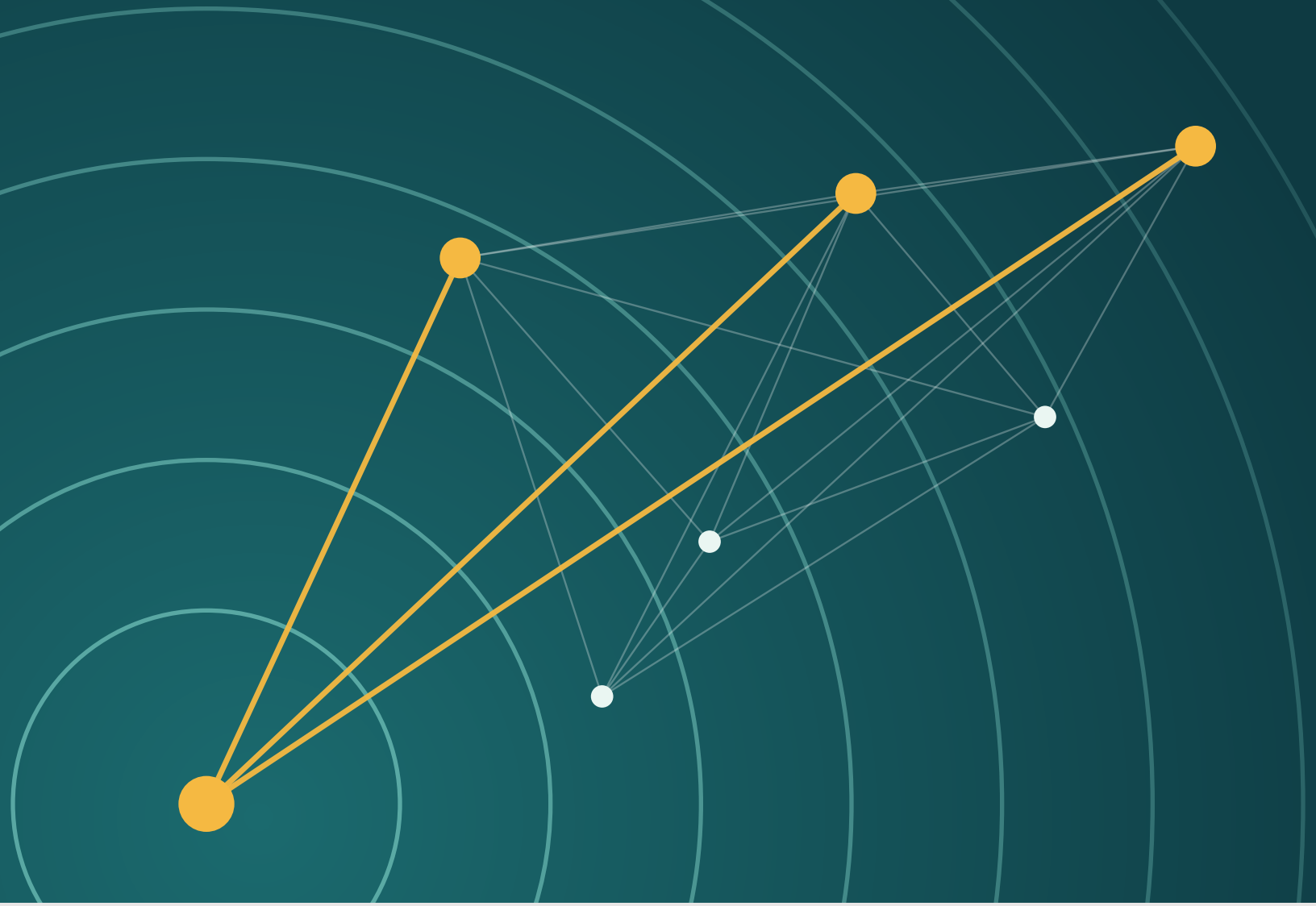

Practical Ways of Countering Chinese and Russian Influence in a Multipolar World

Joey Hood, Ambassador (ret)

THE FLETCHER SECURITY REVIEW

Recently, a senior executive of a global telecommunications company warned me that China had largely caught up to the West in terms of quality and reliability of its software and hardware, and its state-subsidized financing allowed Chinese companies to greatly undercut others on price. Everyone in the industry, he said, was tired of hearing from Westerners what a threat the Chinese government posed to data and infrastructure security through their companies. After all, it is widely believed that Western telecom companies collaborate with their governments, as well, he asserted. The executive laid out his challenge: what did the West have to offer the world on telecoms that China could not do at least as well and far cheaper, notwithstanding these security concerns?

