GPF | GEOPOLITICAL FUTURES

Keeping the future in focus
https://geopoliticalfutures.com

Washington’s Chinese Tech Conundrum

by Phillip Orchard - November 15, 2019

In early November, the budding U.S.-China “**tech cold war**” took a rather surreal turn. The U.S. government announced a national security review on the threat posed not by Chinese telecommunications giants like Huawei or Chinese artificial intelligence firms developing battlefield applications for the People’s Liberation Army, but rather by TikTok, a wildly popular Chinese social media platform best known for 15-second clips of Gen Zers (those born between 1996 and 2010) **doing very Gen Z things**. Last week, U.S. Senate Minority Leader Chuck Schumer pressed the secretary of the Army to refrain from using TikTok as a recruiting tool.

The supposed threat has to do with data. With some 500 million users, including 80 million in the United States, TikTok is collecting a ton of data. TikTok is owned by ByteDance, a private Chinese firm, and it’s not even available inside China. But since even private firms in China have little choice but to cooperate with the Communist Party of China’s demands, Beijing could ostensibly use the app to, say, monitor the movements of intelligence targets. Such concerns are not wholly invalid. After all, even U.S.-based tech giants are under mounting scrutiny over the oceans of user data they can hoard.

This illustrates a fundamental feature of U.S.-China competition: Given the blurring lines between commercial and military or intelligence technologies, it’s not hard to come up with reasons why just about *any* **emerging Chinese technology could threaten U.S. interests**. Chinese 5G infrastructure, for example, could ostensibly be weaponized to divert sensitive data to Beijing or wreak havoc on U.S. military logistics and communications lines just as the **PLA makes its move on Taiwan**. Chinese-made train cars could be rigged to paralyze major U.S. cities. Chinese-made smart refrigerators could be programmed to become sentient en masse and stage an ice boxer rebellion. (Theoretically, at least.)

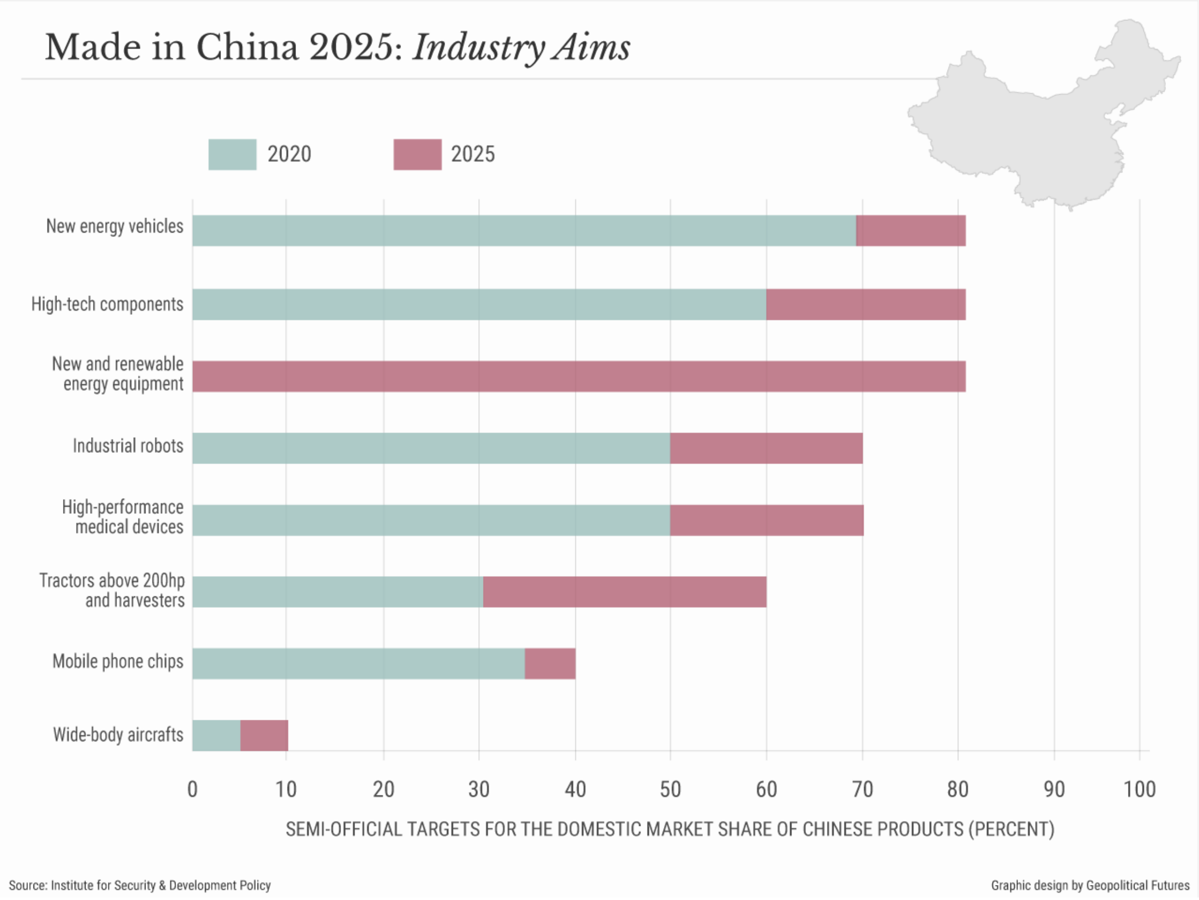
As a result, Washington is scrambling to develop a coherent approach to managing an array of threats that’s extremely unclear in both scope and severity. Just as problematic, Washington’s ability to mitigate such threats without doing more harm than good to U.S. interests is similarly murky. Bottom line: The U.S. will struggle to strike an ideal balance, but the broader geopolitical competition will push the U.S. to err on the side of mitigating worst-case scenarios – however real or imagined.

