Journal of Aerospace & Security Studies
2024 | Volume III | pp. 97-121

5G Geopolitics: Securitisation, Sino-US Contention and Technological Dependence for Developing States

Mustafa Bilal

Abstract

This paper provides a nuanced perspective on the interplay between security, geopolitics, and economic pragmatism in the global 5G domain. It examines the origins and dynamics of the diplomatic pressure campaign led by the United States against Chinese telecommunications companies since 2018. Using a qualitative methodology and Securitisation Theory, the study analyses how US policymakers and academics have framed Chinese telcos as national security threats. The study also explores the broader implications of Sino-US tensions over 5G. The findings reveal that securitising Chinese telcos, notably Huawei, has been a strategic move to curtail their expanding global influence. However, state responses to this campaign have been shaped by differing geopolitical and economic considerations. While most US allies have distanced themselves from Chinese telcos, many developing states, such as those in Africa and South Asia, have continued to embrace them due to their strong economic, political, and technological ties with China.

Keywords: 5G, China, US, Geopolitics, Chinese Telcos, Huawei, Securitisation, Developing States.

Introduction

5G is crucial for the digital transformation of societies as it holds the key to unlocking the potential of future industries via its speed, latency, and bandwidth.[1] This paper examines how 5G has become a priority area in international relations, underscored by GSMA's estimation that 5G will make up 15% of global mobile networks by 2025.[2] There are estimated to be 1 billion 5G connections in China alone.[3] However, think tanks in the United States (US) have expressed concern that the country is likely to face vulnerabilities as China's lead in 5G development could impact both economic prosperity and national security.[4] This concern was also underscored by the admission by former US Secretary of Commerce Gina Raimondo that the 5G race had begun and the US

1 Börje Ekholm, "How 5G's Innovation Potential Will Lift Digitalization to the Next Level," *World Economic Forum,* January 12, 2024, https://www.weforum.org/agenda/2024/01/5g-innovation-digitalization/.

2 GSMA, "New GSMA Study: 5G to Account for 15% of Global Mobile Industry by 2025 as 5G Network Launches Accelerate," press release, February 25, 2019, https://www.gsma.com/newsroom/press-release/new-gsma-study-5g-to-account-for-15-of-global-mobile-industry-by-2025/.

3 GSMA, "China's 5G Market Is Set to Add Almost $260 Billion to the Chinese Economy in 2030 with Connections Set to Top 1 Billion This Year, " press release, December 13, 2024, https://www.gsma.com/newsroom/press-release/chinas-5g-market-is-set-to-add-almost-260-billion-to-the-chinese-economy-in-2030-with-connections-set-to-top-1-billion-this-year/.

4 Ngor Luong, *Forging the 5G Future: Strategic Imperatives for the US and Its Allies*, report (Washington, D.C.: Atlantic Council, September 4, 2024), https://www.atlanticcouncil.org/in-depth-research-reports/report/forging-the-5g-future-strategic-imperatives-for-the-us-and-its-allies/.

would strive to win.[5] From the US perspective, compelling allies and friendly states to ban Chinese telecommunications companies (referred to as 'telcos') was key to winning this race.

Against this backdrop, the paper explores how development and deployment of 5G infrastructure has become marred by contentious geopolitics. It examines how the US has adopted a strategy centred on restricting market access to Chinese telcos and pressuring their allies to follow their lead. Central to this examination is emphasising this strategy's core foundation: *securitisation of Chinese telcos*.

The paper will seek to address the following research questions: Why has 5G become a focal point of Sino-US tensions? How did the US diplomatically pressure allies to ban Chinese telcos? How have Western academic publications further propagated this securitisation discourse? And how have developing states like Pakistan and India navigated the Sino-US geopolitical tensions over 5G?

Theoretical Framework

Scholars have asserted that there are three clusters of research on the politics of cybersecurity. The third cluster focuses on securitisation, in which the thematic points are the actors and their practices and policies that construct specific issues as security threats.[6] Securitisation theory holds the most explanatory power

---

5 Timothy M. Bonds et al., *America's 5G Era: Gaining Competitive Advantages While Securing the Country and Its People,* report (Santa Monica: RAND Corporation, 2021), https://www.rand.org/pubs/perspectives/PEA435-1.html.

6 Myriam Dunn Cavelty and Andreas Wenger, *Cyber Security Politics: Socio-Technological Transformations and Political Fragmentation,* First Edition (London: Routledge, 2022).

considering the topic of this research.[7] Therefore, it will be helpful to analyse the securitisation discourse regarding Chinese telcos propagated by the US through the lens of securitisation theory. In this regard, the paper draws on work of the Copenhagen School, which has influenced academic understanding of securitisation and adapts it to the cybersecurity of telecommunication infrastructure.

The book *Security: A New Framework for Analysis* is widely regarded as a foundational text on the concept of securitisation.[8] It argues that securitising moves are essentially speech acts through which specific issues are framed as existential threats. For instance, in the case of US policymakers, framing of Chinese telecommunications companies as existential threats exemplifies such a securitising move. The process of securitisation is completed when the targetted audience - such as US allies - accepts this framing, legitimising extraordinary measures to address the perceived threat. Notably, Donald Trump vehemently criticised Chinese telcos and even boasted about convincing 'many' countries to abandon them because they posed a significant security threat.[9] The British government even admitted that geopolitical pressure from the US partly contributed to its decision to ban Chinese telcos.[10] The book also underscores how an

7 Clara Eroukhmanoff, "Securitisation Theory: An Introduction," *E-International Relations,* January 14, 2018, https://www.e-ir.info/2018/01/14/securitisation-theory-an-introduction/.

