the Chinese government said, "While ensuring the stable operation of the server and providing quality service to users, the CAICT should also protect users' information security and safeguard national interests."[17] This new root name server could further splinter the internet and provide other governments an alternative to the current system.

A splintered internet will lead inevitably to an even more splintered big-tech enterprise. US companies are still the overall global leaders in internet services and search engines—except in China. While Google holds more than 90% of the worldwide search engine market, it holds less than 5% of the market in China.[18] Baidu, China's top seach engine provider, is focused primarily on the domestic market and as a result has little market penetration elsewhere. Those metrics should give no comfort to American companies—or US leaders. Consider that in the first quarter of 2020, China had more than 900 million internet users, and that number was growing at a rate of 5% annually. In fact, China has more internet users than the United States and the European Union combined.[19]

If China is successful at creating a separate splinter of the internet, Baidu, along with Alibaba and Tencent, collectively known as "BAT," will be ready with the corresponding search engines and internet services. Over time, this Chinese version of the internet and aligned technology companies could become favored by Digital Silk Road countries and authoritarian governments elsewhere. If successful, they could eat into the international market currently dominated by the United States and its corresponding technology giants, including Facebook, Apple, Amazon, Netflix, and Google. No longer "citizens of the world," major US technology companies would need to operate more like "national champions." Under this scenario, Americans would continue to access quality technology goods and services from US providers and partners, but with less choice and at a higher price.

The inherent strengths of the West and its democratic allies worldwide nonetheless provide a foundation for continued success. The concern is less commercial than ideological. The Chinese governing model—state direction and subsidy of a technology industry subsequently used to control its population—may gain more purchase elsewhere. A "digital curtain" could divide up much of the world into competing (and increasingly incompatible) camps for information and communications. China could be poised to take a larger share of emerging economies with growing populations in the BRI nations of Central Asia, Latin America, Africa, the Middle East, and possibly even southeastern Europe. This scenario does not bode well for US ideals or interests over the long term.

Mitigating the downside of a fragmented technology world will require cooperating in ways that run counter to current trends, with nations turning inward in the name of self-reliance and security. It will also require a commitment by the United States to international standard-setting organizations that, mostly out of the public eye, can make decisions with long-term consequences. As noted by Lindsay Gorman of the Cyberspace Solarium Commission, China has set an explicit goal of becoming "a standards-issuing country." Gorman adds, "China coordinates national standards-work across government, industry and academia as part of its push to increase international influence."[20] A March 2020 letter signed by seventeen US senators spanning the political and ideological spectrum voiced concern over China's use of international bodies to enshrine its preferred norms and rules for advanced surveillance technology. "China is currently working to use standards setting bodies to gain the imprimatur of international legitimacy and support across a range of emerging technologies . . . in service of [its] anti-democratic vision for technology."[21]

Over time China's well-coordinated and aggressive advocacy for international standards that reflect its interests and values will bear fruit at America's expense—and those of our European and Asian allies as well. Solarium's Gorman notes that, by contrast, the US approach to standardization has been bottom-up, stakeholder driven, and generally resistant to central planning. "For years, U.S. technological dominance in internet technologies meant that a lack of a coordinated approach did not seriously stifle U.S. competitiveness. . . . This hands-off approach may no longer be sufficient."[22]

The Showdown in Semiconductors and the Future of Telecom

Although other nations in Europe and Asia—including China—have developed successful semiconductor industries, the United States remains the dominant provider and player in the design and production of the most technically advanced chips used for many technologies, most notably telecommunications (5G) and AI. America's electronic design automation (EDA) vendors have held a lead in this market for three decades.[23] The United States also continues to dominate the production of semiconductor capital equipment. American companies generate more than half the global revenue for chip manufacturing equipment compared with Japan's 27% and Europe's 17%.[24]

Recently the United States has not been shy about exploiting some of these advantages, particularly in the area of telecommunications. In May 2019, President Donald J. Trump signed an executive order prohibiting US companies from using foreign telecommunications equipment deemed to be a national security risk.[25] Six months later, the Federal Communications Commission (FCC) barred American rural customers from tapping into an $8.5 billion government fund to buy from Huawei or other Chinese providers. The executive order was extended in May 2020 with what seemed a nuclear option for the telecommunications global supply chain: in addition to severing direct access to US suppliers, the order cut off Huawei's access to equipment manufactured overseas using American technology and software.[26] This meant that Huawei could no longer obtain semiconductors from its largest and most important supplier in Taiwan. The Commerce Department has since "clarified" the order to allow cooperation with Huawei on standards setting.[27] Huawei had reportedly been stockpiling chips for months in anticipation of the US action, but it faces a wrenching supply challenge in the future.

