US-India Technology Sharing

Rajeswari Rajagopalan and Trisha Ray

As great power competition intensifies in the Indo-Pacific, technology has become one of its key components. It goes without saying that the primary tech challenges facing India and the United States in the Indo-Pacific come from China. Several decades of intense economic linkages have led to significant technology transfers that have also partly contributed to China's growing technological prowess and thus intensified the competition between China and the United States. China's growing technological might is being leveraged to undermine and threaten not just the United States or the West but also China's neighbors in the Indo-Pacific. In response, the US and its partners in the Quad have identified technology as an important area for cooperation. Though they do not specifically identify China, the kinds of initiatives that the Quad countries individually and collectively are undertaking are designed to counter China's leveraging of technology over others. Nevertheless, there is still significant room for further cooperation between the US and India, in particular to deal with the emerging technological challenges that China poses. In this essay, we outline both the challenges and the opportunities for enhanced cooperation between the United States and India in this area.

THE CHALLENGE

China's growth over the last four decades has been impressive, but as its wealth has grown, China has sought to challenge the United States and the liberal international order as well as its domination in the Indo-Pacific. The integration of China into the global economy and its rise as a manufacturing power has also given China access to advanced technologies that it is now employing in its pursuit of regional hegemony and global parity with the United States. The technology challenge from China has evolved in the last two years. The initial challenge came from state-supported entities like Huawei that sought to corner the 5G telecom market. State support allowed Huawei to sell its 5G technology at highly competitive rates, giving it a significant advantage and making it an attractive partner for many countries, especially in the developing world. The threat

this posed to telecommunication security led to actions by many countries, including India and the US, to limit Huawei's entry into their telecommunication systems.

With support from the Chinese state, Huawei has been able to develop 5G technology and sell it far more cheaply than its competitors. But Huawei's connection to the Chinese state also makes any telecommunication network that uses Huawei technology potentially vulnerable to China. Another aspect to using Chinese apps and telecom service providers is that it allows China to control access to information as well as engage in disinformation campaigns. India and the US cooperated in highlighting the threat from Huawei to other countries, thus significantly limiting Huawei's spread. This was an early success, though not a complete one. In the last few years, the threat has expanded when compared to other areas, from platforms and software to critical minerals and semiconductors. The rise of Chinese apps like TikTok, for instance, is particularly pernicious because they lead to transfer of significant personal data from ordinary citizens to servers in China. Moreover, TikTok has become a source of news and information controlled by China's state authorities, thus posing a danger to open societies everywhere.

Possibly the most pertinent rising threat today comes from China's dominance in semiconductor production. Currently, although China has advanced in many areas through careful planning and concerted action, it still has not managed to control all parts of the semiconductor supply chain; the US and its partners, such as Taiwan, Japan, South Korea, and the Netherlands, still control the highest reaches of technology in semiconductor manufacturing. However, China is pushing determinedly in this direction, because of the importance of semiconductors not only to civilian applications but even more critically in military systems. If the current trends continue, China could hold the largest share of semiconductor manufacturing by the end of this decade. But it also needs to be noted that China is still not capable of manufacturing cutting-edge computer chips and continues to rely on external supply. Any Chinese success in capturing the semiconductor manufacturing industry would pose major challenges, putting at risk the military and technological power of other countries. China has some capacities in this regard, but it cannot be expected to produce high-end chips that use very advanced semiconductor nodes. For example, the US produces 4 nanometer (nm) chips while China is making 12 nm chips.[1]

Finally, it is critical to acknowledge that technology trends and threats cannot be viewed in isolation, especially in the complex security and geopolitical environment of the Indo-Pacific. In this region, for instance, cyber-enabled threats have compounded "traditional" security threats, such as terrorism, contested borders, and maritime disputes. In conjunction with these regional tensions, nonstate actors, including those sponsored by states, operate below the threshold of outright conflict—targeting institutions, sowing distrust in institutions, and inflicting economic and social damage. Between 2020 and 2021, the Indo-Pacific region witnessed a 168 percent increase in cyberattacks, with health systems and the financial sector being the worst hit.[2] Heightened tensions with China have contributed to hybrid threats. In 2020–21, against the backdrop of Sino-Indian border skirmishes in Galwan, Chinese advanced persistent threat (APT)

actors attacked India's transportation sector, as well as the electricity grid of the state of Maharashtra.[3] Chinese APT actors have similarly conducted multiyear espionage operations in relation to the South China Sea dispute, targeting governments in Southeast Asia, as well as Australian defense contractors, manufacturers, universities, government agencies, legal firms, and other foreign companies.[4] Other aspects of hybrid operations too have moved online, leveraging targeted advertising on social media. Furthermore, organized groups can spread disinformation and misleading narratives and can target individuals and communities using tactics such as mass-reporting, trolling, and other forms of online harassment. We still have a very limited picture of the true growth and scale of these types of operations, especially outside the Anglosphere, given that platforms (and funders) have only begun to recognize this phenomenon relatively recently.[5]