8 Barry Buzan, Ole Wæver and Jaap de Wilde, *Security: A New Framework for Analysis* (Boulder: Lynne Rienner Publishers, 1998).

9 Pia Victoria Freiin von Blomberg, "Cybersecurity in the European Union: The Securitization of Chinese 5G Providers," (Bachelor Thesis, Ludwig-Maximilians-Universität München, 2023), https://epub.ub.uni-muenchen.de/105955/.

10 Toby Helm, "Pressure from Trump Led to 5G Ban, Britain Tells Huawei," *Observer*, July 18, 2020, sec. Technology, https://www.theguardian.com/technology/2020/jul/18/pressure-from-trump-led-to-5g-ban-britain-tells-huawei.

external power (the US) leveraged references to threats to national security and intelligence sharing as a means to influence and align the decision-making of its allies with its own strategic priorities. This point was exemplified by former Secretary of Defense Mark Esper, who cautioned that any state adopting Chinese telecommunications companies risked jeopardising its relationship with the US.[11] Similarly, former Secretary of State Mike Pompeo issued veiled warnings, suggesting that states embracing Chinese telcos would do so at the expense of their diplomatic and military ties with the US.[12]

Methodology

A comprehensive literature search was conducted across multiple academic databases, including JSTOR, SpringerLink, and Taylor & Francis, using a combination of keywords and Boolean operators to refine the search. Keywords included 'Chinese telcos,' 'securitisation,' '5G development,' 'Western perspectives,' and 'Developing States.' Google Scholar was also used to identify relevant publications from 2019 to 2024. The rationale for focusing on this time frame stems from the Trump administration's initiation of the securitisation of Chinese telcos, highlighted by Trump's declaration of a national IT emergency in May 2019.

All identified publications were imported into Zotero, a reference management software, to facilitate organisation, track keyword

---

11 Claude Barfield, "The Munich Security Conference: Good News and Bad on US-China, Huawei, and 5G," *American Enterprise Institute,* February 20, 2020, https://www.aei.org/technology-and-innovation/the-munich-security-conference-good-news-and-bad-on-us-china-huawei-and-5g/.

12 Øystein Soknes Christie, Jo Jakobsen and Tor Georg Jakobsen, "The US Way or Huawei? An Analysis of the Positioning of Secondary States in the US-China Rivalry," *Journal of Chinese Political Science* 29, no. 1 (2024): 77-108, https://link.springer.com/article/10.1007/s11366-023-09858-y.

connections, and streamline citations. Titles and abstracts were screened against predefined inclusion criteria to ensure relevance to the research objectives, particularly with regard to Chinese telcos and securitisation. The primary sources included peer-reviewed journal articles, books, think tank reports, and dissertations. To include diverse perspectives, the review included publications from the European Union, Pakistan, and India. Full-text assessments ensured that each publication explicitly addressed one or more research questions. Key themes, such as securitisation narratives and geopolitical framing, were systematically extracted from the texts. The extracted data were analysed qualitatively to identify patterns, themes, and insights aligned with the research questions, providing a comprehensive understanding of the securitisation of Chinese telcos within varying geopolitical contexts.

National Security and 5G

According to Barry Buzan, there are five sectors of security, including the military and economy.[13] In the case of 5G, economic and military imperatives are driving its development, as 5G has the potential to revolutionise commercial industries and military-industrial complexes by leveraging its defining technical features: highest speed and bandwidth, lowest latency, and ultra-reliability.

Moreover, the military's demand for data is expected to grow with the integration of emerging technologies such as Artificial Intelligence (AI). 5G can not only meet this increasing demand but also enable critical advancements, including improved connectivity between sensors and shooters, powering algorithms to enhance battlefield transparency in complex information environments, improving intelligence, surveillance, and reconnaissance (ISR)

[13] Marianne Stone, "Security According to Buzan-A Comprehensive Security Analysis?," (paper, Security Discussion Papers Series 1, Sciences Po, Paris, 2009), https://docs.neu.edu.tr/staff/nur.koprulu/Security_for_Buzan.mp3_10.pdf.

capabilities, streamlining logistics, and supporting the development of more autonomous weapon systems.[14] Therefore, a state that achieves a first-mover advantage in 5G technology will strengthen not only its economic power but also its military power, amplifying its strategic position globally.