The Chinese government has been keenly aware of these hardware dependencies and is working to develop alternatives to American capital equipment and EDA tools. The barrier to entry is steep—the cost of creating manufacturing plants for the most advanced chips can run into the multiple billions. Huawei's ability to mitigate the effects of US restrictions will largely depend on its ability to develop international alternatives. Given the attractiveness of Huawei's market, this might be possible in just a few years.[28]

Irrespective of where the battle over semiconductors leads, the telecommunications sector is on an inexorable path toward fragmentation, and the COVID-19 crisis is accelerating it. The industry is heading back to the days of separate and competing global standards and a lack of interoperable equipment. We may see the effective dismantling of a truly global supply chain, replaced by more government-sanctioned sourcing arrangements between groups of like-minded countries, potentially leading to a new telecommunications cold war. Nations would be forced to choose either China's 5G capabilities, which entails buying into China's authoritarian-friendly standards framework, or a more expensive and potentially less capable alternative.

Again, this is starting to happen. Last year, the United States launched a campaign—mostly fruitless—to convince NATO members to exclude Huawei from new 5G networks. The economic benefits of transitioning to Huawei 5G, however, outweighed the security concerns raised by the United States. But the scale of China's deception at the onset of the pandemic caused a number of European allies to rethink prior decisions to allow Huawei to compete for all, or even part, of their future telecom infrastructure. According to news reports, the British government is proposing a 5G alliance of ten democracies to explore alternatives to Huawei. The alliance comprises the countries in the Group of Seven (G7)—Canada, France, Germany, Italy, Japan, the United Kingdom, and the United States—as well as Australia, South Korea, and India.[29] The alternate Chinese-led bloc will presumably consist of BRI and Digital Silk Road countries, among other authoritarian-leaning states. The challenge for the next decade will be to counter China's 5G technology advantages, not with punitive (and often counterproductive) sanctions, but with sustainable and effective alternatives.

In China there is no expectation of separation among the private, public, and nonprofit sectors—academia, business, and the military. This is not a model the United States can or should seek to emulate. Nonetheless, the post-COVID-19 technology order will require the return of a robust role for government—direction, regulation, funding, and linkage to policy goals—that would have been anathema to Silicon Valley as late as a decade ago. But to produce more than just headlines and disruption, the US government will need to overhaul its "whack-a-mole" approach to dealing with foreign companies, people, and research in sensitive technology areas. Today, expertise and authorities are scattered throughout the federal government within the major cabinet departments and in subordinate or independent agencies such as the FCC, the National Telecommunications and Information Administration, the Food and Drug Administration (FDA), and more.

The United States will need to rethink—reimagine even—the governing structure for supervising its technology industry, monitoring the activities of foreign companies, and representing its interests and values to allies in an international setting. In early June, the Senate Permanent Subcommittee on Investigations published a bipartisan report criticizing the executive branch's oversight of foreign telecommunications companies.[30] Within the Trump administration, that responsibility had fallen to an ad hoc "Team Telecom" created by an April 2020 executive order. It was heavily weighted toward national security equities: the secretary of defense, the attorney general, and the secretary of homeland security were formal members of the committee. Other "advisory" members, without executive authority, included the State Department, the Department of Commerce, and the Department of Treasury as well as the Council of Economic Advisers.[31] Despite this security orientation, the subcommittee report found that Team Telecom provided "minimal oversight" of Chinese state-owned telecommunications companies operating in the United States. Significantly, the report recommends that Congress turn Team Telecom into a statutorily authorized committee. Its existence and authority would be formalized into US law and thus overseen by Congress. Among other powers, this statutory body would have the authority to recommend that the FCC revoke existing licenses. The Lawfare blog considered it an "important signal that Congress may get more involved in empowering and monitoring the executive branch's supply-chain security process for foreign telecoms."[32]

