A World Divided:
The Conflict with Chinese Techno-Nationalism Isn't Coming – It's Already Here

Four years ago, Chinese President Xi Jinping told an elite audience at the World Economic Forum at Davos that "integration into the global economy is a historical trend," asserting that "[a]ny attempt to cut off the flow of capital, technologies, products, industries and people between economies … runs counter to the historical trend." This year at Davos, speaking via video-teleconference because of the novel coronavirus outbreak, Xi was calling a very different tune, warning that other countries should not try to "start a new Cold War, to reject, threaten or intimidate others, to willfully impose decoupling, supply disruption or sanctions, and to create isolation or estrangement [which] will only push the world into division and even confrontation."

President Joe Biden's incoming trade and national security teams will face a number of urgent choices as they sift through the wreckage of the Trump administration, and few are more important than deciding which — if any — of the previous administration's China-focused trade and export control policies should continue into the new term. Although the early signs are that Biden's China team is bringing a deep bench of talented and experienced public servants, in the realm of technology policy, they will be inheriting a geopolitical landscape that has transformed dramatically since the last Democratic administration four years ago. Understanding what has changed will be key to ensuring that the United States remains a global technology leader so it can both "build back better" its domestic industries and counter Beijing's problematic behavior.

The last Democratic administration held power during an era of technological globalism, marked by the fluid movement of supply chains and unfettered information flows. While global supply chains remain critically important, especially given record trade deficits, the renewed techno-nationalism by Beijing and a bruising trade war mean the landscape has been permanently altered. It is now a complex world of rampant cyber and technology espionage, "splinternets," and national barriers to data flows. The emerging world is increasingly divided between rival technology **spheres of information** and communications technology ranging from hardware and software to banking and payment systems that form the superstructure of both core institutions and individual daily lives. **One ecosystem**, dominated by China, features Chinese firms that are either implicitly or explicitly controlled by the state, creating technology for both a protected domestic market and for international export. On the other side, by contrast, is a more amorphous technology environment. It stretches across the Organization for Economic Co-operation and Development (OECD) countries and is dominated largely by Western equivalents (with some limited Chinese penetration), though its regulations and norms remain in flux as various countries and political movements debate how the social contract should change to accommodate modern information technology.

The edges where these two spheres meet are now a persistent site of conflict, with the demands of global interconnectivity and supply chains chafing against a range of trade and export security concerns. For the U.S. government, this world presents new and difficult challenges, especially regarding how to promote growth and trade while at the same time protecting American technology from illegal export and theft. While it may have diagnosed critical structural problems correctly, the Trump administration did many things wrong in strategy and execution.

It didn't work with allies and overreached in many areas. But the Biden team can't just go back to the way things were done before or simply implement what industry would prefer. It needs to chart out its own independent course that considers the national interest and the interests of the people, not just those of corporate America. What's good for Silicon Valley or Wall Street's quarterly numbers is no longer necessarily what is good for America's long-term technological or industrial interests.

The bottom line is that long-term competition with China is here to stay and the best defense is a good offense. Of course, the United States needs to invest in innovation, workforce, and supply chains, and the Biden administration's "Build Back Better" innovation plans are an excellent move in that direction. But no team can win on offensive prowess alone. It needs defense, too. The United States needs to protect its innovation base from China and cannot blindly allow its technological advantage to be acquired by China's state-owned enterprises and "national champions." The incoming Commerce Department leadership, for example, needs to use export controls to carefully restrict critical technology from Beijing and to shape behavior. Yet, export controls are not always the best tool. Sometimes the best tools will be economic sanctions, reviews by the Committee for Foreign Investment in the United States, or domestic R&D investments. The incoming administration needs to carefully assess when export controls are the right tool and when it needs to use other, more effective regulatory tools or elements of national power.

How the United States Got Here

It wasn't so long ago that technological globalism dominated the international landscape, particularly among the "Davos set." Futurists of the "Fourth Industrial Revolution" predicted that borders and national sovereignty would become less relevant, supplanted by international communities united around transnational social media platforms and supply chains. Large technology corporations were becoming "multinational" in every sense of the word, moving their headquarters to whichever nation offered the most advantageous tax code and resisting national efforts to regulate their conduct. The "globalized" supply chain for information technology was in fact heavily reliant on specific choke points, including component assembly in the People's Republic of China and semiconductor manufacturing in Taiwan.