Cybersecurity and Technical Vulnerabilities of 5G

Beyond the military, 5G carries serious implications for national security, as critical sectors will increasingly depend on its networks. These sectors include the automated industries of the future, networks managing thousands of driverless cars, and hospitals where remote surgeries will rely on 5G's ultra-low latency.[15] Even a minor disruption in such systems could endanger countless lives. Given the transformative societal and industrial applications of 5G, the risks of sabotage are likely to increase exponentially. Achieving the lowest latency and fastest speeds necessitate placing software and servers at the network's edge, which creates additional vulnerabilities. These edge systems, while crucial for efficiency and performance, could become prime targets for malicious actors, amplifying the stakes for national and global security.[16] The former US Federal Communications Commission (FCC) Chairman Tom Wheeler highlighted these vulnerabilities by noting that 5G might be the last physical network overhaul in generations as only software updates would be needed afterwards. This would require the vendor

---

14 Kelley M. Sayler, *National Security Implications of Fifth Generation (5G) Mobile Technologies*, report (Washington, D.C.: Congressional Research Service, March 14, 2023), https://sgp.fas.org/crs/natsec/IF11251.pdf.

15 D. Loghin et al., "The Disruptions of 5G on Data-Driven Technologies and Applications," in *IEEE Transactions on Knowledge and Data Engineering* 32, no. 6 (2020): 1179-1198, https://ieeexplore.ieee.org/document/8961984.

16 Tom Wheeler, "5G in Five (Not so) Easy Pieces," *Brookings*, July 9, 2019, https://www.brookings.edu/articles/5g-in-five-not-so-easy-pieces/.

to have persistent access to the network, which could compromise its security if the vendor was unreliable.[17] Moreover, professionals at the FCC have observed that 5G networks will pave the way for the widespread adoption of the Internet of Things (IoT). The anticipated complexity of IoT networks, coupled with the sheer number of interconnected devices, significantly heightens concerns about cyber insecurity. These vulnerabilities could be exploited to disrupt critical systems, compromise sensitive data, and undermine trust in the digital infrastructure that underpins modern society.[18] Thus, the complexity of 5G technology and its network infrastructure has been used to justify the political securitisation of Chinese telecommunications companies. This securitisation hinges on fears of potential cyber espionage or large-scale network disruptions, which could exploit the vulnerabilities inherent in such a complex and critical system.[19]

Case Study: Salt Typhoon Cyberattack and Chinese Telcos

The securitisation of Chinese telcos gained traction in October 2024 following a high-profile cyberattack widely reported across the US.[20] Media outlets revealed that a group of Chinese hackers, later identified as 'Salt Typhoon,' had infiltrated a substantial

---

17 Iryna Bogdanova, "Politicisation of the 5G Rollout: Litigation Way for Huawei?" (paper, Social Science Research Network, February 2023), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4345025.

18 Shane Fonyi, "Overview of 5G Security and Vulnerabilities," *The Cyber Defense Review*, Spring (2020): 117-132, https://cyberdefensereview.army.mil/Portals/6/CDR%20V5N1%20-%2008_%20Fonyi_WEB.pdf.

19 Karsten Friis and Olav Lysne, "Huawei, 5G and Security: Technological Limitations and Political Responses," *Development and Change* 52, no. 5 (2021): 1045-1273, https://onlinelibrary.wiley.com/doi/10.1111/dech.12680.

20 Chris Jaikaran, *Salt Typhoon Hacks of Telecommunications Companies and Federal Response Implications,* report (Washington, D.C.: Congressional Research Service, November 15, 2024), https://crsreports.congress.gov/product/details?prodcode=IF1279.

portion of the US telecommunications network. The severity of the breach prompted Senator Mark Warner, Chair of the Senate Intelligence Committee, to describe it as the most significant telecom hack in US history, stating that it dwarfed previous cyberattacks against the country.[21] Subsequent confirmations by the Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) validated these reports, detailing how Salt Typhoon exploited vulnerabilities in telecom infrastructure, particularly through compromised switches and routers. Brandon Wales, former Executive Director of CISA, indicated out that major US telecom providers, including AT&T, Verizon, and Lumen, were affected, with vulnerable edge devices - specifically Cisco routers - identified as the primary intrusion vector.[22]

The incident underscored the risks associated with critical network infrastructure, intensifying calls for action against reliance on Chinese-manufactured telecommunications equipment. In response, the U.S. House of Representatives proposed legislation allocating over USD 3 billion to support telecom companies 'to rip and replace' Chinese-made equipment,[23] reflecting a policy shift driven by concerns over national security and cyber resilience.

China strongly refuted allegations linking the Salt Typhoon cyberattack accusing US officials of using cybersecurity as a

---

21 Ellen Nakashima, "Top Senator Calls Salt Typhoon 'Worst Telecom Hack in Our Nation's History,'" *Washington Post*, November, 21 2024, https://www.washingtonpost.com/national-security/2024/11/21/salt-typhoon-china-hack-telecom/.

22 Brandon Wales, Interview by Steven Rosenbush, *WSJ CIO Network,* October 7, 2024, https://cionetwork.wsj.com/video/cio-network-summit-7/8/.

23 David Shepardson, "US House to Vote to Provide $3 Billion to Remove Chinese Telecoms Equipment," *Reuters*, December 8, 2024, https://www.reuters.com/world/us/us-house-vote-provide-3-billion-remove-chinese-telecoms-equipment-2024-12-08/.

pretext to smear Beijing for geopolitical gain.[24] Chinese analysts argue that the forced removal of Chinese telecom equipment would significantly raise costs for US operators and degrade user experience. Zhang Xiaorong, Director of the Beijing-based Cutting-Edge Technology Research Institute, asserted that such isolationist actions by the US would also harm the global telecom industry.[25] Nevertheless, the scale and scope of the Salt Typhoon hack are likely to prompt policymakers to accelerate efforts to eliminate Chinese telecom presence entirely, both domestically and among allies. With the incident occurring just weeks before the inauguration of Trump's second presidency, the incoming administration is expected to aggressively relaunch its international securitisation campaign against Chinese telcos.