We should empower and consolidate an elite cadre of professionals—drawing on the best talent from industry, government, and academia—to oversee America's international technology collaborations from a holistic perspective: from research centers to supply chains to connectivity standards. They can also more ably represent US interests in venues such as the International Telecommunication Union, which, like the WHO, has come under significant Chinese influence. The Arms Control and Disarmament Agency, separated from the State Department in 1961, provided a base of institutional knowledge on the arcane details of nuclear weapons and treaty negotiations; it was disbanded in 1999 after the end of the Cold War. The answer to sorting through these thorny technology questions—in a way that avoids crude and counterproductive restrictions providing little security benefit—may lie in a similar independent agency or an empowered organization nested within an existing department. Foreign governments—not just China, but those in Europe—are set up much more effectively to advance national equities and share international decision making in the technology realm. The US government, as many have observed, is still largely organized around a 1947 model designed during the smokestack era.

Biotech Maneuvering and Mastery

Even before the COVID-19 pandemic galvanized the world, China had set a clear goal to dominate the biotechnology market—everything from pharmaceuticals to medical equipment to genetic engineering. During a Senate hearing in November 2019, Tara J. O'Toole, senior fellow and executive vice president at In-Q-Tel, said that "China has said repeatedly and forcefully . . . that they intend to own the bio-revolution. And they are building the infrastructure, the talent pipeline, the regulatory system, and the financial system they need to do that."[33]

Until a few years ago, the Chinese pharmaceutical industry was producing generic drugs of varying quality under a difficult regulatory system riddled with corruption and cronyism.[34] The Chinese government responded with multibillion-dollar investments and by revamping its drug approval and quality control process to more closely resemble that of the United States

China now possesses the second-largest pharmaceutical market in the world.[35] It also controls the global supply of the ingredients for thousands of essential generic medicines. The trauma of the COVID-19 crises exposed Americans and Europeans to their overdependence on one country. According to Rosemary Gibson, author of *China Rx: Exposing the Risks of America's Dependence on China for Medicine*, fully 90% of the chemical ingredients for generic drugs in the United States to care for people with serious coronavirus infections requiring hospitalization are sourced from China.[36]

In a 2019 speech predating the pandemic, Chinese economist Li Daokiu said, "We are at the mercy of others when it comes to computer chips, but we are the world's largest exporter of raw materials for vitamins and antibiotics. Should we reduce the exports, the medical systems of some western countries will not run well."[37] In a March editorial widely quoted and criticized in the United States, China's official news agency reportedly asserted, "If China announces that its drugs are for domestic use and bans exports, the United States will fall in the hell of a new coronavirus epidemic."[38]

As a result of this vulnerability, many are calling for the United States to "reshore" its capacity to manufacture vital pharmaceuticals and even, in some cases, to outlaw importation from China altogether.[39] But we are not reliant solely on China. India is the world's second-largest exporter of active pharmaceutical ingredients.[40] As the intensity of the pandemic grew in March, the Indian government, looking to the needs of its people, ordered its pharmaceutical manufacturers to stop exporting twenty-six drugs, most of them antibiotics.

At this point, it is not clear whether rebuilding a robust domestic pharmaceutical production capacity is even possible. The issue is not technical capability but rather the cost and time necessary to build the infrastructure. Undeterred, President Trump recently used executive order authority to award a $354 million, four-year contract to a new company called Phlow to manufacture pharmaceutical ingredients and generic medicines used in treating patients hospitalized for COVID-19.[41] When asked about the challenges ahead, White House trade adviser Peter Navarro said, "If we have strong Buy American procurement, that will establish a robust base level of demand that provides the appropriate incentives for our pharmaceutical manufacturers to invest and locate domestically."[42] Despite these efforts, it is likely that the United States will remain dependent on China and other nations for key pharmaceuticals for a long time. Thomas Cosgrove, a former senior FDA official, said it will take "decades and billions" to bring the pharmaceutical supply chain back to the United States.[43]

In addition to pharmaceutical production, the US medical equipment industry went all in on globalization in pursuit of cost savings and shareholder value. Those decisions, allowed if not encouraged by US government policy, were reasonable at the time from a business perspective, but they proved nearly fatal, literally, when the United States faced the same major bio-threat and pharmaceutical requirements at the same time as the rest of the world.