Three Uncertainties

Over the next few months, using new powers granted by the **Export Control Reform Act of 2018**, the U.S. Commerce Department is expected to clarify what Chinese “emerging and foundational technologies” it truly considers problematic. It will also continue laying the groundwork for concrete measures to address them, including export controls, import bans, restrictions on investment and research and development collaboration, and so forth. This task is complicated by three sources of uncertainty.

The first question, of course, is just how much any particular Chinese technology – or even U.S. technologies manufactured in China – can realistically harm U.S. national security. Some are fairly obvious; the U.S. has ample interest in keeping Chinese nationals from swiping research from U.S. biotech labs, for instance, or in depriving Chinese weapons-makers of cutting-edge U.S. semiconductors and software. Undeniably, Chinese advances in quantum computing, artificial intelligence, robotics, aeronautics, space and so on have the potential to diminish the U.S. military’s conventional edge over the PLA.

But with most other Chinese tech and advanced manufacturing firms in the U.S. crosshairs, the threat is largely theoretical at this point. Even **concerns about 5G** hinge largely on a range of assumptions about how quickly and widely the technology will be adopted, what sorts of applications it spawns, and the difficulty developing sufficient cybersecurity measures such as encryption. There’s also a tendency to overrate China’s innovative capacity. Beijing is helping Chinese firms narrow the gap with the U.S. in R&D spending, sure, but the **innovation record of Chinese firms** (particularly bloated state-owned enterprises) has been mixed, at best. The U.S. and its high-tech allies in Northeast Asia and Europe have a decadeslong lead in most sectors, and China cannot close the gap through forced technology transfers or cyberespionage alone.



(***click to enlarge***)

The second question is whether the U.S. really has the tools to address potential threats. U.S. tools can be lumped into two categories: defensive and offensive. Implementing most defensive measures would be relatively straightforward. The U.S. could, for example, simply prohibit members of its military, intelligence community, and other sensitive departments from using data-hoarding Chinese apps like TikTok – or just ban such apps from the U.S. altogether. Already, it’s effectively banned Chinese telecommunications equipment from U.S. networks. It’s also likely to do more to encourage the development (and widespread adoption) of more sophisticated encryption and cybersecurity practices.

