

Digital Entanglement Lessons Learned from China's Growing Digital Footprint in South Korea

Author(s): Kristine Lee, Martijn Rasser, Joshua Fitt and Coby Goldberg

Center for a New American Security (2020)

Stable URL: <https://www.jstor.org/stable/resrep27454>

Accessed: 30-11-2024 15:23 UTC

JSTOR is a not-for-profit service that helps scholars, researchers, and students discover, use, and build upon a wide range of content in a trusted digital archive. We use information technology and tools to increase productivity and facilitate new forms of scholarship. For more information about JSTOR, please contact support@jstor.org.

Your use of the JSTOR archive indicates your acceptance of the Terms & Conditions of Use, available at <https://about.jstor.org/terms>



JSTOR

Center for a New American Security is collaborating with JSTOR to digitize, preserve and extend access to this content.



OCTOBER 28, 2020

Digital Entanglement

Lessons Learned from China’s Growing Digital Footprint in South Korea

By [Kristine Lee](#), [Martijn Rasser](#), [Joshua Fitt](#) and [Coby Goldberg](#)

[Executive Summary](#)

[Introduction: The Fragmentation of the Global Telecommunications Landscape](#)

[Examining the Trajectory of South Korea’s Digital Entanglement with China](#)

[The Risks of Digital Entanglement](#)

[Policy Recommendations for the U.S. Government](#)

[Conclusion](#)

Executive Summary

Communication networks are the lifeblood of modern-day societies. They form the conduit for the information flows fueling the world’s economies. These networks also enable and transmit the media that inform and shape beliefs, perceptions, and, ultimately, what is considered truth. In the hands of liberal democracies, controlling this infrastructure means preserving free and open societies and safeguarding democratic norms and values. For authoritarians, it is a pathway to solidify their rule through oppression and marginalization, to expand influence abroad, and to subvert the rules-based order. China’s push to dominate digital infrastructure leaves liberal democratic countries at a critical juncture.

The fallout of the COVID-19 pandemic has accelerated the splintering of the global telecommunications landscape. Leaders in Beijing are redoubling efforts to export Chinese fifth-generation wireless (5G) infrastructure, with notable success in Latin America, Africa, and central and eastern Europe. The U.S. government is now the leading voice in trying to blunt that expansion, after allies such as Australia and Japan took decisive action to exclude Huawei, the Chinese technology company that is the predominant manufacturer of 5G radio access network (RAN) equipment, from their networks.

Washington policymakers made considerable progress on that front across western Europe and in India during 2020 as views on China hardened and U.S. export controls on Huawei sowed doubts over the company’s longer-term ability to deliver quality products and services. Now the focus is on the Asia-Pacific, with Beijing’s leaders making overtures to Seoul and leveraging China’s economic heft over numerous countries in Southeast Asia. Regional digital entanglement with China has profound consequences for the United States. It bears the risk of chipping away at alliances and partnerships; impairing U.S. ability to project force; encroaching on America’s economic sway; and eroding democratic values, norms, and institutions by proliferating illiberal uses of technology.

The South Korean experience is an illustrative case study of digital entanglement with China. This paper focuses on South Korea’s 5G networks for the purposes of scoping, but the spotlight on telecommunications networks offers just one window into a broader trend of technology and economic interdependencies between Seoul and Beijing. In particular, the paper’s focus on 5G illuminates four central observations that could also apply to other technology areas: (1) the U.S.-China strategic competition has wedged South Korea between its most important ally and its largest trading partner; (2) geopolitical risk assessments are not top of mind in South Korea’s technology policymaking calculations; (3) the country’s political leadership largely defers to private industry on the use of Chinese equipment; and (4) South Korean privacy regulations remain relatively fluid and are evolving both to meet domestic pressures and to generate new market opportunities. These trends are evident in the history of South Korea’s economic entanglement with China and the risk of coercion carried with it. Ongoing entanglement with digital infrastructure—and 5G networks in particular—increases the potential for and reach of adverse economic statecraft by Beijing and will make it more difficult and costly to unravel.

South Korea’s digital entanglement with China holds important lessons for the bilateral relationship with the United States, Seoul’s relations and standing in the Indo-Pacific, and the region’s resilience to China’s growing influence. This report advances a set of four guiding principles to frame eight actionable policy recommendations for South Korea and the United States to take together to bolster the bilateral relationship and, in

concert with others, for effective multilateral initiatives. The recommendations emphasize affirmative and proactive steps that South Korea, the United States, and their allies and partners can take to craft and promote secure and resilient digital infrastructure and to mitigate risky economic dependencies.

Principle 1: Advance an evidence-based framework for evaluating and communicating 5G network security risks.

Recommendation 1: Expand mechanisms for sharing intelligence with South Korea and other allies on 5G network and supply chain security issues.

Recommendation 2: Launch a public diplomacy initiative to better inform citizens in South Korea and other Indo-Pacific countries about 5G network security.

Principle 2: Set conditions to cultivate cost-competitive, readily available 5G equipment providers to compete with Huawei.

Recommendation 3: Mitigate the economic impact South Korea and other allies confront in rejecting Huawei by bolstering the presence of other 5G RAN market players.

Recommendation 4: Promote development of 5G infrastructure built on a modular architecture with open interfaces by investing in open RAN technology.

Principle 3: Invest in diplomatic and security arrangements that mitigate vulnerability to coercion.

Recommendation 5: Work with South Korean counterparts to strengthen and streamline geopolitical risk assessments into technology policymaking mechanisms.

Recommendation 6: Engage multilateral groupings to mitigate Chinese economic coercion throughout the Indo-Pacific.

Principle 4: Advance an affirmative technology cooperation agenda.

Recommendation 7: Pursue multilateral approaches to technology policy coordination and collaboration to:

- ❑ Strengthen regional cybersecurity postures;
- ❑ Include South Korea within an alliance innovation base;
- ❑ Retake the initiative on promoting norms around technology use;
- ❑ Close the Indo-Pacific digital divide; and
- ❑ Bolster technology capacity in the Indo-Pacific, including through continuing to promote deeper alignment between South Korea’s New Southern Policy and the United States’ Indo-Pacific Strategy.