By 2018 China provided nearly half of all US imports of personal protective equipment (PPE).[44] When coronavirus cases were initially surging in spring 2020, many other afflicted nations stopped exporting masks and protective gear, including South Korea, Germany, India, and Taiwan.[45] Instead of dropping exports of PPE, China rapidly stepped up production to twelve times its supply before the outbreak of the pandemic.[46] This effort was marred later by reports of quality problems with some of the Chinese products,[47] but the speed and scale of China's response still resonated, especially in contrast with the efforts of the United States and other Western countries. In early May, Andrew Cuomo, governor of the state hit hardest by the virus at the time, announced that New York hospitals must build a ninety-day supply of PPE to prepare for another outbreak. Cuomo said, "You can't be dependent on China to have the basic equipment to save lives in the United States."[48]

To regain and sustain a major domestic sourcing capacity for PPE, US industry needs more clarity regarding the magnitude and time frame of the expected need. Companies want to avoid a repeat of what occurred during the 2009 swine flu outbreak, when a number of providers doubled staff and purchased new equipment only to find the crisis over. One in particular, Prestige Ameritech, came to the brink of bankruptcy as a result.[49] On top of relying on global sources for key protective equipment, successive administrations and congresses neglected the national PPE stockpile after the 2009 H1N1 outbreak.[50] Without purchase guarantees from the government, companies will be reluctant to invest in production capabilities of medical supplies like PPE in the face of so many uncertainties.

Despite struggling with the effects of COVID-19, China has spent the last several months cementing and expanding its existing global relationships using its Belt and Road Initiative and Health Silk Road. By taking full advantage of the world's struggles with COVID-19, China is promoting yet more widespread reliance on its products while, as with telecom and the internet, offering an alternative model to the West.

China introduced its Health Silk Road model in the WHO back in 2017.[51] The message was that 21st-century health challenges require a more high-tech approach and that China was the country to lead the world in delivering those technologies, including 5G telecommunications. When the COVID-19 pandemic struck, global media were flooded with images of 5G-enabled technologies helping combat the virus, including health consultants employing telemedicine, robots taking temperatures, and drones delivering face masks.[52]

China is also using COVID-19 to strengthen its humanitarian reputation. China's Jack Ma and Alibaba Foundations have delivered supplies to dozens of countries, including the United States.[53] As the United States pulled inward to deal with the impact of the pandemic and its economic repercussions, China stepped into the void. When the United States froze its funding to the WHO in April 2020, China significantly increased its contributions. Recently, China announced that it would donate $2 billion over two years to help nations respond to the pandemic.[54]

Of course, the Belt and Road Initiative, and now the Health Silk Road, are a means for China to deploy its telecommunications and surveillance infrastructure globally. Without alternatives, struggling nations will accept these offers of "benevolent" assistance. China's technology companies and telecommunications and surveillance infrastructure will become ingrained in every aspect of these nations' workings, opening doors to greater data collection, increased leverage, and ultimately strong influence over the recipient nations' policies. The very nature of authoritarian governments allows them to control their populations, track movements, and trace contacts, whether to prevent the spread of disease or, very often, the spread of unwelcome ideas and viewpoints. In the pandemic response, authoritarian governments and democracies alike cannot avoid the necessity of using technology for public health and public safety. But how these powerful tools are used and viewed varies greatly. For a good number of countries—in Africa, Latin America, Central Asia, the Middle East, and even eastern and southern Europe—the COVID-19 experience validates a more aggressive approach to technology and governance. China already had a foothold in some of these countries, providing automated tools for internal security—facial recognition, drones, AI, and more. These tools can spread further in the name of public health.

When faced with today's coronavirus pandemic or an unknown pandemic of the future, it is vital to have cooperative research on a global scale that enables preparedness, treatment, and ultimately eradication. According to an Ohio State University study, collaborations between US and Chinese scientists have actually intensified despite the geopolitical tensions between the two countries. China has significantly increased its funding for COVID-19 research and is participating in research teams with US and UK scientists.[55] This is happening despite Donald Trump's recent presidential proclamation aimed at limiting the entry of Chinese graduate students to the United States.[56]

