The U.S., China, and the Technology Cold War: How Washington and Beijing are Shaping the Future of Technology

Adam Segal
Director of the Digital and Cyberspace Policy Program
Council on Foreign Relations


Transcript has been edited for clarity.

What I’m going to do today is talk about U.S.-China tech competition. I’m going to talk about how we got here, and in particular what’s shifted with both countries so that they both began to see science and tech competition as increasingly important to the competition between the two of them. I’ll talk a little bit about what we’re seeing and how that competition is playing out. And then I’ll end with some kind of speculative thoughts about how we might think about, “Could there be a winner in this competition?”, or to put it another way, “Who loses less from this competition?”

So, how we got here. I think [Tom Fingar] hinted at this [in his introduction], that there were probably no two countries that benefited more from the globalization of science and technology than the United States and China. China, of course, starting in 1978, came out of wanting to reform a type of technology system that was based on the Soviets’. [China] knew that it had already missed a wave of technological innovation and wanted to ensure that it didn’t miss the next wave. So, it began reforming the domestic science and technology system, but also increasingly relying on outside sources of technology – outside money and outside people and ideas. And those outside influences really had a dramatic impact on Chinese innovation and really helped the Chinese move up the value chain very, very quickly.

On the U.S. side, the U.S. innovation system has also benefited immensely from the access to people and ideas. We’ve been hearing for decades about the weaknesses in science and education, [and] math training at the high school level. And one of the ways the United States managed to build that kind of a detour run, that problem, was to import that talent. Places like Stanford and M.I.T. and every other major university in the United States [have] really been able to exploit talent from China, India and other places. The impact of Chinese and Indian immigrants on the [Silicon] Valley, of course, has been talked about, [as has] the role that they’ve played on entrepreneurship and innovation.

So, both countries benefited immensely from this globalization of science and technology, and around the same time, both countries began having serious doubts about it. And I do want to stress that this was both countries. We tend to frame it as the Trump administration reacting to China. But China itself had also began to think about, in particular, its role in the global economy. Chinese policymakers were unhappy and remain unhappy about being the “factory to the world.” [Being grounded on] energy intensive, labor intensive, polluting industries was not where it wanted to be stuck. They wanted to move up the value chain, and it was increasingly worried about dependence on foreign suppliers for critical technologies.

This has been a longstanding worry of the Chinese leadership, and this [worry about dependence on foreign input] certainly focused in the 1980s and 90s. And in 2006, China introduced the Mid- to Long-Term Program on science and technology. It introduced the idea of indigenous innovation, it sets metrics
for China becoming a science power and technology power, [and] it sets metrics for reducing dependence on foreign technology. And so, the Chinese also began to think about how they fit into this global system.

The other major shock to the sight of the Chinese system was the Snowden revelations. The revelations from the NSA contractor started showing the ability of the US to exploit technology platforms. China had long assumed there were back doors in U.S. products that provided the NSA and U.S. intelligence agencies access to networks in China. And so, when Snowden basically reinforced that belief, they began thinking about how [to] reduce that dependence, especially in critical information technologies, in I.T., and how do you begin pushing foreign suppliers out [and] replacing them with domestic producers?

So, Snowden, the Mid- to Long-Term Plan, and then I think the Made in China 2025 [initiative all] continue this idea that these new technology sectors tend to be zero sum, that the first mover gains humongous advantages, that there are massive network effects, and [that] the countries that control those technologies are the ones that are going to dominate these important sectors. So, [it’s] a very zero-sum idea about technology and technology competition, [and] I think [it] became very prominent among many Chinese policymakers and Chinese analysts.

On the U.S. side, we had an earlier debate about the rise of China. In the end of the 2000s, around 2007, the National Academies produced a report called The Gathering Storm, which talked about the globalization of science and the rise of China and India in particular as science competitors. But even in that report, the idea that China was going to compete on cutting-edge technology seemed to be several decades away. There was, I think, still a pretty robust discussion about [cutting edge, especially in certain areas of A.I.] So [we’ve seen] a shift in the competitive capabilities [of] China. Second, of course, under the Trump administration, [is] a focus on a great power competition, and science and technology being part of that. So, [that’s] parallel to the shift in Chinese thinkers about zero-sum competition on the US side, [including] a real focus on international relations being increasingly zero-sum and [being] defined by great power competition.