I knew this particular executive was due for a transfer soon, but he did not yet know where, so I sensed an opportunity to make a rhetorical point. I asked him to embark on a thought experiment with me and imagine that he had two opportunities in front of him: he could either spend the next ten years as CEO of his company's operations in the city of his choice in China or in the United States, and the only stipulation was that whatever destination he chose, he must bring his family.

He responded without hesitation, "Of course I would choose the United States." So, I parried, if you would choose the Western solution for your own family, why would you choose the Chinese solution for the personal data and the most intimate communications of millions of other citizens? He nodded in assent to my logic but made a grave prediction: "What you have just said is right, but if nothing else changes, the United States has only about another ten years, and the choice you described will no longer be decided in America's favor. China is catching up fast with your soft power. Do not sleep."

The fact is that American diplomats have not been sleeping when it comes to countering strategic adversaries like China and Russia but have repeatedly looked in their toolbox and largely found only rhetorical arguments with limited utility, or economic sanctions, the metaphorical hammer of diplomacy. In practical terms, diplomats could wag their fingers, and if that did not work, threaten punitive measures. Neither approach has been successful over the long run, and like this regional tech CEO pointed out, the soft power "pull" of America's and Europe's competitive universities, business environments, and entertainment options will only last for so long. American

diplomats and their European partners need to build upon practical field solutions.

* First, they should take advantage of their commanding positions in multilateral development banks to offer attractive financing early in the project cycle.

* Second, they should share information aggressively - including by bringing in nontraditional partners - that demonstrates in vivid terms how a nation's sovereignty is put at risk by Chinese or Russian entities.

* Third, just like China, they should compete everywhere, not only in the biggest markets.

STRATEGIC FINANCING

For instance, take China's expansion into 5G telecommunications around the world. Constraining this expansion has been a U.S. strategic goal for more than a decade. In the National Defense Authorization Act (NDAA) for 2019, Congress barred the federal government from purchasing equipment from the major Chinese telecommunications companies.[i] The Executive branch also adopted a number of restrictions, including the sale of chips and software to Chinese companies, and a ban on equipment purchases by any American entity, private or public.[ii] Legislators and policymakers have routinely cited Chinese laws requiring private companies to share data with intelligence agencies as a major threat to states' sovereignty, and potentially even our collective security.[iii]

U.S. Marine Corps Lt. Col. Benjamin Pimentel and defense technology industry professionals attend a 5G network systems demonstration at Marine Corps Base Camp Pendleton, California, Dec. 5, 2024. | U.S. Marine Corps photo by Lance Cpl. Samantha Devine (public domain)

To implement these policies, U.S. diplomacy has largely focused on trying to persuade foreign partners to adopt our domestic measures as their own, but this strategy has produced few results beyond our traditional western democratic partners. My conversations on this topic with diplomats and business leaders across the Middle East and North Africa have typically followed the same rhythm. Relying on our talking points from Washington, my colleagues and I would explain the potential risks of relying on Chinese equipment and software and urge our interlocutors to formulate domestic regulations to protect their telecommunications infrastructure from "untrusted actors."

The responses routinely fell along these lines: 1) We understand the risks and do not wish to be lectured. 2) Do you expect us to believe that Western governments do not cooperate with their companies to engage in the same behavior as China? 3) What American alternative do you propose?

"China is catching up fast with your soft power. Do not sleep."