Political concerns are nonetheless creeping into the process, and we can expect a further decline in cooperation—and thus advancement—in the scientific realm. China has introduced new policies that require scientists to obtain approval to publish their results. Some suggest that this measure is designed to prevent what happened early in the pandemic, when some poor-quality Chinese COVID-19 studies were posted online. Others are concerned that this is primarily an effort by the Chinese government to control and limit information that may not reflect well on its response to the outbreak.[57]

On the US side, officials are warning American companies to be extremely careful to protect their research against potential Chinese attempts to steal it. The race for a COVID-19 vaccine—along with other treatments neglected during the crisis—could suffer if national pride and perceived self-interest thwart collaboration. In this respect biotechnology may more closely resemble the recent course of AI—a previously open field now being targeted for controls and restrictions justified on national security grounds. The basic foundations of AI algorithms—forms of mathematics available from open sources—are virtually uncontrollable across borders. Biotechnology is more vulnerable to restriction and, accordingly, to the potential loss of needed advances in medicine and public health.

The global response to COVID-19 has shown a great need for international cooperation and, at the same time, revealed the challenges of achieving that cooperation when all nations are struggling with the same problem. There are many reasons why China's reputation should be marred by the world's coronavirus experience: there is strong evidence that the government suppressed attempts to alert others to the threat of COVID-19, and there is evidence that the Chinese government continues to underreport cases. Yet, even taking undercounting and potential deception into account, China's death rate per capita is almost certainly lower than that of the United States.[58] In late June, the EU released a list of non-European countries whose citizens would be allowed onto the continent, which included Canada, Australia, and South Korea. China is on the list pending confirmation that EU travelers will be allowed to reciprocally enter mainland China. Citizens and residents of the United States, Brazil, and Russia were barred because of the continued spread of the virus in those countries.[59] China holds the cards in many of the needed medical capabilities and is using that advantage to extend its global reach by offering medical assistance *along with* 5G technology. When the world looks back on this pandemic, China's strategic, opportunistic response may emerge as the turning point for the new world order.

Conclusion

The experiences of a global pandemic have caused the American public and its leaders across the political spectrum to look more skeptically—and fearfully—at the highly globalized system of technology commerce and innovation. With widespread sickness, job loss, or worse looming, it seemed as if the United States had lost the ability to take care of its own people. Foreign dependencies impeded a rapid and effective national response, highlighting our limitations in knowledge, capacity, and essential materials and supplies. This pandemic came at a time when the United States and China were already growing estranged and on the path to decoupling in many areas of technology. In the wake of the COVID-19 outbreak, the United States has made it a priority to become more self-sufficient and less dependent on China for critical medical equipment and supplies. China is leveraging the needs of other nations to expand its telecommunications infrastructure and model of internet governance. The combination of attitudes—one self-focused and the other opportunistic—could lead to a new digital cold war, in which the technology path chosen by a country comes with a corresponding set of norms, standards, and practices conducive to either democratic values, supported by the United States and the West, or an authoritarian model, underwritten by China.

The United States needs a more comprehensively planned and funded government strategy on critical materials and technologies. This strategy will need to be nuanced—it must foster research collaborations while loosening China's grip on essential drugs and medical supplies and ensure that we are not again caught flat-footed and scrambling by another Chinese advance like 5G.

We must sustain America's leading position in technology innovation by participating in international research collaborations and sustaining the use of technology through global standards and norms. Even as we work in concert with like-minded partners and support an international research environment conducive to the well-being of all, the legitimate needs of individual nations for independence and national security must be respected. The United States must strengthen the voice of democratic values in a world where technology is increasingly used to suppress information, spread disinformation, and control populations.

It is tempting to use current American strengths in manufacturing sectors, such as semiconductors, to hold China back and, presumably, advantage our position over time. But these policies could backfire. They provide China with a platform from which to argue that it is the open, engaged, and forward-leading player on the world stage while the United States and the West cling to the past. Through a combination of necessity and national pride, China will be further incentivized to enhance its own capabilities to the point where the advantage, and thus leverage, we do have in certain technologies fades away. It is generally a better bet to build on our strengths than try to weaken others.

Those US strengths include human capital educated in the world's top research institutions; an environment that attracts the most talented people to learn, stay, and invest here; and a vibrant commercial technology enterprise that is helping revive high-value manufacturing in this country.[60] But government cannot simply get out of the way. It must invest in a more pragmatic strategy for technology that transcends the pandemic and sustains US leadership in the post-COVID-19 world.