And then finally, a sense that the openness of U.S. science and technology was being exploited, that the Chinese had for a long time been exploiting both the openness of American universities, American networks, [and] other places, and [now] you needed to start thinking about, “How do you stop that flow of technology?” Now, again, this is not only the Trump administration; you can see some of these thoughts starting to percolate through at the end of the Obama administration.

In particular, a report that PCAS did (the President’s Council on Science and Technology Advice) on semiconductors – that report, [which was] reported at the end of Obama administration, talks about China’s mergers and acquisitions with semiconductors, [about] taking advantage of market forces to move up the value chain with semiconductors and what the U.S. would need to do [to accomplish that]. That report comes down on the conclusion that we need to run faster, but it was certainly sensitive to the idea that China was acquiring technologies both illegally and legally.

And then the report that came out of the Defense Innovation Unit which looked at Chinese investment in the [Silicon] Valley, in particular, and in a range of emerging technologies [such as] quantum and A.I. So, at the end of the Obama administration, you were clearly beginning to see this is worry about openness and [about] China moving up the value chain.
So, on both sides, I would say [there is] a real ideational shift and an increasing tendency to see conflicting interests on the technology side. So, I think [that’s] what happened and [explains] how we got here. What we’ve seen on the U.S. side is a real attempt to try and stop the flow of technology out of the United States and to slow Chinese growth.

[In regards to addressing concerns about the flow of technology], the Trump administration is focused on a number of areas. The first was on foreign investment in the United States. So, [they’ve made] reforms to the Committee on Foreign Investment in the United States (CFIUS) to expand CFIUS’s review to [include] a broader range of technologies and look at different types of purchases — including minority shares — [and to] reform the export control laws [to be broader] and [to] look at emerging technologies. We’re seeing now that process of [defining] what these technologies are, especially in machine learning and AI, and how we draw the line between military use and civilian use.

[We are also seeing] a prolonged campaign against Huawei, the Chinese telecom company. First, [there was a] focus on making sure Huawei was not in U.S. networks. So, first [came] blocking contracts with [the] Department of Defense (DOD) and preventing Huawei phones on defense bases, then blocking access to government procurement, and now thinking about how to pull Huawei out of telecoms in rural, third, and fourth tier markets. And then using the sanctions list to try to cripple Huawei through a series of sanctions violations, IP theft and other alleged violations of U.S. law. And [now there is] a prolonged campaign to try and convince U.S. allies and friends not to use Huawei in the build out on 5G.

The [Trump] administration’s messaging on this has not been particularly effective. It has been essentially kind of a two-step process. First, it argues that 5G is a different type of security threat, [and] that you can’t deal with the 5G security threat the way you dealt with the fourth and third generations [of networking], which was primarily to try and segregate periphery networks from core networks [and to] do inspections of code [and] inspections of equipment.

The US has consistently argued that that’s not possible to do in 5G [because] there’s too much data at the peripheries [and] in the base stations, and that because there is so much software involved and the software is constantly being updated. [Because of that, they argue that] you can’t really do code checks because [if you] check it one day, the next day it’s updated [and] you’re still going to have the problem of backdoor.

So, 5G in of itself is an almost unsecurable [sic] kind of network, which means you have to rely on the provider, and you can't rely on Huawei. [And] you can't rely on Huawei for a number of reasons. One, [analysts] point to [their] history of I.D. theft and other sanctions violations. They [also] point to the 2017 National Intelligence Law, which in some readings seems to suggest that any Chinese company or entity has to serve as an espionage tool and would not be able to report it. They point to buggy software and equipment, although that is true across all 5G manufacturers. And in some cases, they’ve pointed to backdoors that were not immediately closed.

This messaging has not been effective for most of our partners except for Australia, Japan and New Zealand. I think it hasn't been particular effective for a number of reasons. I think first, for most countries the threat is [getting] spied on by the U.S. or China or both, and they have no belief that using Huawei or not using Huawei changes that. In fact, it probably means no matter what they use, they’re still going to get spied on by the U.S. or China, [so] you might as well at least get the cheap product, a good product, and roll out the 5G as quickly as possible.