AVENUES FOR COOPERATION

Though India and the United States have taken steps to counter these challenges, most of their efforts have been unilateral. For example, India was one of the earlier countries to ban various Chinese apps, including TikTok, in the immediate aftermath of the Galwan River clash in 2020. Though this may have been done partly to assuage domestic public opinion in India following Chinese aggression in Ladakh, it also had important security benefits that are only now being realized. Over the last couple of years, many countries have recognized the threats posed by seemingly innocent Chinese apps, making the Indian action quite prescient. Many of these apps allow access to the devices where they are installed, potentially making the devices accessible to Chinese state security agencies and compromising their information security. Similarly, India has acted decisively to stem Chinese control over India's 5G telecommunication network. Though Indian concerns about Huawei predate the Galwan crisis, it also helped provide the impetus for banning Huawei from India's 5G service network. India also went ahead with additional measures to control Chinese involvement in various aspects of India's infrastructure including in telecommunications. These were effective measures, but they were measures that India took unilaterally.

Similarly, the US has undertaken some unilateral actions, though it has not gone as far as India. For example, despite growing security concerns, the US still has not banned Chinese apps like TikTok, but it has taken multiple actions to restrict China's access to technology. This includes the CHIPS and Science Act as well as the new round of technology controls to prevent the flow of high technology semiconductors and semiconductor manufacturing equipment to China.

The absence of US-India joint actions leaves considerable scope for bilateral cooperation in this space. The first and the most basic measure would be to engage in more intense discussions about cooperating in areas where India and the US have taken individual actions. Unilateral actions are less effective than joint actions by multiple countries. Especially considering that both India and the US broadly agree on the threat they face, initiating dialogue about how to respond to these threats is critical. For example,

the US could join India in banning Chinese apps, and it could prevent China from dominating the semiconductor industry by involving India in such policies as "friendshoring." Friendshoring could include helping India design and manufacture various systems and technologies that are currently procured from China. In fact, US Commerce Secretary Gina Raimondo, after meeting with Indian Commerce Minister Piyush Goyal, suggested that "India has an opportunity to become a key supplier in the entire electronics supply chain and not just semi-conductors."[6] She clarified, however, that the US is "not looking for technology decoupling from China," which is a difficult goal to achieve, at least in the short term. But given India's technological challenges in these areas, this would require the US to provide the technology that is required for manufacturing in India.

Another serious threat is China's use of cyberwarfare. India and the US have been the most affected in terms of the number of cyberattacks worldwide. While not all attacks emanated from China, a large number of them did. The United States' "defend forward" cyber strategy aims to "intercept and halt cyber threats" at their source, including working with the private sector, allies, and partners.[7] India's cyber posture is primarily defensive, although it apparently possesses "modest" offensive cyber capabilities, primarily directed against Pakistan, but with a growing focus on China.[8] There are a handful of Indian APT actors operating at varying levels of sophistication, employing measures from phishing to leveraging zero-day exploits. There is a need to develop a shared understanding in containing malevolent actors like China that carry out cyberattacks on critical infrastructure. This cooperation can extend to retaliatory action as a means of deterrence at a later stage. A shared understanding can begin with consultations and intelligence sharing about China's cyber activities, joint investigation of attacks, and sharing of measures to protect cyber and other critical infrastructure. This should also include a common understanding about what might be considered serious attacks that require retaliation and whether such retaliation should take place jointly or by the affected parties. Such retaliation could include publicizing details of Chinese cyberattacks and a common and public commitment to respond if such attacks take place. A cyber deterrence strategy should include not just retaliation to Chinese cyberattacks, but also publicized cooperative action against any kind of cyberattacks, including private nonstate actors from any part of the world. This would signal to China both Indian and American capacity to retaliate, as well as their commitment to cooperate in detecting and responding to cyber dangers.

NOTES

1. China claims that it is making 7 nm and more advanced 5 nm chips despite being denied certain critical technologies such as extreme ultraviolet (EUV) equipment. Scott Foster, "China on Course to Elude US Chip-Making Equipment Bans," *Asia Times*, October 3, 2022, https://asiatimes.com/2022/10/china-on-course-to-elude-us-chip-making-equipment-bans.