NOTES

1. Thomas Friedman, *The World Is Flat* (New York: Farrar, Straus and Giroux, 2005).

2. Kirk Lancaster, Michael Rubin, and Mira Rapp-Hooper, "Mapping China's Health Silk Road," *Asia Unbound* (blog), Council on Foreign Relations, April 10, 2020, https://www.cfr.org/blog/mapping-chinas-health-silk-road.

3. Chad P. Bown, "COVID-19: China's Exports of Medical Supplies Provide a Ray of Hope," Peterson Institute for International Economics, March 26, 2020, https://www.piie.com/blogs/trade-and-investment-policy-watch/covid-19-chinas-exports-medical-supplies-provide-ray-hope.

4. Milton Mueller, "Internet Governance," in *Oxford Research Encyclopedias: International Studies* (International Studies Association and Oxford University Press, 2017), https://oxfordre.com/internationalstudies/internationalstudies/view/10.1093/acrefore/9780190846626.001.0001/acrefore-9780190846626-e-245.

5. Mueller, "Internet Governance."

6. Gordon M. Goldstein, "The End of the Internet?" *The Atlantic*, July/August 2014, https://www.theatlantic.com/magazine/archive/2014/07/the-end-of-the-internet/372301/.

7. Jeff John Roberts, "The Splinternet Is Growing," *Fortune*, May 29, 2019, https://fortune.com/2019/05/29/splinternet-online-censorship/.

8. Matt Burgess, "What Is GDPR? The Summary Guide to GDPR Compliance in the UK," *Wired*, March 24, 2020, https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018.

9. Burgess, "What Is GDPR?"

10. Mehdi Daoudi, "Beware the SplinterNet—Why Three Recent Events Should Have Businesses Worried," *Forbes*, July 12, 2018, https://www.forbes.com/sites/forbestechcouncil/2018/07/12/beware-the-splinternet-why-three-recent-events-should-have-businesses-worried/#59ad890a2c00.

11. Merrit Kennedy, "New Russian Law Gives Government Sweeping Power over Internet," NPR, November 1, 2019, https://www.npr.org/2019/11/01/775366588/russian-law-takes-effect-that-gives-government-sweeping-power-over-internet.

12. Elizabeth Schulze, "Russia Just Brought in a Law to Try to Disconnect Its Internet from the Rest of the World," CNBC, November 1, 2019, https://www.cnbc.com/2019/11/01/russia-controversial-sovereign-internet-law-goes-into-force.html.

13. Schulze, "Russia Just Brought in a Law."

14. Elizabeth C. Economy, "The Great Firewall of China: Xi Jinping's Internet Shutdown," *Guardian*, June 29, 2019, https://www.theguardian.com/news/2018/jun/29/the-great-firewall-of-china-xi-jinpings-internet-shutdown.

15. "FAQ," root-servers.org, accessed June 24, 2020, https://root-servers.org/faq.html.

16. Wei Sheng, "China's Imaginary Root Server to Fix Imaginary Threat," *TechNode*, December 24, 2019, https://technode.com/2019/12/24/chinas-imaginary-root-server-to-fix-imaginary-threat/.

17. Xinhua News Agency, "China Greenlights Establishment of Root Server," December 8, 2019, http://www.xinhuanet.com/english/2019-12/08/c_138613999.htm.

18. "Search Engine Market Share Worldwide," Statcounter GlobalStats, accessed June 24, 2020, https://gs.statcounter.com/search-engine-market-share.

19. "Number of Internet Users in China from December 2008 to March 2020," *Statista*, released April 2020, https://www.statista.com/statistics/265140/number-of-internet-users-in-china/#:~:text=As%20of%20the%20first%20quarter,app%20market%20in%20the%20country.&text=In%202018%2C%20China%20accounted%20for,four%20billion%20internet%20users%20worldwide.

20. Lindsay Gorman, "The U.S. Needs to Get in the Standards Game with Like-Minded Countries," *Lawfare*, April 2, 2020, https://www.lawfareblog.com/us-needs-get-standards-game-minded-democracies.

21. Rob Portman et al., letter to US Secretary of State Michael R. Pompeo, March 11, 2020, https://www.portman.senate.gov/sites/default/files/2020-03/China%20Warren%20AI%20Letter_0.pdf.