On these points, the American diplomat is caught flat-footed. In one case, a foreign official responded to our points about the security risks by stating, "We are fully aware of the technology's back doors, and they are a benefit to us, not a risk." (In other words, potential surveillance options were not a net negative for this official.) In another case, our interlocutors claimed that they would try to take cybersecurity precautions, but ultimately the cost savings offered by Chinese firms were just too great to ignore for a country with a struggling economy. Because the American private sector has — to date — not offered an alternative to firms like Huawei and ZTE, American diplomats have been empowered to advocate for "trusted actors" like European firms Nokia and Ericsson through initiatives like the "Clean Network."[iv]

Pitching non-American solutions can work, but it is not an ideal solution. At times, the approach comes off as more anti-China than pro-America, according to my foreign diplomatic colleagues.

Looking to Washington for senior-level engagement has generally not been fruitful, as those officials tend to focus on the world's biggest, most advanced economies. Beijing, however, is competing everywhere, and so must the United States.

Certainly, establishing partnerships with these powerful allies and the domestic companies that they regulate was a master stroke. Under the first Trump Administration, Under Secretary for Economic and Business Affairs Keith Krach could rightly take credit for initiatives like the "Clean Network" and the "Blue Dot Network" to promote shared standards for trusted technology.[v] At the same time, I recall collaborating with U.S. colleagues for almost two years to arrange a single visit by a senior official to engage with Arab governments about these and other secure technology initiatives and concerns. Time lags such as this do not suggest urgency to our interlocutors.

Threats certainly have not worked, either. After enactment of the NDAA for fiscal year 2019, American diplomats dutifully relayed points to our foreign counterparts about the risks of "untrusted actors." In one case,

we made no headway, so we moved to hard power points, regretting that we may need to end certain aspects of our military cooperation in order to prevent our networks from being compromised by untrusted technology. This bilateral partner begrudgingly complied with our wishes, but contacts close to this country's leaders tell me the experience left a bitter after-taste, and one they have not forgotten, even years later. Over time, the application of hard power like this only causes our partners to seek to diversify their partnerships so that they are not so vulnerable to being forced into a decision by any particular foreign government, even one with a close and historic relationship like the United States. Although it is often overlooked in favor of more well-known aphorisms, Chinese strategist Sun Tzu in fact put moral influence at the top of his list of principles.[vi] Without it, our allies and partners will go along with us only when forced to do so.

My experience in another country offered a potential alternative to the finger-wagging-and-threat approach described above. Over lunch one day with a senior official from a multilateral development bank, we discussed our shared concerns about growing Chinese government influence in advanced telecommunications, and lamented the paucity of Western tools or alternatives, other than to refer foreign governments to Nokia and Ericsson, companies that sometimes did not have much interest in the smaller markets. Then a light bulb went off. I said, "You're a bank; why can't you offer attractive financing and write into the terms of the loan that it can only be used to purchase from trusted vendors, or at least from European firms?" The executive reminded me that the U.S. government was the largest single shareholder in that particular bank, so it could propose such a solution if it wanted to. Then my work turned toward convincing my Washington colleagues. For good measure, I also enlisted the support of a European ally with a great stake in this particular country's cybersecurity, given its geographic proximity and its importance in controlling the flow of irregular migrants. Together, we brought in the European Union to bolster our eventual proposal within the multilateral development bank.

Approaching the issue from these several angles produced a result that Washington probably would not have pursued all on its own, at least not in time to be of any relevance. The bank approved the proposal, and it was swiftly put before relevant government officials, who just as quickly accepted it. Asked later why this deal had come together so smoothly when years of previous attempts had not proven fruitful, one interlocutor told me, "When you can match or do better than the Chinese offer, it is natural that you would require us to use your technology. That is not a constraint on our sovereignty; it is an agreement between partners." In this case, incentives were effective where hand-wringing and threats were not.

What made this approach effective was not ingenuity alone, but timing and structure. By intervening before procurement and vendor selection, and by aligning incentives, contracting conditions, and financing terms, we changed the competitive field without coercion. This is the broader lesson: projects that are conditioned upstream are easier to defend politically, finance efficiently, and execute successfully downstream. Financing

accelerates outcomes only after contracting and risk allocation are sound; it cannot substitute for early project shaping.