Contentious Geopolitics of 5G and Sino-US Tensions

Numerous studies have analysed the interlinkage between emerging technologies and geopolitical risk. This linkage underscores why contentious geopolitics have impeded global 5G deployment.[26] The impediment is partly explained by Deloitte's assessment, highlighting that the state leading in 5G development

24 Lewis Wiseman "Terrifying Chinese Hacking Campaign Sees Large Numbers of Americans' Data Stolen, US Officials Say," *ABC News*, December 5, 2024, https://www.abc.net.au/news/2024-12-05/united-states-allege-china-behind-salt-typhoon-telecoms-hack/104687712.

25 "US' Forcible Removal of Chinese Telecom Equipment Only Increases Cost, Harms User Experience: Analyst," *Global Times*, December 8, 2024, https://www.globaltimes.cn/page/202412/1324601.shtml.

26 Khalid Khan et al., "Geopolitics of Technology: A New Battleground?", *Technological and Economic Development of Economy* 28, no. 2 (2022): 442-62, https://journals.vilniustech.lt/index.php/TEDE/article/view/16028.

could attain a competitive advantage for many years.[27] Such assessments underline why the debate over 5G is frequently viewed through the lens of zero-sum geopolitical competition between the US and China. Notably, according to Nigel Inkster, the domination of 5G has become a key battleground in the broader geopolitical Sino-US contestation. Moreover, he has posited that China's lead in the global 5G market represents another 'Sputnik moment' - challenging long-held presumptions of US supremacy in telecommunications.[28]

Successive US administrations have thus initiated a domestic crackdown on Chinese telcos by enacting laws to prevent the transfer and sales of telecom equipment to Chinese telcos.[29]

On the international front, the US capitalised on concerns that resonated with Western audiences, particularly those related to data privacy, to garner opposition to Chinese telcos. Senior US officials have been warning and applying diplomatic pressure on other states to restrict market access for Chinese telcos. In fact, countering the latter's global digital expansion became one of the rare issues that has had bipartisan consensus in the US. To operationalise this strategy, the U.S. State Department launched the 'Clean Network' initiative in August 2020, aimed at addressing 'long-term threats to data security from malign authoritarian actors.' [30] It focused on forging joint declarations on 5G security with countries

---

27 Dan Littmann et al., *The Imperative for US Leadership on the 5G Deployment*, report (New York: Deloitte, 2018), https://www2.deloitte.com/us/en/pages/consulting/articles/5G-deployment-for-us.html.

28 Nigel Inkster, *The Great Decoupling China, America and the Struggle for Technological Supremacy* (London: Hurst Publishers, 2020), 156.

29 Qingxiu Bu, "Behind the Huawei Sanction: National Security, Ideological Prejudices or Something Else?" *International Cybersecurity Law Review* 5 (2024): 263-300, https://link.springer.com/article/10.1365/s43439-024-00112-6.

30 Christie et al., "The US Way or Huawei?," 80.

across Central and Eastern Europe. Subsequently, in May 2021, Congress proposed the Transatlantic Telecommunications Act (TTA) to fund development and protection of 5G infrastructure in Eastern Europe.[31]

The TTA was similar to the agreements China had signed with Belt and Road Initiative (BRI) states, which guaranteed market access for Chinese telcos. However, explicit binaries in the language of such agreements (democratic vs. authoritarian) contributed to a gradual securitisation of 5G across Europe as European security and technical experts started echoing US concerns regarding the risks posed by Chinese telcos. For instance, this led to the European Parliament referencing the Prague Proposals (2019), a report that assessed the cybersecurity risks associated with 5G deployment. The proposals outlined principles for states to follow, including implicit recommendations to limit cooperation with China on 5G infrastructure.[32]

China's Pursuit of Leading the 5G Race

Even before US attempts at choking technology access to Chinese telcos and urging allies to ban them, China had long been cognizant of the geopolitical imperative of leading the 5G race. Since 2016, Chinese officials have argued that innovation in emerging and established industries will be spurred by 5G.[33] Chinese development strategies also highlight progress in 5G and associated sectors to promote long-term growth, further

31 Bogdanova, "Politicisation of the 5G Rollout."
32 Friis and Lysne, "Huawei, 5G and Security," 1186.
33 Elisa G. Prestes, "The Digital Geopolitics of 5G: Elements to Understand the Chinese Technological Development of the Fifth Generation of Mobile Telephony," *Geousp* 26, no. 2 (2022), e-194823, https://www.scielo.br/j/geo/a/dRW7hLXpQzRKS3WfZYTgLrq/.

underscoring its significance.[34] For instance, China considers 5G crucial for achieving the goals envisioned in its 'Made in China 2025' plan. Moreover, China's 5G market is expected to contribute nearly USD 260 billion to the Chinese economy in the coming years.[35]