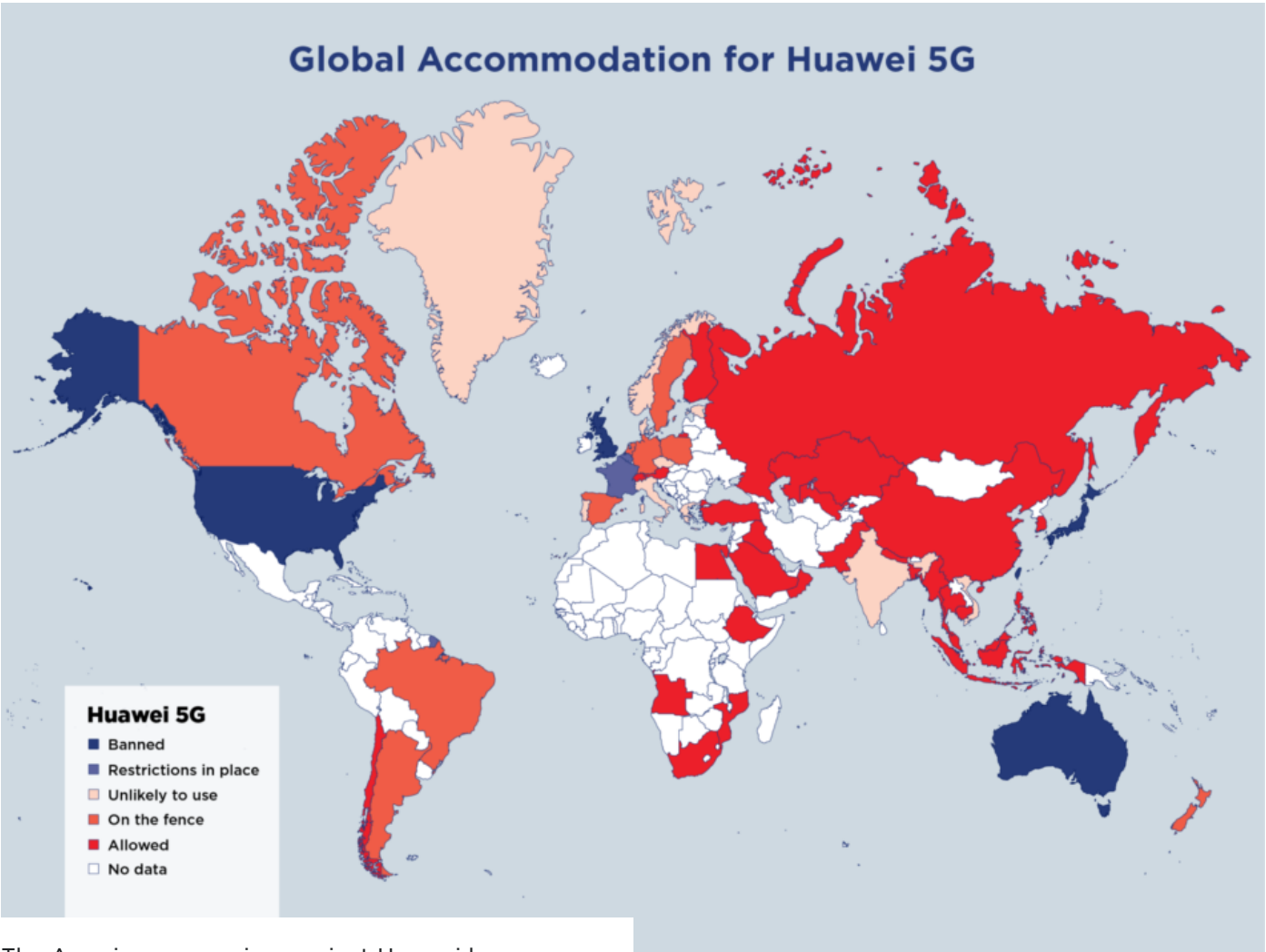
Recommendation 8: Create an alliance framework for technology policy.

Download the full report.

Introduction: The Fragmentation of the Global Telecommunications Landscape

The COVID-19 pandemic has emerged as a critical inflection point for U.S. allies and partners evaluating the inclusion of Chinese telecommunications equipment in their networks. Democracies around the world have bristled at Beijing’s lack of transparency in managing the global health crisis, with some countries such as the UK and India publicly signaling their intent to eliminate Huawei from their networks and other like-minded countries more quietly assessing alternative paths.

As the United States has sought to blunt China’s digital expansion and the attendant rise of illiberal norms around the use of technology, there has been a trifurcation of the global telecommunications landscape, with fault lines forming around countries’ willingness to use Chinese equipment. On one side stand U.S. allies such as Japan, Australia, and New Zealand and European countries, with a few notable outliers, that have decisively eschewed the use of Huawei in their networks. On another are countries that have embraced Huawei, particularly across Latin America, Africa, and Central Asia. The third and arguably most consequential bloc encompasses American allies caught in the middle—including South Korea and rapidly developing Association of Southeast Asian Nations (ASEAN) countries—that have military or intelligence-sharing agreements with the United States, but whose economies are deeply dependent on China or for whom cost considerations are determinatively important in rolling out their telecommunications networks.



The American campaign against Huawei has fragmented the global telecommunications landscape. Many allies and partners are still on the fence about allowing Huawei as a 5G equipment vendor. This map was created with information from a Bloomberg report, with supplemental data from Reuters and LightReading. (94)

Despite availability of competitive alternatives to Chinese 5G telecommunications equipment such as the equipment produced by Ericsson, Nokia, and Samsung, the pandemic has emerged as an opportunity for the Chinese Communist Party (CCP) to leverage critical emerging technologies to tout its superiority to Western models of governance and advance its narrative of total control. Dominating global 5G networks has been a long-standing pillar of the CCP’s technological ambitions—made all the more urgent as the party seeks offramps from the economic stumble caused by the pandemic.¹ At the opening of the 13th National People’s Congress (NPC) in May 2020, the annual convening of China’s top legislature and the country’s premier political event, Premier Li Keqiang emphasized the need to step up “develop[ing] next-generation information networks and expand 5G applications.”² The NPC proceeded to rubber-stamp a \$1.4 trillion six-year spending plan focused on infrastructure beginning in 2020, with 5G wireless networks as its backbone.³

Dominating global 5G networks has been a long-standing pillar of the CCP’s technological ambitions—made all the more urgent as the party seeks offramps from the economic stumble caused by the pandemic.

With this renewed political momentum, Beijing has again turned its focus outward, cultivating warming relations with hedging countries like South Korea to help achieve its aim of 5G dominance. Through a much-anticipated summit between Xi Jinping and South Korean President Moon Jae-in in the fall of 2020, Xi is likely to lobby for expanding Huawei’s presence in South Korea. In exchange, Beijing is poised to backstop Seoul on high-priority issues for the Moon administration. China’s ambassador to South Korea, for example, met with South Korea’s Unification Minister in August 2020 about resuming stalled talks with Pyongyang.⁴ China’s leverage over North Korea makes it more difficult for Seoul to reject Huawei outright. Indeed, South Korea’s ambassador to the United States, Lee Soo-hyuck, has noted that he was proud that his country had the freedom to choose between the two great powers, rather than being wedded to either one’s agenda.⁵

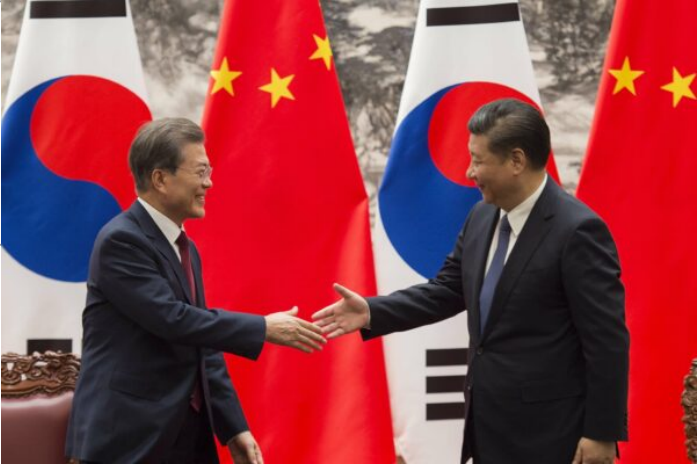
South Korea is not alone in facing tradeoffs around its growing exposure to Chinese telecommunications equipment. The dilemmas that South Korean companies and policymakers face as they weigh China’s role in their country’s digital future closely mirror those of other U.S. allies and like-minded partners. The UK, like South Korea, long wrestled with the decision to allow Huawei to build parts of its 5G networks before ultimately spurning the provider in mid-2020.⁶ Meanwhile, some countries are approaching the issue by banning Huawei from their networks without saying so outright. France quietly told domestic operators that they will not be able to renew licenses for using Huawei equipment once they expire in 2028, while assuring the Chinese government that the decision was about supporting European business solutions, rather than containing China.⁷ Looking even closer to home, Canada has put off making a final decision on Huawei, allowing political uncertainty to push providers to voluntarily reject Huawei without requiring a firm political decision that would further sour relations with Beijing.⁸