But defensive measures won’t cover everything. All telecommunications networks, with or without Chinese tech, will be inherently vulnerable to Chinese cyber operations. Moreover, U.S. interests aren’t confined to U.S. shores. Thus, the U.S. is also toying with offensive measures effectively aimed at taking down potentially problematic Chinese firms altogether. This is the point of the onagain, off-again controls on exports of U.S. components and software to Huawei, which relies overwhelmingly on U.S. semiconductors, software and chip design – as well as the diplomatic offensive aimed at keeping Huawei equipment out of places the U.S. relies on for military logistics. When the U.S. briefly slapped an export ban on Huawei's state-owned rival, ZTE, in May 2018, it nearly brought the firm to its knees.

However, there are several reasons to doubt the effectiveness of offensive measures like export controls. For one, it only really works if a Chinese firm is truly dependent on U.S. technology, market access or funding. And the U.S. has near-total dominance over only a small number of sectors, such as semiconductors. For another, as demonstrated this summer when several U.S. suppliers announced that they had exploited loopholes in the soft ban on sales to Huawei, private multinational firms would have overwhelming incentives to find ways to continue selling to China – even if it requires moving operations overseas. Finally, it's unclear how long Chinese dependence on U.S. firms will actually last. A core reason why Chinese firms like Huawei and ZTE have struggled to make the leap in sectors like semiconductors is that it just always made more sense to keep buying from the U.S. and focus their resources on what they're actually good at (or on serving Beijing's political and diplomatic goals). Cut off from critical suppliers, such firms would come under enormous pressure to develop suitable replacements – while Beijing ensures that they don't wither and die in the meantime. It may sound trite, but necessity really is the mother of innovation.

More Harm Than Good?

This highlights the third source of uncertainty: Can the U.S. go after Chinese firms without doing more harm than good to U.S. interests in the process? The reality is: Most proposed U.S. measures would carry major potential risks and costs – to U.S. consumers, to U.S. diplomatic relationships, or to the health and innovative capacity of the U.S. firms that Washington would ostensibly be trying to protect. It's estimated, for example, that between 10 percent and 30 percent of the revenues of leading U.S. firms like Intel, Advanced Micro Devices and Qualcomm come from China. Every semiconductor they can't sell to Huawei is less revenue for them to sink into R&D. As mentioned, there's also the thorny fact that the U.S. has a monopoly on only a handful of technologies. So, there'd be little point in banning sales to China in industries where tech is already widely available. Indeed, **U.S. export controls** on globally available satellite technologies in the 1990s were deemed counterproductive.

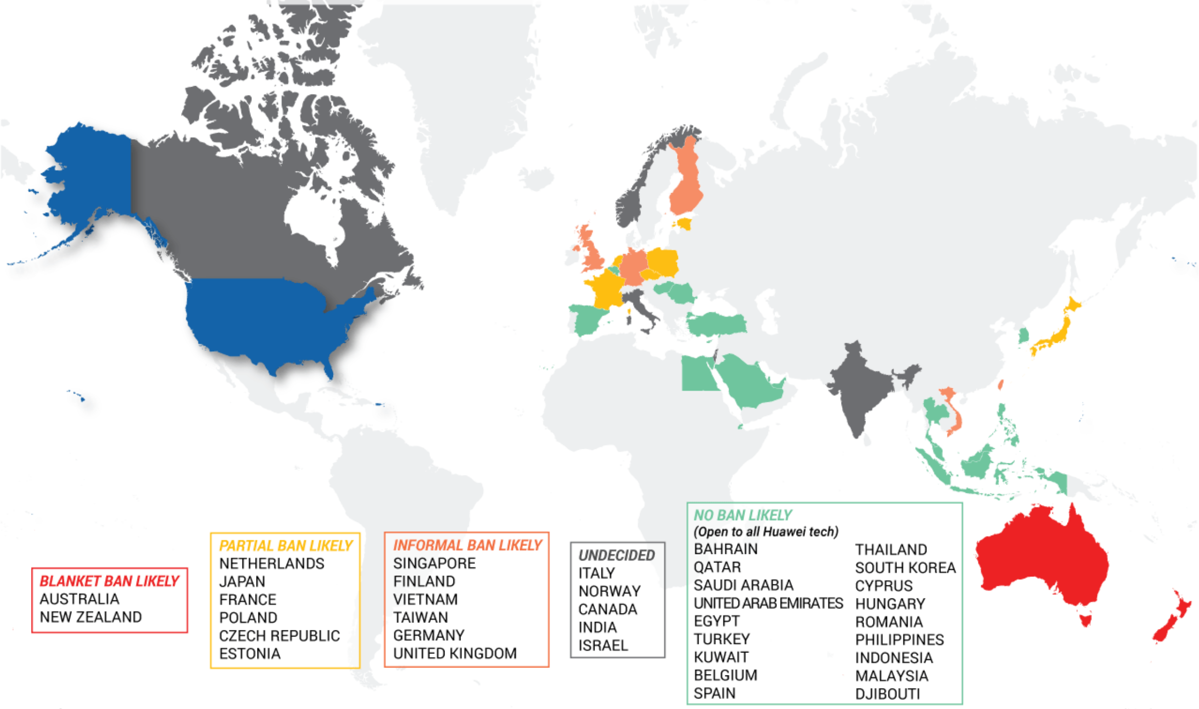
Meanwhile, Silicon Valley startups would suffer from the loss of Chinese investment. A core U.S. strength, moreover, is its ability to attract the best and brightest from other countries, so a U.S.