Although the cracks in this global system are now visible for all to see, the first fissures became visible much earlier in China. Its Great Firewall has morphed over time from a clunky anachronism into a startlingly efficient surveillance model for "digital authoritarianism" around the world. When the 2008 financial crisis shook global confidence in the U.S. financial system, China seized the initiative to push for alternatives to U.S.-led global institutions, launching frameworks such as the Asian Infrastructure Investment Bank and the Belt and Road Initiative. Before long, these "Chinese alternatives" intertwined with China's broader push for cyber sovereignty. In 2013, the revelations of Edward Snowden raised serious questions for governments across the globe about the risks associated with the national origins of hardware and software, shattering global confidence in the international ICT standards regime and driving a major shifts toward the pursuit of domestic supply chain security, data localization, and privacy regimes (such as the European Union's General Data Protection Regulation, or GDPR). During the Trump era, China was frankly able to capitalize on global loss of confidence in U.S. leadership to push an alternate, fragmented vision of the digital commons.

In the United States (and increasingly in many other OECD nations), meanwhile, China's planetary-scale cyber espionage campaign and rampant theft of U.S. trade secrets reached such a crescendo that they could no longer be ignored. Even the once China-friendly U.S. business community began raising serious questions about why U.S. ICT manufacturing was so over-centralized within the borders of a country long known to be a major strategic competitor and cyber threat to the United States. These trends culminated in a series of U.S. government policy moves that began with the Obama administration's executive order on cyber sanctions and soon expanded to include the Office of the United State Trade Representative's Section 301 investigation into China's forced technology transfer practices and follow-on tariffs; the Department of Justice's "China Initiative" against economic espionage and trade secrets theft; the Department of Defense's secure supply chain efforts on semiconductors; and the National Institutes of Health's and National Science Foundation's investigations and sanctions against unreported researcher income from Chinese "talent programs." For its part, the Commerce Department undertook long-overdue regulatory moves to modernize the process of adding state-linked Chinese firms to the Entity List, modify regulations surrounding "military end use," and use the Foreign Direct Product Rule to address concerns about Huawei. During this period, Congress also moved aggressively to update foreign investment screening through the Foreign Investment Risk and Review Modernization Act and the U.S. export control regime through the Export Control Reform Act. Non-Chinese companies have naturally reacted to these actions by seeking to diversify their supply chains, and in rare cases have tried to "de-couple" from the China market.

China has flexed its own muscles in return, responding to these U.S. measures with a renewed emphasis on technology independence. In public, the key elements of its response include massive subsidies for the development of domestic technologies and support for "national champion" firms designed to both meet China's domestic technology needs and erode the global market share of Western multinationals. Quietly, China has invested immense sums of money in Silicon Valley firms with technology relevant to national security, drafting behind Pentagon investments and offering follow-on rounds of investments, in order to bring their innovations into China's industrial ecosystem. And in secrecy, China has ramped up cyber and technology espionage and extended its regulatory tentacles far deeper into private Chinese enterprises to ensure that they will function as arms of the state when national security is at stake.

The Rise of China's Technology Sphere

The United States and its partners now face an emerging world whose citizens live in one of these entirely different technology ecosystems. The residents of China's technology sphere live in cities connected by Huawei and ZTE devices and in micro-economies run through Chinese mobile payment systems like Alipay, all under the watchful eye of dense, overlapping surveillance that includes layers of CCTV, facial recognition, and big data predictive policing, though much of their tech is dependent on Western components and patents. The residents of the developed world, by contrast, live in an environment managed via Apple, Google, Cisco, Nokia, and Ericsson hardware, most of which is currently made in China, and on the large social media platforms (Facebook, Twitter, Netflix, etc.), with limited amounts of Chinese hardware and software sometimes tossed into the mix for reasons of cost and expediency.