U.S. export controls on semiconductors to Huawei may have galvanized allies and partners in Europe and beyond to take steps toward banning or restricting the use of the Chinese telecommunications provider in their networks, but for American allies closer to China’s periphery, the decision may be more complex.⁹

Beyond Huawei’s heavily discounted prices, Beijing exerts significant leverage over large swaths of the region through its web of infrastructure loans and deep trade relationships.

Many emerging economies in Southeast Asia, where China’s economic heft far outstrips that of the United States, face a particularly fraught decision calculus. Beyond Huawei’s heavily discounted prices, Beijing exerts significant leverage over large swaths of the region through its web of infrastructure loans and deep trade relationships. China was already ASEAN’s largest trading partner when the China-ASEAN Free Trade Agreement went into effect in 2010, and bilateral trade volume has more than doubled in the decade since.¹⁰ Against this backdrop, rejecting Huawei’s telecommunications gear may come with steep diplomatic and financial costs.¹¹

China’s technology companies have emerged as leading players in a diverse set of high-tech projects across the Indo-Pacific ranging from data centers to “safe cities,” or public security platforms that leverage a network of connected devices through the Internet of Things to purportedly address a series of urban challenges such as transportation efficiency and crime prevention. Beijing’s position at the center of the Indo-Pacific’s digital architecture poses a series of acute challenges to U.S. and allied interests by allowing Beijing to introduce new technology standards that favor Chinese companies, opening the door to widespread data collection and mechanisms for social control, and compromising American military-cooperation and intelligence-sharing agreements with digitally entangled partners.



Korean President Moon Jae-in meets with Chinese President Xi Jinping during a four-day visit to Beijing in December 2017. At the time, the Moon administration was trying to mend ties after fallout from the U.S. terminal high altitude area defense (THAAD) row pummeled the Korean economy. (Nicolas Asfour-i-Pool/Getty Images)

Beijing’s position at the center of the Indo-Pacific’s digital architecture poses a series of acute challenges to U.S. and allied interests by allowing Beijing to introduce new technology standards that favor Chinese companies.

Notably, since 2018, the region as a whole registered a democratic decline, and governments of some countries have moved toward more statist visions of the internet.¹² Although Beijing’s export of its technologies is just one factor driving the spread of illiberalism, China is nonetheless positioned to bend the region toward a less open and free digital future. As global telecommunications markets grow more fragmented, Beijing is poised to double down on its export of digital infrastructure to American allies, such as South Korea, and to other similarly positioned countries that are highly dependent on Chinese markets and wary of the risk of coercion.

The Philippines: A Snapshot of Digital Entanglement with China in Southeast Asia

Though today South Korea is home to the United States’ largest overseas military installation, until 1992 that title was held by another nation that now finds itself caught between its American security guarantor and a domineering China: the Philippines.¹³ The only U.S. treaty ally that borders the disputed South China Sea, the Philippines has made a financial and strategic calculation to embrace not merely Huawei, but Chinese telecommunications writ large.

Defending the Philippines’ decision to work with Huawei in 2019, the Philippine Secretary of the Interior argued that it was acting in line with countries like the United Kingdom and Germany.¹⁴ But even as global momentum swung against Huawei this summer amid tightening U.S. export controls, both members of the Philippines traditional telecommunications duopoly, PLDT and Globe Telecom, reaffirmed that they would use Huawei equipment for their 5G rollouts.¹⁵ U.S. State Department officials have hinted at the possibility of offering funds through the Export-Import Bank or the U.S. Agency for International Development to assist budget-wary allies like the Philippines in changing course.¹⁶ But the island nation’s troubled telecommunications operators have more to consider than cost when it comes to Huawei.

The Philippines has some of the slowest 4G speeds in Southeast Asia, despite being home to the world’s most avid users of social media.¹⁷ Ostensibly to address the issue, Prime Minister Rodrigo Duterte awarded a license to a new market entrant, Dito Telecommunity, to break up the Philippines’ telecommunications duopoly. Dito, which is 40 percent owned by China Telecom, hopes to make a commercial launch in 2021.¹⁸ Dito has tried to assuage opposition concerns, particularly over the Defense Department’s decision to allow its towers inside military bases, by signing a \$20 million partnership with American security firm Fortinet.¹⁹ But with billions of dollars needed upfront to prepare its rollout, it has taken out a \$500 million loan from the Bank of China.²⁰

But Chinese telecommunications companies have not been allowed in merely to provide cheap networks. Through the “Safe Philippines Project,” finalized during Xi’s visit to the Philippines in 2018, Huawei and China International Telecommunication and Construction Corporation are building more than 12,000 CCTV cameras and integrated command centers across several cities with the help of nearly \$400 million in loans from China Eximbank.²¹

Pressed on the potential danger of digital entanglement with China, Duterte has argued that China’s resultant leverage is meaningless so long as the two nations’ interests are in line. China and its military “do not mean harm” as long as “we do not also do something that is harmful to them,” he said.²² Duterte’s vocal skepticism about the China threat is not unique among leaders in the region—“What is there to spy in Malaysia? We are an open book,” Malaysian Prime Minister Mahathir Mohamad argued in 2019 in defense of a contract with Huawei.²³ But for the

Philippines, a U.S. treaty ally that in 2016 won a landmark case against China in The Hague, Duterte’s confidence in the benign nature of Chinese digital entanglement might be misplaced.²⁴

Examining the Trajectory of South Korea’s Digital Entanglement with China

By some metrics, South Korea is at the forefront of 5G network deployment and innovation.²⁵ In April 2019, South Korea became the first country in the world to launch commercial 5G services, and South Korea’s Ministry of Science and Information and Communications Technology (ICT) raced to install 5G kits at airports, train stations, and large shopping centers to boost coverage.²⁶ South Korea expects to have 10 million 5G subscribers by the end of 2020, and the Blue House announced its intent to ensure nationwide 5G coverage by 2022.²⁷