22. Gorman, "U.S. Needs to Get in the Standards Game."

23. Doug Fuller, *Cutting off Our Nose to Spite Our Face: US Policy towards China in Key Semiconductor Industry Inputs, Capital Equipment, and Electronic Design Automation Tools* (forthcoming July 2020).

24. Fuller, *Cutting off Our Nose.*

25. Eric Geller, "Trump Signs Order Setting Stage to Ban Huawei from U.S.," *Politico*, May 15, 2019, https://www.politico.com/story/2019/05/15/trump-ban-huawei-us-1042046.

26. Carrie Mihalcik, "FCC Bars Huawei, ZTE from Billions in Federal Subsidies," *CNET*, November 22, 2019, https://www.cnet.com/news/fcc-bars-huawei-zte-from-billions-in-federal-subsidies/.

27. Sean Keane, "Huawei Ban Timeline: US Companies Allowed to Work with Huawei on 5G Standards," *CNET,* June 17, 2020, https://www.cnet.com/news/huawei-ban-full-timeline-us-restrictions-china-trump-executive-order-security-threat-5g-commerce/.

28. Fuller, *Cutting off Our Nose.*

29. Justin Sherman, "The UK Is Forging a 5G Club of Democracies to Avoid Reliance on Huawei," Atlantic Council (blog), June 2, 2020, https://www.atlanticcouncil.org/blogs/new-atlanticist/the-uk-is-forging-a-5g-club-of-democracies-to-avoid-reliance-on-huawei/.

30. David McCabe, "Senate Faults Oversight of Chinese Telecom Companies in U.S.," *New York Times*, June 9, 2020, https://www.nytimes.com/2020/06/09/technology/senate-china-telecom-security.html.

31. Harris, Wiltshire and Grannis LLP, "President Trump Formalizes Team Telecom Process for Reviewing Foreign Investments in U.S. Telecommunications Market," HWG advisory, April 9, 2020, https://www.hwglaw.com/president-trump-formalizes-team-telecom-process-for-reviewing-foreign-investments-in-u-s-telecommunications-market/.

32. Justin Sherman, "Senate Report Finds Poor Executive Branch Oversight of Chinese State-Owned Telecoms," *Lawfare* (blog), June 17, 2020, https://www.lawfareblog.com/senate-report-finds-poor-executive-branch-oversight-chinese-state-owned-telecoms.

33. Claudia Adren, "Chinese Biotechnology Dominates the U.S. Senate Hearing on Biological Threats," *Hometown Preparedness News*, November 19, 2019, https://homelandprepnews.com/countermeasures/40093-chinese-biotechnology-dominates-u-s-senate-hearing-on-biological-threats/

34. "The Next Biotech Superpower," *Nature Biotechnology* 37, no. 11 (November 2019): 1243, https://www.nature.com/articles/s41587-019-0316-7.

35. "The Next Biotech Superpower."

36. "The Coronavirus and America's Small Business Supply Chain," testimony of Rosemary Gibson before the US Senate Committee on Small Business and Entrepreneurship, March 12, 2020, https://www.sbc.senate.gov/public/_cache/files/1/c/1c39a1bc-f22c-4178-951e-29b92dcb2182/3AD9C94FB267763A83913E2303A6A772.gibson-testimony.pdf.

37. Jeff Ferry, "It's Time to Rebuild Domestic Drug Production in the US, for Both Health and Economic Reasons," *IndustryWeek*, March 17, 2020, https://www.industryweek.com/the-economy/article/21126380/its-time-to-rebuild-domestic-drug-production-in-the-us-for-both-health-and-economic-reasons.

38. "Coronavirus and America's Small Business Supply Chain," testimony of Rosemary Gibson.

39. Ferry, "It's Time to Rebuild Domestic Drug Production."

40. World Health Organization, *China Policies to Promote Local Production of Pharmaceutical Products and Protect Public Health* (Geneva: World Health Organization, 2017), https://www.who.int/phi/publications/2081China020517.pdf?ua=1.