So, [the message that you can't rely on Huawei] doesn't seem to be a pretty convincing argument as far as I can tell on the espionage side. The U.S. has also tried to argue that Huawei or the Chinese government could disrupt 5G networks to gain leverage over a country that wasn’t doing what it wanted to. I think there are very few countries that are seriously worried about that kind of threat. Perhaps if you
can imagine that you’d be involved in the Taiwan Straits crisis or South China Sea [crisis], then you could imagine the Chinese exerting that kind of influence. But, clearly, China has lots of ways of exerting influence on smaller countries without turning them off 5G or Internet of things devices. Using that type of tool would be a onetime thing. It would it would totally undermine Chinese technology companies internationally. It's hard for me to imagine why [China] would use those tools for most cases.

Clearly, mixed messaging from the [Trump] administration itself has not been helpful. In many cases, after U.S. officials have gone to Europe and talked about what a security risk Huawei is, the president will then tweet that he's willing to do business with anyone. [That] reinforces in European partners’ minds that this is really an economic competitiveness issue and not a security issue.

And then finally, the decision by the British to say, “We can, in fact, segregate the risk. We can push it out to the to the periphery and reduce Huawei’s presence both in the sector and in the networks overall and in the core. And we can have an adequate level of security,” seriously undermines the US’s ability to convince other allies.

The final step of the U.S. reaction, [which] Tom mentioned in his introduction, [is what] the Department of Justice [broadly calls the] China Initiative, and this includes a cyber component. We’ve seen the Department Justice start to indict Chinese hackers for cyber-enabled theft of intellectual property. They’ve alleged that Chinese hackers were behind the attack on Equifax and behind attacks on I.T. services and clouds through an operation called Cloud Hopper.

And we’re seeing a crackdown on academics involved in the Thousand Talents Program and [other] such efforts to lure foreign and Chinese expertise back to China. Many of those cases seem to be people that are double-dipping — not necessarily involved in espionage — but [people who] are taking two salaries, not reporting their salary, and reproducing some of the research that they’re doing in the United States in their labs in China. So, we’re seeing a closer look at those collaborations, [and] who’s being transparent about them and who’s reporting on them. So, [there’s] a real attempt on the U.S. side to try and stop the flow of external technology.

The final component which we don’t know very much about and [which] is purely speculative is [thinking about a potential] shift to a more disruptive set of actions [on the cyber side of things]. Cyber command has talked about persistent engagement in forward defense; they talk about stopping attacks before they get to U.S. networks [by] operating in what's called gray space, [meaning] the space between Chinese networks and U.S. networks. The primary leaks about those operations have been focused on Russian influence operations. But before John Bolton left the White House, he gave a talk at one of the D.C. think tanks [where he said that the U.S. is] engaged in those type of types of operations against Chinese hackers as well. So, we don’t know what that disruption looks like, and we don't know if it’s likely to be more disruptive.

On the Chinese side: as I’ve said, China has a long-standing concern for dependence on foreign technology and its worry about where it sits in global supply chains. And the primary response, of course, has been Chinese spending on research and development, science and technology. China went from spending about 1.1% of GDP to close to 2.5%. Now [China] spends more than the E.U. and Japan do on research and development, and, depending on how you measure the purchasing power parity or just market exchange, will soon catch [up to] the United States.

So, I don't think we should seriously doubt that the Chinese are spending significant resources. This has been a primary concern [of theirs], and we’ve seen a huge focus on these critical emerging technologies. [There’s] lots of writing, of course, about the AI strategy inside of China and on quantum, and on the increasing coordination with Chinese tech companies as national champions in this space.
The second tool the Chinese have is the Belt Road Initiative and terrific diplomacy. So, they’re expanding Chinese connections and science and technology diplomacy along the Belt and Road; the Chinese Academy of Science now has agreements [with] and a Belt and Road Center [within] it. [The Academy] is doing more training and setting up research labs along the Belt and Road. The investment in the first wave of the Belt and Road is primarily hardware — fiber optics, satellite communication — and now we are seeing the expansion out into e-commerce [such as] Ali Baba in Malaysia and other places, Fintech in particular, and then smart cities, which also, of course, means surveillance technology.