But as South Korea’s 5G ambitions expand and continue to encompass fields such as autonomous vehicles and smart cities, China is quietly seeking to shape the course of South Korea’s digital future.²⁸ Huawei’s enmeshment within South Korea’s digital ecosystem is significant. South Korean companies supply Huawei and other Chinese tech giants with semiconductors, memory chips, smartphone displays, and other components.²⁹ Through a partnership between Huawei and the Korean Ministry of Education, South Korean students annually participate in Huawei’s Seeds for the Future program, which provides scholarships for students to spend two weeks in Beijing and at Huawei headquarters in Shenzhen learning about China’s technology and innovation ecosystem.³⁰ In May 2019, Huawei unveiled an open lab in Seoul for South Korean companies to test their platforms with the purported aim of “building a 5G ecosystem through cooperation with Korean ICT companies, in particular, small businesses.”³¹ The same month, South Korean database management company TmaxData signed a memorandum of understanding (MOU) with Huawei to use the Chinese tech giant’s servers for its own cloud services center.³²

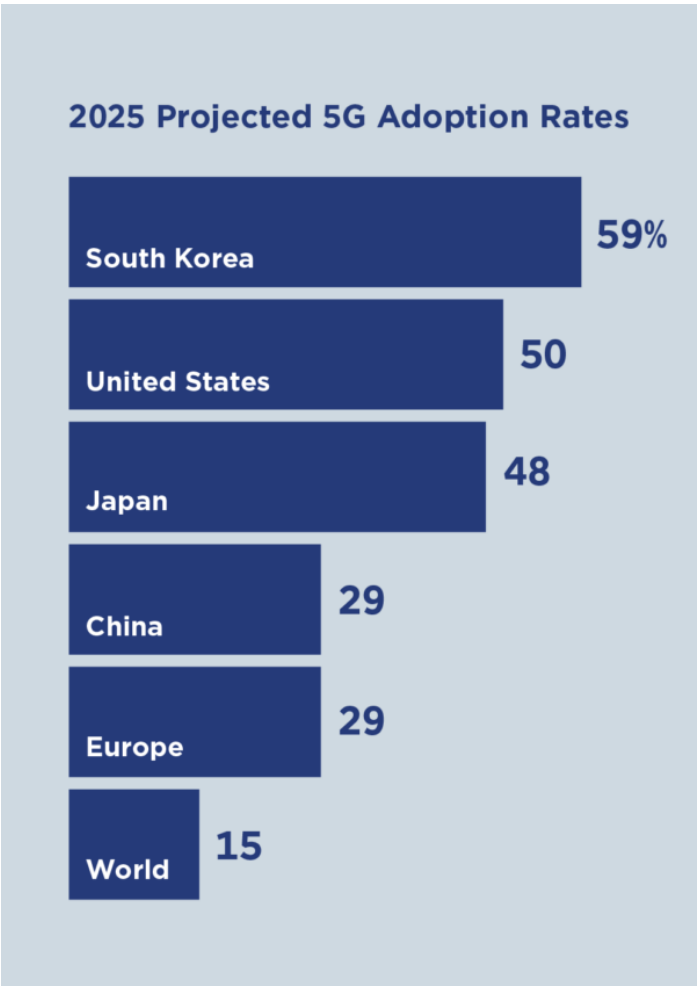
Four primary endogenous and exogenous trends in South Korea’s politics and economy have characterized the overall disposition of the country’s digital ecosystems and potentially increased its receptivity to digital entanglement with China:

First, and perhaps most consequentially, ongoing U.S.-China trade and political tensions have landed South Korea in a familiar bind, wedged between its most important ally and its largest trading partner.³³ While the Trump administration focuses on strategic competition with Beijing and has arrayed coercive economic measures against it, Seoul has charted a different path. Stung by Chinese punishment after then-President Park Geun-hye installed the U.S. terminal high altitude area defense (THAAD) missile defense system, the Moon administration has pursued a policy of “balanced diplomacy.”³⁴ With the THAAD incident seared into the country’s political memory, Seoul has been wary of additional economic retribution if it restricts domestic use of Huawei’s equipment.³⁵ Indeed, in 2019, Beijing warned South Korean companies such as Samsung and SK Hynix, which rely heavily on the export of components to Huawei, that there would be repercussions if they responded too aggressively to U.S. trade restrictions.³⁶ Only in September 2020, with added U.S. government restrictions on sales to Huawei set to kick in, did the Korean companies announce that they would stop supplying Huawei—nearly two months after Taiwan Semiconductor Manufacturing Company had announced plans to do so.³⁷

Second, geopolitical risk assessments are not applied in a consistent and streamlined manner in South Korea’s technology policymaking calculations. While South Korean officials have not dismissed the security risks of partnering with Huawei to build South Korea’s 5G infrastructure, they have also chosen not to elevate national security issues as a critical determinant of the country’s telecommunications policies and overall posture toward Chinese investment in their domestic digital markets. Blue House officials have, for example, noted that South Korea uses Huawei hardware for less than 10 percent of its 5G networks and that the equipment is “isolated from defense and security telecoms networks” and thus will not have an impact on South Korea-U.S. security interests.³⁸



Philippine President Rodrigo Duterte and Chinese President Xi Jinping attend a meeting at the Great Hall of People in April 2019. During his trip, Duterte concluded 19 agreements with Chinese companies to invest in the Philippines. Duterte has visited China five times since taking office. (Pool/Getty Images)



By 2025, South Korea and the United States are expected to have the highest rates of cell phone users subscribed to 5G, 59% and 50% respectively. Together, the two will have enormous market-setting power. Source: Eun-Young Jeong, “5G Underwhelms in Its First Big Test,” The Wall Street Journal, December 31, 2019.

While South Korean officials have not dismissed the security risks of partnering with Huawei to build South Korea’s 5G infrastructure, they have also chosen not to elevate national security issues as a critical determinant of the country’s telecommunications policies and overall posture toward Chinese investment in their domestic digital markets.

Third, and relatedly, the Blue House has largely delegated the authority to include or exclude Huawei from the country’s 5G networks to individual companies, and absent clear political leadership, South Korean industry has become reliant on Huawei to its detriment. South Korean companies remain divided about the role that Huawei has to play in South Korea’s 5G future. Huawei currently provides network equipment to one of South Korea’s major carriers, LG Uplus, while the other two carriers, SK Telecom and KT, have opted not to use Huawei gear.³⁹ For corporations, the economic case for using Chinese equipment is compelling. Some South Korean companies, most notably LG Uplus, have calculated that the benefit of using Huawei’s cheaper equipment outweighs the risks of privacy breaches and other security concerns.⁴⁰ Although its 5G customer base trails behind that of SK Telecom (with 45 percent of total 5G subscribers) and KT (30 percent), LG Uplus still accounts for about a quarter of 5G users, according to data from South Korea’s Ministry of Science and ICT.⁴¹

Fourth, the legal and regulatory environment around privacy protections in South Korea remains fluid and is evolving to meet political and public health demands and to potentially generate new commercial opportunities abroad. For many years, South Korea took a relatively lax approach to data privacy. In 2015, for example, the South Korean Supreme Court ruled that eBay Korea was not required to pay compensation after a 2008 hacking incident in which a backdoor was used to leak the personal information of about 10 million people, dismissing the plaintiff’s charge that eBay Korea should have done more to protect consumer data.⁴² In a bid to bring its laws into line with the EU’s General Data Protection Regulation, however, South Korea’s National Assembly passed major amendments to the country’s Personal Information Protection Act in January 2020. The amendments introduced the use of “pseudonymized information,” making it more difficult to identify an individual based on their data, and added “purpose limitation” requirements to limit the possible uses of collected data.⁴³ But the emergence of the COVID-19 pandemic has pulled the regulatory environment away from such strict curbs. The government shored up its ability to collect and utilize data—through extensive contact tracing and surveillance technology—without consent to curb the spread of COVID-19 within South Korean borders.⁴⁴ At the height of the viral outbreak, South Korean officials and the Korea Centers for Disease Control and Prevention leveraged the country’s smart-city technologies coupled with location tracking and financial transaction records to trace carriers of the virus.⁴⁵



South Korean chipmakers Samsung Electronics and SK Hynix were earning upwards of \$8 billion from annual sales to Huawei before American sanctions forced them to cut ties in September. (SeongJoon Cho/Bloomberg via Getty Images)

These four trends are unpacked further in the following section that examines the origins and the risks of South Korea’s digital entanglement with China.