On the international front, China first officially unveiled the 'Digital Silk Road' (DSR) in 2015 in a government white paper. 5G was stated to be the foundation of the DSR for emerging technologies such as AI and IoT.[36] China's then-Foreign Minister, Wang Yi, outlined that the DSR would be a key priority for advancing 5G cooperation under the BRI. As part of this strategy, China views establishing itself as a standards-setter in 5G as a core foreign policy objective of the DSR.[37] To this end, Beijing has leveraged its leadership in 5G development to shape international technical standards. By 2019, China had signed over 85 cooperation agreements on technical standardisation, involving nearly 50 BRI-participating countries.[38] These agreements are expected to advance China's aspiration to become the world leader in setting

---

34 Hannah Reilly, "Connection and Competition: Navigating the U.S.-China Race to 5G," (CMC Senior Theses, Claremont Graduate University, 2021), https://scholarship.claremont.edu/cmc_theses/2910/.

35 "China's 5G Market Is Set to Add Almost $260 Billion."

36 John Hemmings, "Reconstructing Order: The Geopolitical Risks in China's Digital Silk Road," *Asia Policy* 15, no. 1 (2020): 5-22, https://www.jstor.org/stable/26891385.

37 He Yujia, "Chinese Digital Platform Companies' Expansion in the Belt and Road Countries," *The Information Society* 40, no. 2 (2024): 96-119, https://www.tandfonline.com/doi/abs/10.1080/01972243.2024.2317058.

38 Erik Baark, "China's Digital Silk Road: Innovation in a New Geopolitical Environment," *East Asian Policy* 16, no. 01 (2024).

international standards for next-generation telecom technologies as part of its 'Standards 2035' strategy.[39]

China has also accelerated efforts to develop and promote an alternative internet architecture. In 2019, Huawei introduced a New Internet Protocol (IP), which Western academics interpreted as a manifestation of China's geopolitical ambitions. This initiative is seen as part of a broader strategy to internationally advance an 'internet with Chinese characteristics,' focused on state-centric control and governance over digital infrastructure.[40]

Western Securitisation of Chinese Telcos

As discussed in the preceding section, China has established robust technological partnerships with states worldwide, primarily through the DSR. However, an analysis of the discourse surrounding China's digital cooperation reveals that dominant narratives often originate from Western think tanks. These perspectives, closely align with those of US policymakers, frequently portray China's digital initiatives as having ulterior motives, such as undermining democratic institutions, exporting digital authoritarianism, and engaging in data theft.[41] The most

---

39 Fakhar Hussain et al., "Infrastructure Development for the Digital Silk Road (DSR) and its Implications for China Under the Belt and Road Initiative," *Asia-Pacific Social Science Review* 23, no. 4 (2023), https://animorepository.dlsu.edu.ph/apssr/vol23/iss4/7/. The 'China Standards 2035' strategy builds upon the earlier 'Made in China 2025' plan, to establish China as a global standard-setter in emerging technologies, including 5G, by promoting technical standardisation and enhancing compatibility across industries.

40 Inkster, *The Great Decoupling*, 147.

41 Richard Heeks et al., "China's Digital Expansion in the Global South: Systematic Literature Review and Future Research Agenda," *The Information Society* 40, no. 2 (2024): 69-95, https://www.tandfonline.com/doi/full/10.1080/01972243.2024.2315875.

commonly referenced example in Western literature is the Chinese construction of smart cities with the latest surveillance technologies, like AI-enabled facial recognition. Leading Chinese firms such as Huawei and ZTE have been involved in more than 350 smart city projects globally. However, Western academics have deemed these projects the most extensive intelligence collection network ever built.[42]

Western publications also assert that increasing overseas expansion of Chinese telcos accompanies significant geopolitical implications as they continue to construct the backbone of ICT infrastructure in both developing and developed states. In this context, Western scholars have posited that China's objective of expanding digital cooperation with other states should be a major concern for the US and its Western allies since key players in China's telecom sector are state-backed telcos. They substantiate their argument by highlighting that China's state-backed banks, such as the Export-Import Bank of China (EXIM) and the China Development Bank (CDB), have provided tens of billions in financing China's overseas ICT projects.[43]

Furthermore, Western literature frequently frames China's digital cooperation as a form of 'data colonialism,' wherein China is perceived as exerting control over digital infrastructure, IT systems, and data flows in partner states.[44] Given the intrinsic link between data and states' economic and political power, the increasing digitisation of the global economy has emerged as a critical arena for geopolitical competition. In this context, much of the reviewed Western literature on the security of 5G networks references China's 2017 National Intelligence Law. This law is widely

42 Hemmings, "Reconstructing Order," 14.

43 Ibid., 7.

44 Lizhi Liu, "The Rise of Data Politics: Digital China and the World," *Studies in Comparative International Development* 56, no.1 (2021): 45-67, https://link.springer.com/article/10.1007/s12116-021-09319-8.

speculated to impose a legal obligation on Chinese companies, including telecom firms, to 'participate in assisting intelligence work,' regardless of their global operations.[45] This interpretation amplifies concerns about the security implications of Chinese digital infrastructure in a highly interconnected world.