crackdown on Chinese immigrants, students and research collaboration wouldn’t be cost free. Already, the threat of additional U.S. tariffs, along with potential bans on federal procurement of ITC equipment with components made in China, has forced U.S. electronics makers with manufacturing operations **in China to spend billions rerouting complicated supply chains elsewhere. Chinese** retaliation would be inevitable, whether in the form of reciprocal sanctions, nationalist consumer boycotts, harassment of U.S. firms in China or the ever-looming ban on **rare earths exports**.

Finally, there could be costs to the U.S. diplomatic and alliance structure. With 5G, for example, **the U.S. has effectively threatened** to curtail intelligence and military cooperation with countries that use Huawei telecommunications equipment. For most countries, caving to the U.S. would be breathtakingly expensive and delay their 5G rollout by several years. (Many use Huawei for 4G, meaning they’d need to rip out old infrastructure in addition to taking on the vast buildout required for 5G – and do so with more expensive suppliers.)

Reluctance to Ban Huawei Technology

How have countries hosting U.S. troops and other potential key U.S. partners responded to U.S. calls to ban Huawei from 5G networks?



Source: Defense Manpower Data Center

© 2019 Geopolitical Futures

*(**click to enlarge**)*

The underlying problem for the U.S. is that preparing for potential tech threats means estimating the power of technological applications that often don't even yet exist – and tech innovation moves fast. When faced with an unclear emerging threat, the U.S. tends to ignore the problem before overcorrecting to overwhelm it with blunt power. Ideally, the solution for the U.S. would be a "small yard, high fence" approach that preserves national security without undermining its own ability to innovate and compete in global markets – and without upending its invaluable global alliance structure. But the threat environment is simply too murky, too dynamic and too laden with potential for unintended consequences for the U.S. realistically to be able to strike an optimal balance anytime soon.

The problem for China, meanwhile, is that it can do little to allay U.S. fears of worst-case scenarios. Chinese firms can promise to refuse state demands for cooperation, but it'd be naive to put much faith in that. They can open up their source code to foreign inspectors, but source code can quickly change. China certainly can't abandon its **attempt to scramble up the manufacturing value chain** or **turn the PLA into a high-tech fighting force**. So, the issue cannot be separated from the broader suspicions and colliding interests that will define U.S.-China relations for decades to come. To the U.S., in other words, it's perfectly rational to consider depriving a potential adversary of capabilities that might prove dangerous – however blunt and potentially destructive. And given the trajectory of Chinese firms and the possibility that U.S. leverage may soon evaporate, Washington will be tempted to strike fast and ask questions later.

Author: Phillip Orchard
Read more from this author on geopoliticalfutures.com