The Origins of South Korea’s Digital Entanglement with China

South Korea’s private sector is deeply dependent on China, a dependency that Beijing has weaponized to limit Seoul’s strategic autonomy. These two factors have led South Korea down the road of digital entanglement with China.

Laissez-faire policies and private sector path dependency

Since normalizing relations with China in 1992, South Korea has reaped immense material benefits from deepening ties with its neighbor. By 2018, South Korea exported more than \$160 billion worth of goods to China, notching an annual trade surplus of nearly \$60 billion with its largest trading partner of nearly two decades. Exports to China are worth more than the total value of those to Korea’s next two largest export markets combined.⁴⁶ As domestic growth slowed despite surging exports, moreover, Korean companies poured investment into China. During the first decade of the 2000s, China surpassed the United States as the top destination for Korean foreign direct investment.⁴⁷

Though growing economic entanglement with China drove profit growth at many Korean companies, it did not come for free. South Korea’s extensive investments in and exports to the Chinese market have left the Korean policymaking process deeply exposed to Chinese pressure. This helps explain South Korea’s ambivalence toward removing Huawei from its 5G networks.

When Huawei first entered the South Korean market in 2007, of course, 3G signals were pulsing through the air and China was a low-end manufacturer assumed to be committed to a peaceful rise. Risks of Chinese economic bullying seemed distant. While Huawei made limited initial headway in the Korean mobile-phone market, it lodged its first major success there in 2013 when LG Uplus chose the Chinese telecoms company as one of its 4G equipment providers. LG Uplus had long languished in third place in the Korean telecommunications market, unable to challenge the more established SK Telecom and KT. Huawei offered LG Uplus a chance to gain a leg up in cost competitiveness—South Korean foreign policy insiders said that Huawei offered as much as a 30 percent discount against alternatives.⁴⁸

Then-South Korean President Lee Myung-bak opted to leave the decision up to the private sector. LG Uplus insisted that it would keep Huawei equipment out of its networks near U.S. military bases, thus mitigating any security risks.⁴⁹ In hindsight, one former Korean trade negotiator said, “It was a digital Pearl Harbor moment.”⁵⁰ Despite the pressure that Washington has exerted on allied capitals to eschew the use of Huawei, the Moon administration has been circumspect about engaging with and directing the private sector, given previous governments’

corruption scandals associated with South Korea’s *chaebols*, or massive and largely family-run conglomerates.⁵¹

Once Huawei was integrated into Korean infrastructure, it became hard to remove. After all, LG Uplus, South Korean exporters, and the government all stood to lose from doing so. LG Uplus had made a long-term bet on Huawei. Once a telecoms operator uses a vendor for 4G, switching vendors for 5G can bring added headaches. LG Uplus thus had significant economic incentives to downplay security concerns—and it signaled its good-faith consideration of security concerns by forming a partnership with S-1, a South Korean security company, to address espionage risks.⁵² If figures from the UK offer even just an anecdotal reference point, the costs of removing Huawei equipment for LG could range from somewhere between hundreds of millions to billions of dollars.⁵³

LG Uplus insisted that it would keep Huawei equipment out of its networks near U.S. military bases, thus mitigating any security risks. In hindsight, one former Korean trade negotiator said, “It was a digital Pearl Harbor moment.”

It would cost other Korean technology companies, too, if South Korea took forceful action against Huawei. In 2019, Huawei purchased \$11 billion worth of South Korean products for its network equipment and cell phones. In the hopes of ingratiating itself further with the Korean business community, it vowed to increase that total in 2020.⁵⁴ Sales to Huawei already accounted for nearly 2 percent of total South Korean exports in 2018.⁵⁵ This provides Huawei an important constituency of advocates within South Korea—its suppliers. As South Korean companies comply with new U.S. sanctions, the producers of some of that \$11 billion worth of parts will see sales drop sharply.

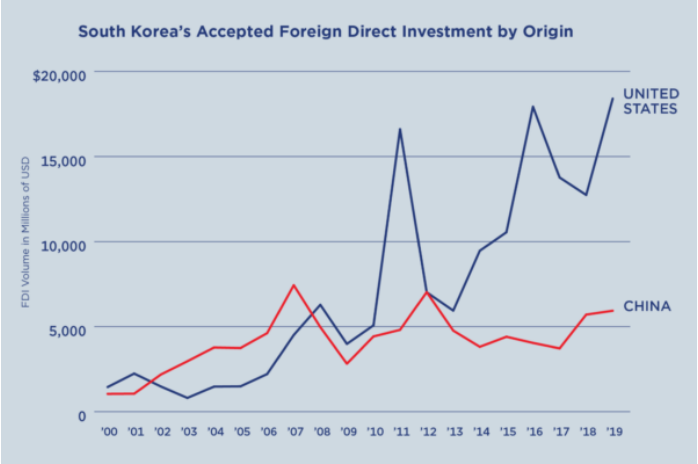
The long shadow of economic coercion

But beyond the concerns of LG Uplus or Huawei’s Korean suppliers, it is the interests of Korean exporters and multinationals at large that force the South Korean government to toe a careful line on 5G policy. Seoul learned a lesson about crossing Beijing in 2017, when China punished South Korea for hosting the United States’ THAAD missile system. In 2016, Chinese tourists had accounted for half of all visitors to South Korea; after the row over THAAD, their number dropped more than 60 percent.⁵⁶ Across China, the government shuttered South Korean retail chains, decimating profits at major conglomerates like Lotte Corporation. Chinese consumers boycotted Korean cars, and Chinese stores stopped carrying Korean cosmetics.⁵⁷ Beijing weaponized Korean exporters’ and investors’ dependence on China.

The shadow of the THAAD aftermath hangs heavily over South Korea’s 5G decision-making. Though South Korea’s Minister of Science and ICT You Young-min suggested in January 2018 that Korean 5G providers should use domestically manufactured equipment, by July he had walked the idea back. Minister You noted at the time, “Huawei security issues in 5G should not be discussed because China is sensitive to it. I’m afraid that there would be a dispute.”⁵⁸ In other words, Korean policymakers had more than security concerns to worry about when it came to Huawei—a move against Huawei could jeopardize the health of the whole economy. Huawei had already penetrated the South Korean market, and if it were to be removed, it would not go quietly.