Huawei: Focal Point of Sino-US 5G Tensions

While US policymakers view all Chinese telecommunications companies with suspicion, Huawei has been the primary focus, viewed through the lens of an increasingly fraught US-China relationship. A pivotal moment came with President Trump's Executive Order declaring a 'national IT emergency' targetting Huawei, which marked the beginning of the US securitisation of Chinese telcos. This executive order politicised telecom technology, transforming what was once a technical issue into a critical national security concern. By 2022, Huawei's founder openly acknowledged the challenging geopolitical environment and its profound implications for the company's international operations.[46] He conceded that Huawei would need to forgo business opportunities in countries with deep security alliances with the US, reflecting the geopolitical constraints imposed by the securitisation narrative.

Consequently, while Huawei was in a prime position to acquire contracts for deploying 5G in European states as it had been a key player in their 4G deployment, it encountered vociferous opposition from the US. For example, the UK was initially open to allowing Huawei equipment in the non-core components of its 5G networks. However, in July 2020, it banned Huawei over its inability to procure

45 Bu, "Behind the Huawei Sanction," 286.

46 Rohit Dube, "Huawei's Trajectory in India - Crippled by the Chinese Military," (paper, Research Gate, 2023), 1-7, https://www.researchgate.net/publication/368652430_Huawei"s_trajectory_in_India_-_crippled_by_the_Chinese_military.

secure components following US sanctions.[47] Huawei officials tried to alleviate Western states' concerns by opening information security labs to invite investigations of its 5G equipment and review source codes. However, such transparency initiatives were not enough to counteract the securitisation discourse propagated by the US.[48]

Geopolitics and Huawei's Diverging Trajectories in Pakistan and India

Studies have highlighted an overlap between the commercial interests of Chinese telcos and the digital development agendas set by host states.[49] For example, developing states like Pakistan have set ambitious digital aspirations, and Chinese telcos are invited to compensate for their technological, financial, and infrastructural shortcomings.[50] This is evident in how China established all-weather optical fibre and satellite communication channels in Pakistan. In the digital age, these communication channels have become what China calls the 'information highway' and form the basis for enhancing cooperation between Chinese telcos and Pakistan.[51] Huawei played an integral role in constructing and operating this information highway. Notably, it has invested USD 100 million to establish a regional headquarters in Islamabad. Moreover, it has built Pakistan's first Cloud Data

47 Jonathan Pelson, *Wireless Wars, China's Dangerous Domination of 5G and How We're Fighting Back* (London: Penguin Random House, 2021), 212.

48 Friis and Lysne, "Huawei, 5G and Security," 1182.

49 Yujia, "Chinese Digital Platform Companies' Expansion," 5.

50 Alivia A. Johnson, "Navigating Incentives of States' Engagement in Huawei Amidst Western Pressures," (Senior Thesis, California State University Maritime Academy, 2023), https://scholarworks.calstate.edu/downloads/6969z805j.

51 Xin Yue Shen, "Chinese ICT on the Digital Silk Road: A Case Study of Infrastructure Building in Pakistan," (Masters Thesis, Simon Fraser University, Burnaby, 2020), https://summit.sfu.ca/item/20723.

Centre and Safe City surveillance system.[52] Studies have also highlighted how Huawei Pakistan's cloud solutions have revamped the country's banking industry. The State Bank of Pakistan has even praised the Chinese telco for assisting banks in navigating the opportunities and challenges posed by the digital age.[53]

Meanwhile, across the border, Huawei incrementally expanded its presence in India over the past two decades. At one point, Huawei had the largest external Research and Development (R&D) presence in India. Moreover, similar to Europe, in 2018, Huawei was positioned to win 5G contracts in India as it was a leading equipment provider to major telecom operators.[54]

Until 2019, Huawei's trajectory in India mirrored its growing presence in Pakistan, reflecting China's broader regional ambitions. However, this trajectory sharply diverged in subsequent years due to shifting geopolitical dynamics. India became a key target audience for the US campaign to securitise Chinese telcos. Unlike other states, the US required little effort to convince India, as the deadly clashes between Chinese and Indian soldiers in the Galwan Valley in June 2020 significantly altered India's approach to Chinese tech firms.[55] In the aftermath of the incident, the Indian government implemented stringent measures against Chinese companies, including Huawei, as part of a broader clampdown on Chinese tech operations. This shift was not merely a reaction to the

---

52 Johnson, "Navigating Incentives of States' Engagement in Huawei," 23.

53 Hassan Nawaz et al., "Huawei Pakistan Providing Cloud Solutions for Banking Industry: A Data Driven Study," *The Asian Bulletin of Big Data Management* 4 (2024): 89-107, https://abbdm.com/index.php/Journal/article/view/122.

54 Manoj Kewalramani and Anirudh Kanisetti, "5G, Huawei & Geopolitics: An Indian Roadmap," (paper, Social Science Research Network, 2019), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3414860.

55 Dube, "Huawei's Trajectory in India," 5.

Galwan Valley clashes but also a reflection of India's recalibrated strategic alignment, influenced by growing tensions with China and closer ties with the US. Consequently, Huawei found itself ensnared in a complex geopolitical struggle, with its operations in India severely impacted by both domestic and international pressures.