So, studies done out of Carnegie and other places show that China tends to be the dominant supplier (not [the] only supplier, but the dominate supplier) of surveillance cameras, artificial intelligence, and other types of surveillance technology along the Belt and Road, and in other developing areas. Along with this new commercial diplomacy is a focus on international standards and how you shape those standards. And so on the Chinese firms side, we’ve seen a massive expansion of attendance at International Standards Forum, in particular the role that ZTE and Huawei have played in the 3GPP, but [also] Chinese at the ITU (International Telecommunication Union) and the International Electro-Technical Mechanical Commission, [and an increasing] number vice chairs across standards sides there [sic].

In reaction to the Trump response, I would I would say primarily you’ve seen three things happen in China. The first is doubling down on indigenous innovation. So, after the list was published and sanctions put on ZTE, President Xi Jinping went around and gave a series of speeches to Chinese scientists and engineers and others about the need to hold core technologies in China’s hands and doubled down on indigenous innovation, particularly in chips. So that is the one area where China imports more in value in chips than it does in oil, and it is a real vulnerability for them. And so, we saw Chinese companies — Huawei, Alibaba, Tencent and others — also announcing their own chip initiatives and adjusting tens of millions, hundreds of millions of dollars into the chip initiatives. And the government [has] set aside another $50 billion for semiconductor investments.

So, [China is] doubling down on indigenous innovation [and] diversifying the sources of technology. As money no longer flows to the U.S. and they’re worried about SIFIs and other controls, [and they’re] looking at other places in Europe, Israel, and [elsewhere], although the U.S. is now trying to convince the E.U. and Israel to institute investment regimes. But, [China is still] able to tap into some technologies there. And then finally, [they continue their] reliance on espionage and cyber-enabled espionage, [which helps] make sure they can have access to technologies that they were cut off from.

So, let me end with some very speculative thoughts about how we [might] think about who might win or, as I said, who loses less in this competition. And I think there are a kind of four things, four variables that maybe that we can we can think about. The first one is — and this comes out of a theory from Mark Taylor from Georgia Tech — that, “States that face security competition can use that to mobilize domestic politics, [in order] to push forward innovative policies.” [The idea behind this is] that [if] you can get domestic coalitions in place that you couldn’t get in place [before, those coalitions will start to] break barriers, and [then you can] spend on R&D and other things you couldn’t before.

Here, I think the evidence [for this theory] is pretty mixed. So, on the U.S. side, I think you’re seeing part of that [or] some of that. We’re having a debate about industrial policy in the United States, which we have not had in a long time. When you have people like Senator Rubio out of his Senate committee [writing] a report that basically says that the nature of the challenge for China forces us to start thinking about industrial policy, I think [that signifies that] we’re in a different place [in terms of thinking about this than we were before].

[We’re] beginning to see the shift, I think, in domestic policy coalitions. The speech that Attorney General Bill Barr gave is another example where he started talking about [the] U.S. buying shares or stakes [and]
controlling stakes in Nokia and Ericsson, the only alternatives to Huawei in 5G out there. So, I think we’re seeing that on the domestic side, but it’s pretty splintered because our domestic politics are still truly splintered. The White House budget is a great example of that. They have put forward increased spending on AI, quantum, and Defense Department, but [have] cut spending on all other forms of R&D.

And so, if you were truly mobilizing on this competition, you would expect to see much broader support for a much broader range of technologies, as opposed to the Trump administration’s fairly narrow focus on a set of technologies that they see as important for national security. So, on the domestic side, I think China is much more able to mobilize the resources it needs to continue this competition. Chinese policy tools, I think are more applicable and suitable for this competition.

The meta problem for the United States, of course, is “How does the U.S. ensure that it stops the flow of technology without damaging itself?”, which is, I think, the way that the debate has been framed. Of course, you want to make sure that critical technologies are not stolen, [and] that people do not engage in espionage, but you have to do it in a way that ensures the openness of U.S. innovations.

That balance, I think, is very hard for the United States to get right. Historically, we tend to swing one way or the other. And even though the intelligence agencies and law enforcement gets that rhetoric, if you read the counterintelligence report, if you read the report for the FBI, they all talk about the need to keep the openness of American universities in place and protected, but then the rest of it, of course, is all focused on competing with China. So, I think that that balance is harder for us to do, so I would weigh [that] on the domestic side, China is probably slightly ahead of the U.S.