Still scarred by the memory of Beijing’s punitive economic policies in 2017, the Blue House continues to uphold its position that individual companies—and not the government—must choose whether or not to use Huawei 5G equipment. Considering the importance of shaping the digital infrastructure of the Indo-Pacific to Chinese foreign policy, passing off responsibility to industry may be of limited use as a tactic to dodge the ire of Beijing. China’s coercive diplomacy, such as the beef boycotts and barley tariffs that met Australia’s call for an investigation into the origin of the COVID-19 outbreak, has been anything but subtle.⁵⁹ On the other hand, discussions between Chinese and South Korean diplomats about working together to approach North Korea offer a distant glimmer of hope for progress on Moon Jae-in’s white-whale issue—that is, if Seoul can avoid provoking Beijing.⁶⁰

The Risks of Digital Entanglement



Korean foreign direct investment (FDI) from China had outpaced flow from the United States in the mid-2000s. However, the trend reversed in the 2010s with the advent of the United States-Korea Free Trade Agreement (KORUS FTA). Since then, the gap has widened significantly with FDI from the United States more than doubling Chinese FDI in 2019. The notable bump in FDI from the United States in 2016 coincides with the THAAD deployment decision. FDI outflows from Korea mirror these trends. Source: Statistics of Foreign Direct Investment, The Export-Import Bank of Korea (Korea Eximbank, 2020), <https://stats.koreaexim.go.kr/en/enMain.do>.



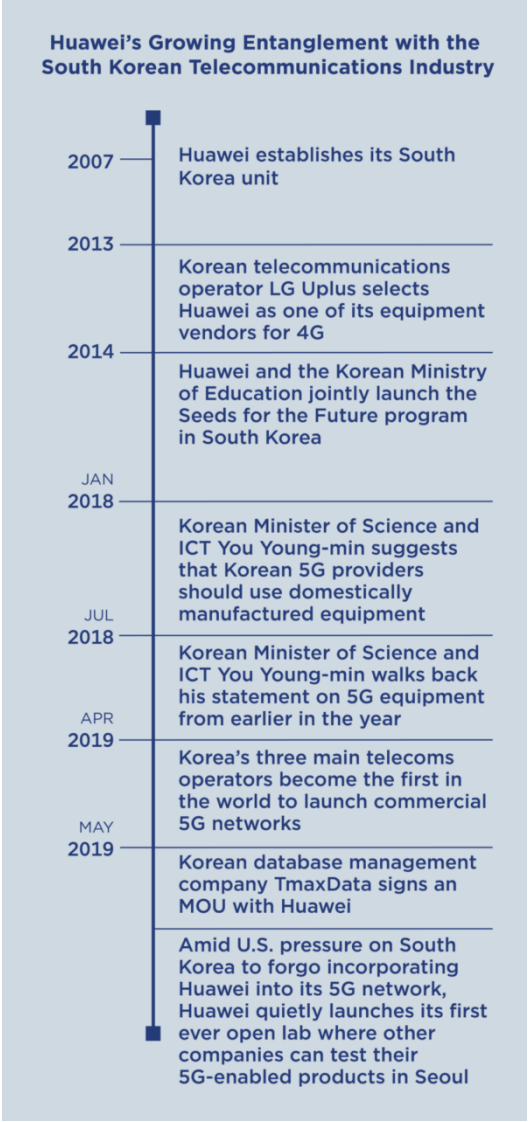
After Seoul announced in July 2016 that it would deploy the THAAD missile defense system, Beijing responded to the perceived slight with an intense campaign of economic coercion. (Chung Sung-Jun/Getty Images)

Proponents of Huawei’s inclusion in South Korea’s 5G network typically point to the understanding between Washington and Seoul in 2014, when LG Uplus agreed to keep Huawei 4G away from U.S. military installations.⁶¹ Even if such an agreement could be augmented reliably to the current 5G situation, the UK debate on using Huawei indicates the extent to which Seoul’s exposure to risk extends beyond locations with a U.S. presence.

The United Kingdom initially decided in early 2020 to allow Huawei 5G, but to limit it to the “periphery” of the overall network and away from areas sensitive to national security. At the time, UK experts noted that attempts to isolate Huawei’s presence to the periphery will become increasingly difficult as the technology becomes more software-driven, which also inherently makes it more vulnerable to hackers.⁶² Part of the technology responsible for 5G’s speed blurs the lines between the network’s core and edge that are clear in 4G networks. This makes it infeasible to cleanly separate sensitive parts of a 5G network from an untrusted vendor, even though it may have been possible with 4G.⁶³ By July, London reversed its decision and banned Huawei 5G outright after a thorough government audit concluded that addressing its myriad coding and security software flaws was beyond the company’s capacity.⁶⁴

If the network were only vulnerable through “backdoors,” LG Uplus’s 5G would be primarily vulnerable to Chinese intelligence agencies. However, the problem of pervasive security flaws that Huawei is incapable of addressing leaves South Korea excessively vulnerable to catastrophic cyberattacks from other actors, such as increasingly bold and capable hackers in North Korea.⁶⁵ The security of user data is far from the only concern—5G will become the cornerstone of communications networks responsible for critical infrastructure such as water supplies, transportation, and power grids.⁶⁶ Even if the networks are never targeted in attacks, similar disastrous disruptions could easily occur if Huawei is compelled to delay maintenance and replacement during a low point in Republic of Korea (ROK)-China relations.⁶⁷

Because of the ubiquity of the internet in even society’s most basic tasks, digital entanglement with China will continue to present a significant threat to South Korean security if it is not addressed. With LG Uplus 5G in place, these risks are already unfolding in real time. For example, amid the COVID-19 pandemic and the growing prominence of telemedicine, South Korean consumers and doctors alike have expressed concern about the security of the networks through which consultations are being conducted. As the country piloted telemedicine well before the pandemic, the use of these technologies to address public health concerns has been met with some opposition, including by the Korean Medical Association, citing safety concerns and the detrimental impact on smaller clinics.⁶⁸ As debates and regulations around the use of telemedicine continue to evolve amid the pandemic, network security issues will only warrant greater scrutiny in South Korea.



Since entering the Korean market in 2007, Huawei has steadily expanded its ties with domestic stakeholders, deepening South Korea’s digital entanglement with China.

Part of the technology responsible for 5G’s speed blurs the lines between the network’s core and edge that are clear in 4G networks. This makes it infeasible to cleanly separate sensitive parts of a 5G network from an untrusted vendor, even though it may have been possible with 4G.

The short-term monetary and diplomatic costs of maintaining South Korean data integrity and security by eliminating untrusted ICT vendors will only increase as the decision is delayed. LG Uplus chose Huawei as a 5G vendor in part because of Huawei’s role in the company’s 4G networks.⁶⁹ Companies may face a similar decision calculus during South Korea’s 6G rollout. Fortunately, there is a path forward that minimizes both South Korea’s security risk and the risk of retribution from China—but it will require a concerted effort from South Korean policymakers and industry alike.

Policy Recommendations for the U.S. Government

Like many other export-dependent U.S. allies, Seoul is ill inclined to adopt policy positions that may provoke Beijing and put Korean companies in the path of China’s economic retribution.⁷⁰ In light of the delicate balance at play, this section advances a set of overarching guiding principles as well as specific recommendations for the U.S. government to, in coordination with South Korea and partners in the Indo-Pacific, mitigate the risks associated with Chinese digital investment into its domestic markets.