Thus, Pakistan and India's engagements with Huawei are emblematic of the broader geopolitical tensions between China and the US over Chinese telcos in general and Huawei in particular. While Huawei's expanding presence in Pakistan reflects Islamabad's increasing technological alignment towards China, the company's shrinking footprint in India underscores the deepening Indo-US strategic partnership in which technological cooperation is a key pillar.[56]

Challenges of Banning Chinese Telcos for Developing States

The Atlantic Council has observed that while the US has effectively curtailed the expansion of Chinese telecom companies among its allies, its efforts have been less successful in other regions.[57] Geopolitical and alliance dynamics partly explain why US securitisation initiatives have been less impactful in many developing states. However, additional factors may account for why these states have resisted US pressures and chosen to contract Chinese telcos for the development of their telecom network.

One contributing factor is the disparity in US engagement. While the US has relied on long-standing strategic and intelligence partnerships to influence its Western allies, its interactions with

---

56 Mustafa Bilal, "Indo-US Strategic Tech Alliance: AI's Prospects and Perils," *Stratheia*, January 17, 2024, https://stratheia.com/indo-us-strategic-tech-alliance-ais-prospects-and-perils/.

57 Reilly, "Connection and Competition," 43.

developing countries have been relatively limited, reducing its capacity to shape their decisions.

Beyond strategic considerations, structural issues in the telecom sector also played a role. In 2021, Jeremy Fleming, then head of Britain's Government Communications Headquarters (GCHQ), acknowledged that Western nations had effectively 'lost the conversation' on 5G infrastructure a decade earlier. He attributed this to the withdrawal of Western telecom companies from investing in foundational infrastructure, which was often dismissed as unprofitable 'white elephant' projects. Fleming conceded that this neglect left Western states with limited alternatives, thereby enabling Chinese telcos to dominate the market in developing regions.[58]

Meanwhile, Chinese telcos capitalised on the vacuum and cultivated strong technological partnerships with developing states, as evidenced by the fact that Huawei has developed 70% of Africa's 4G networks.[59] Hence, according to the Institute for National Security Studies, the US cannot secure leadership in the global 5G race solely by curbing China's technological advancements.[60] A major challenge lies in the absence of a domestic competitor to Chinese telecommunications firms. In response, the US has focused on actively supporting European 5G companies to fill this gap. Toomas Hendrik Ilves, the former President of Estonia, underscored this issue during a 2021 NATO

58 Jonathan E. Hillman, *The Digital Silk Road, China's Quest to Wire the World and Win the Future* (New York: Harper Collins, 2021), 58.

59 Johnson, "Navigating Incentives of States' Engagement in Huawei," 11.

60 Łukasz Gołota, "The Role of 5G Technology in Superpower Rivalry between the United States and China: An Offensive Realist Approach," *Polish Political Science Yearbook* 52, no. 4 (2023): 173-190, https://czasopisma.marszalek.com.pl/images/pliki/ppsy/52/ppsy202396.pdf.

meeting, questioning the efficacy of the US strategy. He pointedly remarked that while the US has been vocal about the risks posed by Chinese telcos, it has yet to provide a viable alternative for states to adopt.[61]

To date, no viable alternative to Chinese telecom companies has emerged, particularly in the context of developing states. Conversely, the Chinese narrative of mutual benefit through South-South cooperation, underscoring co-development with local stakeholders, has resonated strongly with these nations. Developing states view China as a global leader in ICT technology capable of addressing their digital divide with the developed world. In this context, Chung has highlighted the pivotal role of China's engagement in the Global South in implementing national ICT strategies across various socioeconomic sectors. By providing high-quality, competitive services at costs approximately 30% lower than those of Western competitors,[62] China has greatly facilitated digital transformation of many developing nations, reinforcing its appeal as a partner in their technological advancement.

Thus, Hillman has argued that for most developing states, the financial advantages of opting for Chinese telecom companies outweigh concerns about information security, which are often considered secondary. These states prioritise importing digital technologies and technical expertise from China to develop their telecommunications networks in a more cost-effective manner, addressing critical digital infrastructure needs without significant capital outlays.[63] For example, despite Western states' outcry over allegations that Huawei had been transferring data from the African

61 Hillman, *The Digital Silk Road*, 85.
62 Chien-peng Chung, "China's Digital Silk Road," *East Asian Policy* 15, no. 2 (2023): 123-137.
63 Hillman, *The Digital Silk Road*, 85.

Union's headquarters to China for years, the African Union and Huawei subsequently expanded their digital partnership.[64]

Jonathan Pelson has similarly assessed the importance of Chinese Telcos for developing states, noting that the cost of refusing them is substantial. Replacing existing Chinese telecom equipment, he argues, would require billions of dollars, with additional costs incurred from the price premiums charged by Western 5G providers like Nokia and Ericsson compared to their Chinese counterparts.[65]

Banning market access to Chinese telcos poses challenges for developing states, particularly those like Pakistan. For such states, removing Chinese equipment, as the US and its allies have done, would be both financially prohibitive and logistically impractical.[66] Germany, for example, initially resisted an outright ban on Chinese telcos, arguing that it would hinder 5G deployment given the dominance of Chinese companies in 5G patents.[67] However, this year, Germany was compelled to take the economically costly step of phasing out Chinese telecom equipment.[68] Similarly, British

64 Salem Solomon, "After Allegations of Spying, African Union Renews Huawei Alliance," *Voice of America*, June 6, 2019, https://www.voanews.com/a/after-allegations-of-spying-african-union-renews-huawei-alliance/4947968.html.