41. Michael Rea, "An 'America First' Pharma Supply Chain Sounds Good. But It Won't Work," *STAT,* June 17, 2020, https://www.statnews.com/2020/06/17/an-america-first-pharma-supply-chain-sounds-good-but-it-wont-work/; "HHS, Industry Partners Expand U.S.-based Pharmaceutical Manufacturing for COVID-19 Response," MedicalCountermeasures.gov, accessed June 24, 2020, https://www.medicalcountermeasures.gov/newsroom/2020/phlow-us-manufacturing/.

42. Ana Swanson, "Coronavirus Spurs U.S. Efforts to End China's Chokehold on Drugs," *New York Times*, March 11, 2020, https://www.nytimes.com/2020/03/11/business/economy/coronavirus-china-trump-drugs.html.

43. Rea, "'America First' Pharma Supply Chain."

44. Bown, "COVID-19."

45. Rea, "'America First' Pharma Supply Chain."

46. Bown, "COVID-19."

47. Alice Su, "Faulty Masks, Flawed Tests: China's Quality Control Problem in Leading Global COVID-19 Fight," *Los Angeles Times*, April 10, 2020, https://www.latimes.com/world-nation/story/2020-04-10/china-beijing-supply-world-coronavirus-fight-quality-control.

48. Emma Newburger, "Cuomo Calls PPE Shortages a National Security Issue: 'You Can't Be Dependent on China,'" CNBC, May 3, 2020, https://www.cnbc.com/2020/05/03/coronavirus-cuomo-warns-against-dependence-on-china-for-ppe.html.

49. Caleb Watney and Alec Stapp, "Masks for All: Using Purchase Guarantees and Targeted Deregulation to Boost Production of Essential Medical Equipment," policy brief, Mercatus Center, George Mason University, April 8, 2020, https://www.mercatus.org/publications/covid-19-crisis-response/masks-all-using-purchase-guarantees-and-targeted-deregulation.

50. Nick Miroff, "Protective Gear in National Stockpile Is Nearly Depleted, DHS Officials Say," *Washington Post*, April 1, 2020, https://www.washingtonpost.com/national/coronavirus-protective-gear-stockpile-depleted/2020/04/01/44d6592a-741f-11ea-ae50-7148009252e3_story.html.

51. Kristine Lee and Martijn Rasser, "China's Health Silk Road Is a Dead-End Street," *Foreign Policy*, June 16, 2020, https://foreignpolicy.com/2020/06/16/china-health-propaganda-covid/.

52. Lee and Rasser, "China's Health Silk Road."

53. Lancaster, Rubin, and Rapp-Hooper, "Mapping China's Health Silk Road."

54. Lee and Rasser, "China's Health Silk Road."

55. Jeff Grabmeier, "Chinese, American Scientists Leading Efforts on COVID-19," *Ohio State News*, May 26, 2020, https://news.osu.edu/chinese-american-scientists-leading-efforts-on-covid-19/.

56. Stuart Anderson, "Inside Trump's Immigration Order to Restrict Chinese Students," *Forbes*, June 1, 2020, https://www.forbes.com/sites/stuartanderson/2020/06/01/inside-trumps-immigration-order-to-restrict-chinese-students/#4d29bf4b3bec.

57. Andrew Silver and David Cyranoski, "China Is Tightening Its Grip on Coronavirus Research," *Nature*, April 15, 2020, https://www.nature.com/articles/d41586-020-01108-y.

58. Gavin Yamey and Dean T. Jamison, "U.S. Response to COVID-19 Is Worse than China's, 100 Times Worse," *Time*, June 10, 2020, https://time.com/5850680/u-s-response-covid-19-worse-than-chinas/.

59. Matina Stevis-Gridneff, "E.U. May Bar American Travelers as It Reopens Borders, Citing Failures on Virus," *New York Times*, June 23, 2020, https://www.nytimes.com/2020/06/23/world/europe/coronavirus-EU-American-travel-ban.html?smid=tw-nytimes&amp;smtyp=cur.

60. Richard Danzig, John Allen, Phil DePoy, Lisa Disbrow, James Gosler, Avril Haines, Samuel Locklear III, James Miller, James Stavridis, Paul Stockton, and Robert Work, *A Preface to Strategy: The Foundations of American National Security* (Laurel, MD: Johns Hopkins University Applied Physics Laboratory, 2018), https://www.jhuapl.edu/Content/documents/PrefaceToStrategy.pdf.

This page intentionally left blank