The second, variable that I think plays a role in this competition, of course, is international partners in international collaboration. As I said, science and technology has been rapidly globalized. There are centers of excellence in all of these things. And part of why again, why the US has been such a dominant system is not because it is the only science and technology power out there, but because it is the most important node in a network of science and technology collaborations. And so, how the U.S. continues to strengthen those [collaborations], I think, is a real strength of the U.S. Of course, this administration is not particularly interested in alliance relationships or science diplomacy. But, I think it is still probably one of the U.S.’s great strengths.

I think the longer-term issue of the United States is how Europe positions itself in this space. Increasingly, it is defining itself in opposition both to the United States and China. So, when the Chinese talk about technological sovereignty these days, they talk about it as sovereignty from Chinese hardware and to get Chinese hardware and U.S. software to the U.S. platforms. So how do you get those relations? I think it’s important, but on the total, I would give that to the United States. International partnerships [are] still a greater strength [for us].

The third variable is the nature of the technology itself. So, we’re talking tech very, very broadly. But you probably can’t really have any sense of the competition unless we break it down by sectors and how those technologies are structured and how innovation tends to happen in those technologies. Does the innovation tend to be incremental? Does it require having a group of scientists working on the problem to stay together for decades, something like that happened in batteries? Or is it going to be more fluid, more collaborative, something that’s been happening with more breakthroughs?

Here, I think, it’s probably across the board. AI seems to be the type of technology that is extremely open [and] extremely collaborative. We’re seeing a huge amount of talent flow and technology flow [around it], and the ability to attract people seems to be a defining nature of it. The chip side of it — the computational side — is different; those technologies are fairly limited. Quantum, at least on the computing side, also seems to be driven by the ability to spend lots and lots of money and keep teams together. So that, I think, really depends on the technology, and I think we’ll go across those sectors.
The last point that I'll end with, and [what] I think is the fourth variable in how you think about the competition, is the relationship between the tech community and the government. So, [these are the relationships between] Silicon Valley, D.C., or however else you want to thumbnail it or shorthand it. And the interesting thing, I think, about this competition is that although we tend to frame it as a top-down versus bottom-up system, or state-led versus private-sector, both systems are increasingly dependent on their big technology players, both to drive innovation in the private sector — not only just commercially, but also basic R&D — but also to be at the cutting edge of technologies that feed back into the national defense side.

We see that on the Defense Department being more and more worried about how you reach those technologies, experimenting with things like the DIU (the Defense Innovation Unit), and talking about reforms [and how] you can get the technology faster, [or] looking at talent flows [and] how you get more people into the Department of Defense (DoD) who understand technology. And of course, on the Chinese side, we see military-civil fusion, notably the attempt to bring the private sector closer to the Chinese defense industry base.

On this side, the U.S. government has increasingly tended to frame Chinese tech is being completely hostage to the party. And [on this], [I'm] someone who first saw the tech companies as being completely separate or very separate from state-owned enterprises. They grew up in sectors that didn’t exist, and so they managed to only attract the attention of state planners when they got bigger.

[Now], we certainly have seen Xi Jinping tightening control through party presence in the companies through this discussion about buying shares in the companies [and through] national intelligence laws and other regulatory things there. But I would suspect that there are still inherent tensions between what the companies want to do when they think about markets and global markets in particular, and what the party wants to do. Now, it’s very hard to find those gaps these days given the debate inside China, but I would be very surprised if the party did manage to align all of those interests.

On the U.S. side, our divisions are out in the open. Those are both political, with many of the technology workforces not wanting to work with the government because of [issues like] working on surveillance on the border or helping ICE and others. But, there’s also a different view of China and how you compete with China. And here I don't really see either side being able to narrow that gap. So, I would marginally put [down] that China has the strength right now [and] that the US is still struggling. But I think longer term, once we get that [those internal divisions settled and] in place, that it’s still going remain a U.S. competitive strength.

So, for those of you keeping score at home, that comes out to about 2-2. So, in a perfect kind of think tank world I get to say, “On the one hand, on the other hand.” But I think technology, which had usually been a fifth, sixth, seventh on the agenda in the U.S.-China relationship is going to continue to be one of the defining issues that structures the relationship, and increasingly is one not just about concerns about national security, but about values and how we think about how technology is applied, and governance issues.