Principle 1: Advance an evidence-based framework for evaluating and communicating 5G network security risks.

Recommendation 1: Expand mechanisms for sharing intelligence with South Korea and other allies on 5G network and supply chain security issues.

Different American allies have different levels of risk tolerance for building out their telecommunications infrastructure. While perfect alignment on risk is unlikely, information-sharing on 5G network security issues can be improved through regular, established channels of communication. In the South Korean context, the U.S. government could expand Track 1.0 dialogues with Seoul around emerging technology issues, complementing the robust network of Track 2.0 dialogues already in place.⁷¹ Existing communication streams like the U.S.-ROK Cyber Policy Consultations could also be leveraged to share intelligence on new network security issues, including and beyond those associated with Chinese telecommunications equipment. Additionally, the Department of Defense should consistently introduce supply chain security issues in their dialogues with South Korean counterparts, with an eye toward developing reliable alternatives to and precluding deepening enmeshment with China’s defense industrial base.

Recommendation 2: Launch a public diplomacy initiative to better inform citizens in South Korea and other Indo-Pacific countries about 5G network security.

While efforts to align views on critical infrastructure will primarily rely on government-to-government communications, Washington also needs to clearly communicate the risks of using technology originating from illiberal countries to South Korean and allied publics. In the South Korea context, the U.S. government should also expand engagement with South Korean institutions that are already keyed into 5G issues in order to help center security considerations in the broader Korean discourse around 5G. Specifically, Seoul National University, Hanyang University, the Korea Development Institute, and the Korea Institute for International Economic Policy have all been involved in debates about 5G policy and could serve as fruitful partners.⁷² Additionally, the United States could share any unclassified findings about some of the security flaws linked to Huawei’s telecommunications equipment with local news outlets.

Principle 2: Set conditions to cultivate cost-competitive, readily available 5G equipment providers to compete with Huawei.

Recommendation 3: Mitigate the economic impact South Korea and other allies confront in rejecting Huawei by bolstering the presence of other 5G RAN market players.

Samsung, for example, has largely struggled to gain traction in global markets for 5G network installation, lacking the insider access to a massive domestic market that helped power Huawei’s rise. Washington should continue to emphasize the role of Samsung and other providers in advancing high-quality alternatives. At the start of 2020, South Korea and the United States were predicted to account for three-quarters of all 5G subscribers by the end of the year, and the United States is already home to Samsung’s largest 5G equipment market outside of South Korea.⁷³ Verizon also recently became the first telecommunications company to contract Samsung not only for 5G network equipment, but also for long-term network construction and maintenance.⁷⁴ Washington should capitalize on this initial momentum by orienting the Clean Network program in communications with allies less exclusively around eliminating Huawei from allied networks and more affirmatively about creating concrete market opportunities for companies from like-minded countries to advance secure network alternatives.⁷⁵

Recommendation 4: Promote development of 5G infrastructure built on a modular architecture with open interfaces by investing in open RAN technology.

The U.S. government should use its procurement process and research dollars to spur further private sector investment in open RAN technology, creating a cost-effective alternative to the 5G triopoly (namely, Huawei, Ericsson, and Nokia).⁷⁶ In addition to research funding and procurement support, the government can play a larger role in incentivizing the testing of and setting goals toward interoperability, such as through tax incentives. Numerous commercial deployments have demonstrated open RAN’s viability for 5G.⁷⁷ A national level 5G network rollout taking place in Japan in late 2020 will be the largest global deployment so far.⁷⁸

South Korea, home to one of the world’s leading telecommunications industries and some of the world’s most cutting-edge technology companies, is crucial to any such open RAN push. South Korea is also already putting hundreds of millions of dollars into kickstarting early-stage 6G research, which could be another area for bilateral cooperation.⁷⁹ By teaming up with South Korea to develop open RAN telecommunications technology, the United States can leverage South Korea’s leadership in telecommunications to lead on innovation in the next generation of open technologies. Open RAN technology allows a network to use multiple vendors in its rollout, enabling market entry for American and Korean companies currently locked out of many markets by Huawei, Ericsson, and Nokia.

Principle 3: Invest in diplomatic and security arrangements that mitigate vulnerability to coercion.

Recommendation 5: Work with South Korean counterparts to strengthen and streamline geopolitical risk assessments into technology policymaking mechanisms.

Huawei was able to enter the Korean market because the Korean government decided to largely leave the matter to the private sector, and LG Uplus made its decision based on price.⁸⁰ In other words, insufficient consideration was given to the security and geopolitical implications of commercial 5G contracts. South Korea already has robust mechanisms in place to integrate national security considerations early in the policymaking process in areas like energy policy.⁸¹ But the U.S. government should also work with Korean officials to build out mechanisms for systematically bringing national security concerns into decision-making processes on investments around cutting-edge technologies such as next-generation telecommunications equipment. Through robust bilateral discussions, the Committee on Foreign Investment in the United States (CFIUS) investment screening model is being replicated in Israel, for example, to protect domestic intellectual property.⁸²

Recommendation 6: Engage multilateral groupings to mitigate Chinese economic coercion throughout the Indo-Pacific.

A united front is needed to blunt Beijing’s efforts at economic coercion. Economic dependence on China has proven a key challenge for South Korea. Although Beijing’s attempt to disrupt the deployment of THAAD soured public opinion, its punitive actions achieved the intended effect, insofar as Seoul is now more reluctant to defy China.⁸³

U.S. allies and partners around the world should issue joint statements to publicly call out Beijing and condemn specific instances of Chinese coercion. These words should be followed with action. Washington—in concert with a broad set of U.S. allies, including South Korea—should establish a counter-coercion fund.⁸⁴ Members of this fund would come together to define the criteria for what counts as Chinese economic coercion, and then pool resources to help compensate those experiencing losses due to actions taken by Beijing. Variations of this concept have been proposed by American and Japanese scholars.⁸⁵

At the same time, the like-minded countries of the Indo-Pacific should lead the way on reducing Beijing’s ability to issue economic threats. This would entail restructuring key supply chains to reduce dependency on China for key raw materials, such as rare earth elements, and finished products, such as medical equipment. Burgeoning efforts to do exactly this—for example, the U.S.-led Economic Prosperity Network and the Japan-led Supply Chain Resilience Initiative—should be codified, expanded, and funded.⁸⁶

Principle 4: Advance an affirmative technology cooperation agenda.

Recommendation 7: Pursue multilateral approaches to technology policy coordination and collaboration.

Opportunities abound for collective action by like-minded countries. Because existing groupings such as ASEAN, the East Asia Summit, and G20 comprise members that are at odds with the United States and South Korea on these issues, new groupings and forums are needed.

Strengthen regional cybersecurity postures. South Korea and the United States have been at the forefront of dealing with cyberthreats to modern economies and modern democracies. They should engage allies and partners in the Indo-Pacific and beyond to better cooperate on cybersecurity. Step one should be multilateral engagement for setting norms for a free and open cyberspace. In March 2020, the U.S. Cyberspace Solarium Commission issued recommendations—such as for building an enforceable rules-based international order in cyberspace and re-engaging on effective international standards-setting—that provide a good starting point for collective action.⁸⁷ A common approach among these like-minded countries could then serve as an opening for engagement with problematic cyber actors including China and Russia.