It is tempting to generalize this as a conflict between symmetrical Chinese and Western technology spheres. But the reality is more amorphous. The United States and the European Union are deeply divided over fundamental issues related to hate speech, data privacy, and surveillance that have yet to be resolved, and relationships with key countries like Germany, Japan and South Korea need serious mending. Nevertheless, the differences between U.S. and European Union policies pale in comparison to the ways in which the OECD as a whole is at loggerheads with the Chinese approach. And so, these two spheres will continue to chafe against one another, repelling intrusions into their territory and seeking to contest unclaimed domains as new technologies such as 5G and quantum computing reach maturity. At the same time, the populations within the two spheres will still need to communicate and do business with one another. This is not a second Cold War, and even a "post-decoupling" U.S.-China relationship will be deeply economically interconnected by historical standards. The result will be continued awkward negotiations on interconnectivity at the boundaries, as well as opportunities for intelligence services to leverage that interconnectivity for all manner of espionage activities.

The Challenges for the U.S. Government

In this divided world, the U.S. government faces a range of new and difficult challenges in economic, trade, human rights, social, political, military, and diplomatic domains. Rather than overly focus on tariffs and other punitive actions, the incoming administration must strike a delicate balance, pursuing aggressive investment and, in some cases, rebuilding the United States research and technology and industrial base, while also pursuing foreign policies that seek to promote trade that is marked by mutual benefit and reciprocity. The Commerce Department will be critical to this effort, promoting U.S. opportunities in overseas markets while also protecting American technology from illegal export and theft. Key elements of a successful strategy will include:

- Refocus the Bureau of Industry and Security's security mandate to reflect a rapidly changing world in which national security, foreign policy, and ideological challenges with China are rapidly outpacing diminishing, positive-sum commercial opportunities related to China's indigenous innovation, import substitution, and "dual-circulation" strategies. As a core mission, the bureau should begin by placing the interests of the United States, its long-term economic vitality, and its people ahead of the near-term financial interests of Silicon Valley, Wall Street, and other multinationals, which are not always aligned with U.S. interests.
- Integrate the export control agenda into the domestic "build back better" agenda of revitalizing the American economy and industrial base. The old view of export controls as solely designed to address narrow counter-proliferation goals does not match the current global or technology environment.
- Exercise U.S. leadership to ensure a more agile approach among small, allied groups outside of the Wassenaar Arrangement to address export control challenges focused on the areas of emerging technology, select foundational technologies (e.g. semiconductors), and human rights.

- Prioritize meaningful action on export controls vis-à-vis China at the top of the diplomatic agenda early in the Biden administration to include use of "sharp carrots" to both incentivize harmonized approaches and coordinated actions and to deter self-interested, free-riding behavior by certain allies.
- Upgrade the law governing the Committee for Foreign Investment in the United States to include scrutiny of joint ventures and increase its budget and manpower to deal with the greatly expanded caseload associated with unilateral initiation of investigations.
- Use the full range of regulatory mechanisms, including the Entity List and the Foreign Direct Product Rule (FDPR). Huawei's entity listing, coupled with the FDPR, and the entity listing of Fujian Jinhua are a clear demonstration that when certain conditions are met, export controls are an effective tool against illicit Chinese behavior that threatens the national security and foreign policy interests of the United States and its allies.
- Develop an integrated data governance framework that protects the integrity of U.S. networks and data, advances privacy, and ensures reciprocity for U.S. companies in the areas of cloud and value-added telecom platforms.

If implemented, these measures will help the new Biden administration adapt to the significant changes in the trade and security environment over the last four years and ensure its ability to achieve simultaneous goals: strengthening the American economy, accelerating the domestic innovation and job growth, deepening cooperative relationships with like-minded countries, bolstering U.S. military capabilities, and protecting critical intellectual property and core technologies of the future from wholesale technology and cyber theft.

James Mulvenon, Ph.D. James Mulvenon is a leading international expert on Chinese cyber, technology transfer, espionage, and military issues. A Chinese linguist by training, in 2013 he co-authored *Chinese Industrial Espionage*, which is the first full account of the complete range of China's efforts to illicitly acquire foreign technology. Dr. Mulvenon contributed multiple chapters to *China's Quest for Foreign Technology: Beyond Espionage*, which was published in September 2020.