2. "Check Point Research: Asia Pacific Experiencing a 168% Year on Year Increase in Cyberattacks in May 2021," Check Point, May 27, 2021, https://blog.checkpoint.com/2021/05/27/check-point-research-asia-pacific-experiencing-a-168-year-on-year-increase-in-cyberattacks-in-may-2021; "X-Force Threat Intelligence Index 2021," IBM Security, February 2021,

https://www.ibm.com/downloads/cas/AWJ3PE1M?mhsrc=ibmsearch_a&mhq=X-Force%20Threat%20Intelligence%20Index%202021; "X-Force Threat Intelligence Index 2022," IBM Security, February 2022, https://www.ibm.com/downloads/cas/ADLMYLAZ.

3. Insikt Group, "China-Linked Group RedEcho Targets the Indian Power Sector amid Heightened Border Tensions," Recorded Future, February 28, 2021, https://www.recordedfuture.com/redecho-targeting-indian-power-sector; Press Trust of India, "Highways Ministry Asks NHAI, Automakers to Tighten IT Security after Cyber Attack Threats," *Tribune India*, March 21, 2021, https://www.tribuneindia.com/news/nation/highways-ministry-asks-nhai-automakers-to-tighten-it-security-after-cyber-attack-threats-228534.

4. "SharpPanda: Chinese APT Group Targets Southeast Asian Government with Previously Unknown Backdoor," Check Point Research, June 3, 2021, https://research.checkpoint.com/2021/chinese-apt-group-targets-southeast-asian-government-with-previously-unknown-backdoor; Michael Raggi and Sveva Scenarelli, "Rising Tide: Chasing the Currents of Espionage in the South China Sea," Proofpoint, August 30, 2022, https://www.proofpoint.com/us/blog/threat-insight/chasing-currents-espionage-south-china-sea.

5. Emma Briant, "The Grim Consequences of a Misleading Study on Disinformation," *Wired*, February 18, 2021, https://www.wired.com/story/opinion-the-grim-consequences-of-a-misleading-study-on-disinformation.

6. Monika Yadav, "'India Can Be Key Electronics Supplier,'" *New Indian Express*, March 11, 2023, https://www.newindianexpress.com/business/2023/mar/11/india-can-be-key-electronics-supplier-2555041.html.

7. Department of Defense Cyber Strategy, September 2018, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

8. Julia Voo, Irfan Hemani, and Daniel Cassidy, "National Cyber Power Index 2022," Belfer Center, Harvard Kennedy School, September 2022, https://www.belfercenter.org/sites/default/files/files/publication/CyberProject_National%20Cyber%20Power%20Index%202022_v3_220922.pdf.

29 28 27 26 25 24 23 7 6 5 4 3 2 1

ABOUT THE AUTHORS

RAJESWARI RAJAGOPALAN

Dr. Rajeswari (Raji) Pillai Rajagopalan is the director of the Centre for Security, Strategy, and Technology at the Observer Research Foundation, New Delhi. She is also a senior fellow at the Australian Strategic Policy Institute in Canberra. In 2020, she was cochair for a thematic group on strategic technologies for developing India's Science, Technology, and Innovation Policy.

TRISHA RAY

Trisha Ray is a fellow and deputy director at the Centre for Security, Strategy, and Technology at the Observer Research Foundation, a member of UNESCO's Information Accessibility Working Group, a Pacific Forum Young Leader, and a 2022 Schmidt Futures ISF Asia Fellow. Ray completed her MA in security studies from the Walsh School of Foreign Service at Georgetown University.

Strategic Cooperation in the Indo-Pacific *Essay Series*

The Hoover Institution's Huntington Program on Strengthening US-India Relations has partnered with the Observer Research Foundation for this essay series to address issues central to the burgeoning partnership between the United States and India. With contributions by authors holding deep expertise in government, the military, and academia, the series focuses on shared interests in the Indo-Pacific region in areas including governance, trade, security, technology, and energy. This collaborative effort lays the foundation for timely, policy-relevant research to inform public debate and identify joint challenges and opportunities in helping the United States and India advance their strategic partnership and future cooperation.

Huntington Program on Strengthening US-India Relations

The Huntington Program on Strengthening US-India Relations, made possible through the generous support of Claudia P. Huntington, John A. Gunn and Cynthia F. Gunn, Walmart Inc., and The Harold W. McGraw, III Foundation, Inc., focuses on the important relationship between the United States and India, which will advance freedom, security, and prosperity in the twenty-first century. The program's goal is to generate, identify, and further policy-relevant scholarship and connections that will deepen connections between the world's oldest and the world's largest democracies.

For more information about this Hoover Institution research initiative, please visit us online at hoover.org/research-teams /strengthening-us-india-relations-hoover-institution-project.

For more briefs and reports from the Observer Research Foundation, go online to orfonline.org/content-type/issue-brief.

Hoover Institution, Stanford University
434 Galvez Mall
Stanford, CA 94305-6003
650-723-1754

Hoover Institution in Washington
1399 New York Avenue NW, Suite 500
Washington, DC 20005
202-760-3200

HOOVER INSTITUTION