The second step should be to craft multilateral responses to illiberal cyberactivity in accordance with international law. Because the United States, South Korea, and their allies in the region share liberal democratic values, it is feasible to craft consensus responses to cyberoperations such as disinformation campaigns or state-backed technology theft, even with variations in ethical and legal frameworks.⁸⁸

Include South Korea within an alliance innovation base. Washington should forge an alliance innovation base, a community of practice focused on advanced technology protection and innovation, that includes South Korea and other technologically advanced, like-minded countries. The purpose of an alliance innovation base would be twofold: to synchronize technology protection regulations among an informal group of allies and partners, and to offset the opportunity cost of enhanced regulations by promoting market access and research collaboration within a close circle of technologically capable allies.⁸⁹ The open-architecture model of an alliance innovation base framework would enable the United States and South Korea to work together bilaterally or in minilateral groupings of their choice. Some shared military-operational and technical challenges that are promising areas for cooperation include new approaches to maritime intelligence, surveillance, and reconnaissance; building military network resiliency; and diversifying options for 5G and next-generation telecommunications network implementation. One possibility would be a partnership between the Defense Department’s Defense Innovation Unit and the ROK National IT Industry Promotion Agency’s K-Startup Grand Challenge to create a multinational startup challenge focused on addressing regional technology needs.

Retake the initiative on promoting norms around technology use. Washington should launch a set of dialogues with South Korea and other democratic allies to co-develop liberal norms and best practices for the use of cutting-edge technologies, which can then ultimately influence the development of standards. In the South Korean context, for example, Washington can organize dialogues with participation by U.S. and South Korean industry groups on artificial intelligence ethics and cloud computing interoperability standards. The State Department’s Bureau of International Information Programs could also support exchanges between governments and civil-society groups in select democratic allies and advance partnerships between American and foreign think tanks to help integrate on-the-ground knowledge of developments elsewhere into the U.S. conversation about digital norms.

Close the Indo-Pacific digital divide. The United States and South Korea should join forces with Australia, Japan, and potentially India to create a standing multilateral mechanism to support digital infrastructure development in emerging countries in the Indo-Pacific. This effort should have two overriding goals. One is to provide cost-effective alternatives for 5G and future-generation telecommunications infrastructure to promote data integrity and to protect critical infrastructure in the region. The second goal is to ensure that digital infrastructure projects comport with liberal democratic values by, for example, countering China’s export of surveillance technology and know-how. To help garner widespread support in the region for alternative infrastructure, investment criteria should be based on the G20 Principles for Quality Infrastructure Development and those of the Blue Dot Network.⁹⁰

Bolster technology capacity in the Indo-Pacific, including through continuing to promote deeper alignment between South Korea’s New Southern Policy and the United States’ Indo-Pacific Strategy. Building a stronger technology base in various Indo-Pacific countries is a proactive and affirmative approach to reducing the appeal of Chinese technology offerings. The New Southern Policy aims to promote South Korean technology companies across the region, but thus far coordination with the U.S. Indo-Pacific Strategy on 5G in the Indo-Pacific has been limited to policy capacity-building initiatives run by the State Department and the Korean Ministry of Foreign Affairs.⁹¹ Leading Indo-Pacific tech powers like Australia, India, Japan, South Korea, and the United States should pursue joint research and development in areas of mutual interest. Taiwan should be included wherever feasible, although some of these engagements would have to take place privately if partner governments deem it too provocative toward Beijing. There are a range of technology disciplines that are suitable, including artificial intelligence, novel materials and energetics, information and communication technologies, and space technologies.

Recommendation 8: Create an alliance framework for technology policy.

The ultimate approach to these issues is to create a new international grouping to collaborate on matters of technology policy. While this is an ambitious and complex endeavor, many have made the case for such a grouping, most notably British government officials’ call for a “Democracy 10” to tackle 5G and former U.S. government officials’ advocacy for the creation of a “Tech10.”⁹²

In this vein, an international group of researchers proposed an actionable framework for a multilateral technology pact—comprising Australia, Canada, France, Germany, Italy, Japan, the Netherlands, South Korea, the United Kingdom, and the United States, with the EU as a non-voting member. Recommended priority areas include securing and diversifying supply chains in part to safeguard against economic coercion, protecting critical technology with methods such as more robust export controls, and creating new investment mechanisms to promote and proliferate secure digital infrastructure.⁹³

Conclusion

The competition between Beijing’s 5G offerings and nascent democratic alternatives is playing out most consequentially in U.S. allied countries—such as South Korea—that already have deep economic and technological interdependencies with China. Thus far, the U.S. approach has been largely limited to a fierce, at times heavy-handed, global campaign about the dangers of Huawei. Meanwhile, U.S. investments in 5G research and international standard-setting bodies remain either meagerly funded or not yet fully enacted.

Talk is cheap but unwinding digital entanglement with China is not. Many American allies and partners perceive tough reassessments of Chinese technology companies as coming with serious costs to fix a problem that poses unclear risks. Persuading them otherwise will require a deep American investment in the technologies, governing mechanisms, commercial incentive packages, and private sector partnerships that undergird alliances—all of which are too often taken for granted. These investments should, of course, be coupled with a comprehensive communications and public diplomacy strategy. Without a nuanced policy approach calibrated to the domestic needs of allies most exposed to Chinese technological entanglement, the United States might find itself at the head of a shrinking coalition of the increasingly unwilling.

Endnotes

1. “China’s 5G Network: A Strategic Challenge for the United States,” *Brookings Institution*, 2019, <https://www.brookings.edu/research/china-5g-network-a-strategic-challenge-for-the-united-states/>.

Authors



Kristine Lee

Associate Fellow, Asia-Pacific Security Program

Kristine Lee is an Associate Fellow with the Asia-Pacific Security Program at the Center for a New American Security (CNAS), where she focuses on U.S. alliances and partnershi...



Martijn Rasser

Senior Fellow, Technology and National Security Program

Martijn Rasser is a Senior Fellow in the Technology and National Security Program at the Center for a New American Security (CNAS). Prior to joining CNAS, Mr. Rasser served as...



Joshua Fitt

Research Associate, Asia-Pacific Security Program


Joshua Fitt is a Research Associate for the Asia-Pacific Security Program at the Center for a New American Security (CNAS). He focuses on U.S. East Asian security strategy and...










Coby Goldberg

Intern, Asia-Pacific Security Program

Coby Goldberg is the Joseph S. Nye, Jr. Intern for the Asia-Pacific Security Program at the Center for a New American Security (CNAS). Prior to joining CNAS, Coby interned at ...

 Center for a New American Security
1152 15th Street, NW
Suite 950
Washington, DC 20005

 (202) 457-9400  info@cnas.org

-  [Facebook](#)
-  [Twitter](#)
-  [SoundCloud](#)
-  [YouTube](#)
-  [Flickr](#)

- [About](#)
- [Events](#)
- [Internships](#)
- [Careers](#)

- [Support CNAS](#)
- [Follow CNAS](#)
- [Press](#)
- [Contact](#)

© 2020 Center for a New American Security (en-US).