INFORMATION SHARING ON SOVEREIGNTY VIOLATIONS

Constraining problematic Russian activities is another area in which sovereignty-based arguments can be more helpful in the field than hard power threats. When we began to suspect that Russia and its proxies like the Wagner Group were using a foreign partner's territory to facilitate the movement of goods, people, and funding to support their disruptive activities elsewhere, we deployed the usual talking points: this is what we think they are doing, this is bad, and you should take measures to stop it. When that did not happen because our partners cited a lack of evidence, we brandished sanctions. Our partners took that threat seriously enough to board a vessel but reported finding no contraband. We explained that there was no contraband, as it was the proceeds from the cargo — not the cargo itself — that were supporting the Russians' destabilizing activities. Finally, we moved to levying sanctions…and still nothing happened.

Boarding team members from the Coast Guard Cutter Bertholf and Pacific Tactical Law Enforcement Team board a vessel during a counter-narcotic patrol in the Eastern Pacific Ocean, March 3, 2018. | U.S. Coast Guard photo by Petty Officer 1st Class Matthew S. Masaschi (public domain)

I surmised that we needed a different approach. So as with the case of Chinese involvement in telecommunications, I consulted colleagues inside the vast U.S. government apparatus, as well as our close allies, including nontraditional ones who might share our concerns about destabilizing activities in the region. Soon, we had a folder of open-source information to share, all of which pointed to breaches of

this partner's sovereignty. The approach I adopted was this: "If these activities are all known to you, then explain your change in policy, because up to this point, you have told us that you do not support mercenary activities anywhere. If these activities were not known to you, I leave it to you to take steps to address these insults to your sovereignty." In this case, our interlocutors thanked us for the information and then - without causing a bilateral crisis with Moscow - tightened up controls at points of entry.

CONCLUSION

These experiences from the field suggest that information sharing, incentives, and appeals to protecting sovereignty, especially when done in consultation with allies who can act as "force multipliers" can be more effective than moralizing, threatening, or punishing foreign governments into submission. In my experience, those approaches often have not worked, and when they have worked, they probably weakened our bilateral relationship over the long run. Our partners want us to be strong; they do not want us to be bullies. And as my friend the telecom executive warned, America's soft power may not be a competitive advantage over China forever; we need to compete by drawing on our partnerships in the field to bring superior financing and information at key moments.

ABOUT THE AUTHOR

Ambassador (ret) Joey R. Hood was a U.S. diplomat for 25 years, serving at eight embassies and consulates across the Middle East and North Africa. In Washington, he was Acting Assistant Secretary of State for Near East Affairs during the Biden Administration and Principal Deputy Assistant Secretary in the first Trump Administration. He also directed the Office of Iranian Affairs.

NOTES

i Congress.gov. "H.R.3919 - 117th Congress (2021-2022): Secure Equipment Act of 2021." November 11, 2021. https://www.congress.gov/bill/117th-congress/house-bill/3919.

ii Congress.gov. "H.R.3919 - 117th Congress (2021-2022): Secure Equipment Act of 2021."

iii Pompeo, Michael R. “The United States Further Restricts Huawei Access to U.S. Technology.” U.S. Department of State, U.S. Department of State, August 17, 2020. https://2017-2021.state.gov/the-united-states-further-restricts-huawei-access-to-u-s-technology/.

iv Office of the Spokesperson. “The Transatlantic Alliance Goes Clean.” U.S. Department of State, U.S. Department of State, October 17, 2020. https://2017-2021.state.gov/the-transatlantic-alliance-goes-clean/.

v U.S. Department of State. “Blue Dot Network.” U.S. Department of State. Accessed April 27, 2026. https://2021-2025.state.gov/blue-dot-network/.

vi Aiguanli. “The Five Fundamentals of Strategy: Sun Tzu’s Timeless Framework for Competitive Advantage.” Ancient War History, April 23, 2025. https://ancientwarhistory.com/the-five-fundamentals-of-strategy-sun-tzus-timeless-framework-for-competitive-advantage/.