65 Pelson, *Wireless Wars*, 214.

66 Stacie Hoffmann, Samantha Bradshaw and Emily Taylor, "Networks and Geopolitics: How Great Power Rivalries Infected 5G," *Oxford Information Labs*, August 5, 2022, https://oxil.uk/blog/geopolitics-of-5g/index.html.

67 Corina Lozovan, "The 5G Conundrum amid Geopolitics and Security in Europe," (paper, Research Centre of the Institute for Political Studies (CIEP) Institute for Political Studies, Lisbon, 2021), https://ciencia.ucp.pt/en/publications/the-5g-conundrum-amid-geopolitics-and-security-in-europe.

68 Christopher F. Schuetze, "Germany to Strip Huawei from Its 5G Networks," *New York Times*, July 11, 2024, https://www.nytimes.com/2024/07/11/business/huawei-germany-ban.html.

Telecom highlighted that replacing Chinese equipment would cost billions of pounds, yet the UK government pressed ahead with the decision, as noted earlier.[69] These cases underscore the tension between economic pragmatism and geopolitical imperatives, illustrating the difficult trade-offs states face when addressing security concerns in their digital infrastructure.

Way Forward

For the US and its like-minded allies in Europe, geopolitical and economic decisions are intertwined with national security. However, US allies face pressing concerns stemming from diplomatic pressure from the US. Relatedly, in response to the intensifying securitisation of 5G, the EU envisioned a technological sovereignty policy, and EU member states tried to navigate the Sino-US confrontation over 5G diplomatically. Still, most states could not stay neutral and eventually either banned or restricted market access to Chinese telcos. For example, as discussed earlier, European states like France and Germany, who once championed technological sovereignty, could not hold out against pressure from the US to ban Chinese telcos.

Therefore, the contentious geopolitics of 5G has created the challenge of balancing autonomy ambitions with global technological interdependencies. Analysts suggest that developing states like Pakistan are likely to continue relying on Chinese telecom companies to build 5G infrastructure.[70] However, digital infrastructure can be categorised into military, government, and private sector domains, each requiring varying levels of access for

69 Pelson, *Wireless Wars*, 210.

70 CASS, "Air and Space Technologies: Harnessing the Innovation Economy", seminar organised by Centre for Aerospace & Security Studies, Islamabad, September 24, 2024, https://casstt.com/air-and-space-technologies-harnessing-the-innovation-economy/.

foreign firms.[71] This approach could help mitigate security risks while leveraging external expertise.

Building 5G infrastructure, however, presents several challenges. Using multiple vendors may lead to interoperability issues, while environmental factors can further complicate deployment. Technologies like Network Function Virtualisation (NFV), which allows network operators to virtualise various functions, could expand the threat surface, particularly when integrated with open radio access networks (Open RAN). Reliance on foreign cloud vendors also raises concerns about sensitive communications and data security. To address these challenges, Pakistan should evaluate vendor proposals with a security-first perspective, ensuring that long-term national interests are prioritised.[72] Ultimately, developing indigenous capacity for critical digital infrastructure should remain a strategic objective to reduce dependence on foreign technologies and enhance security.[73]

Conclusion

A state's leadership in 5G development is pivotal, as it not only drives economic growth but also enhances national security by enabling dominance in emerging civil and military industries. The

71 Fahad Nabeel (Research Lead, Geopolitical Insights), in discussion with the author, December 9, 2024.

72 Ibid.

73 CASS, "Air and Space Technologies: Harnessing the Innovation Economy", seminar organised by Centre for Aerospace & Security Studies, Islamabad, September 24, 2024, https://casstt.com/air-and-space-technologies-harnessing-the-innovation-economy/; CASS, "Cyberspace as a Global Common: Formulation and Applicability of International Law", roundtable organised by Centre for Aerospace & Security Studies, Islamabad, July 8, 2024, https://casstt.com/cyberspace-as-a-global-common-formulation-and-applicability-of-international-law/.

strategic importance of 5G lies in its transformative economic and military implications, coupled with its potential to introduce unforeseen risks to national security. As such, the controversy surrounding 5G deployment is best understood through a geopolitical lens, where power dynamics significantly shape and are shaped by the evolution of this critical technology.

The development of 5G equipment, standards, and software has become a focal point in the broader geopolitical rivalry, particularly between China and the US. This struggle represents the opening phase of a protracted competition over emerging technologies that will be built on the backbone of 5G infrastructure. For states seeking to preserve strategic autonomy, this rivalry presents a diplomatic challenge, forcing them to navigate a delicate balance between aligning with Chinese or Western telecommunications providers. As Sino-US tensions over 5G escalate, the decisions states make regarding their 5G partnerships will have far-reaching implications, potentially reshaping their broader geopolitical alignments and future relations with both powers. This underscores the centrality of 5G not just as a technological race but as a key determinant of global power structures in the years to come.

Mustafa Bilal has done his BS in International Relations from the National Defence University (NDU), Pakistan. His research interests include technopolitics, astropolitics, military aviation and warfare. He can be contacted at: mustafabilal27924@gmail.com