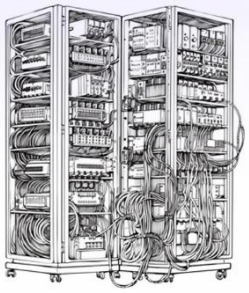
CASS

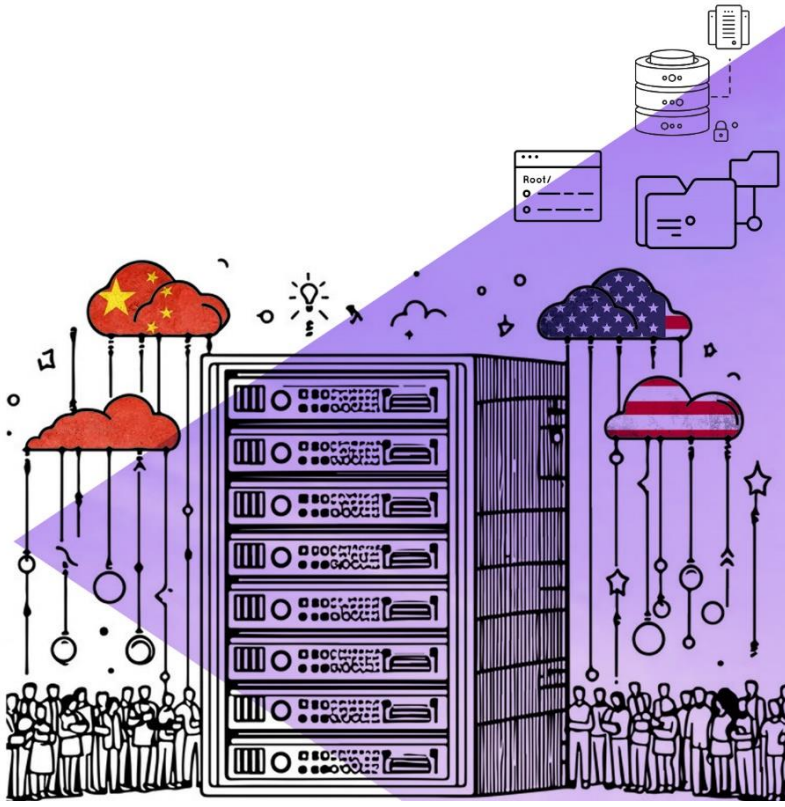
CENTRE for AEROSPACE & SECURITY STUDIES



Virtual Curtain: Geopolitics of Data Centres and US-China Competition

Shaheer Ahmad

Research Assistant



Working Paper

President
Air Marshal Javaid Ahmed (Retd)

Edited by:
Sarah Siddiq Aneel

Layout
Hira Mumtaz

All correspondence pertaining to this publication should be addressed to CASS, Islamabad, through post or email at the following address:

Centre for Aerospace & Security Studies

+92 51 5405011
cass.thinkers@casstt.com
cass.thinkers
cassthinkers
@CassThinkers
Centre for Aerospace & Security Studies

CENTRE for AEROSPACE & SECURITY STUDIES

Virtual Curtain: Geopolitics of Data Centres and US-China Competition

Working Paper

Shaheer Ahmad

Research Assistant

TABLE OF CONTENTS

Abstract **1**

Introduction **2**

Theoretical Framework **3**

Data Centres: Evolution and Significance **5**

Great Power Competition in Data Centres **6**

United States of America 7

People's Republic of China 11

Geopolitical Implications **16**

Data Sovereignty and Digital Colonialism 16

Geopolitical Complications 16

Threat of Escalation over Data Infrastructure 16

Challenges **17**

Cyber-Attacks and Digital Espionage 17

Role of Small and Middle Powers 17

Supply Chain Vulnerabilities 18

Data Bifurcation 18

Erosion of State Control 18

Environmental Cost 19

Energy and Water Usage 19

Recommendations **20**

Build and Diversify Data Infrastructure 20

Encourage Innovation 20

Prioritise International Cooperation 21

Development of Domestic Legislation 21

Conclusion **21**

Abstract

To date, the discourse on techno-politics has largely centred on semiconductor fabrication plants in Taiwan, lithographic innovations of the Netherlands, and critical mineral reserves, such as cobalt and lithium, across Africa. However, the next phase of this geopolitical contest is increasingly being shaped by the importance of data centres: the digital fortresses that power the computational demands of Artificial Intelligence and Machine Learning. With data emerging as the new currency of power, geopolitics of data infrastructure is set to shape the contours of global influence with the United States and China, both vying to lead the next technological revolution. This paper explores the growing significance of data centres, the strategic motivations of major powers, and geocentric challenges that accompany this competition. It argues that, much like earlier industrial revolutions, control over data infrastructure will be a decisive factor in determining geopolitical dominance in the coming age of advanced technologies.

Keywords: Technopolitics, Tech War, Data Sovereignty, 4IR, Digital Colonialism

Introduction

Technological advancements have always been key in the rise and fall of great powers. Beginning in the 16th Century, development of technologies such as the steam engine and telegraph marked a transformative period that positioned Great Britain at the forefront of global influence. Several centuries later, emergence of Silicon Valley in the 21st Century signified a comparable technological shift, establishing the United States (US) as a leading centre of digital innovation and a driving force in the contemporary technological era. The generational leap in Artificial Intelligence (AI), quantum computing, Big Data, and the Internet of Things (IoT) has shifted the axis of geopolitical discourse from traditional concerns of territorial acquisition and resource control to the pursuit of technological supremacy and dominance over advanced innovation ecosystems.

Within this evolving landscape, the next frontier of contestation is poised to focus on the infrastructure underpinning these emerging technologies: data centres. These facilities, which store, process, and distribute vast volumes of digital information, are becoming critical nodes in the macro struggle for technological and strategic advantage. Owing to their growing significance, both the US and China are engaged in an intense competition to build and control data centres across the globe. These facilities have become indispensable to national digital infrastructure, with rough estimates placing their current annual economic output at approximately USD 5.5 trillion - a figure projected to rise to USD 6.3 trillion in the near future.[1] This underscores the pivotal role data centres will play in securing not only technological primacy but also geopolitical influence in the decades ahead.

Given the central role of data in shaping the future of global technology, the race to control data centres is poised to surpass the intensity of competition over space and undersea infrastructure. This contest is increasingly expanding into the broader data centre supply chain, stretching from the strategic maritime hub of Singapore, often likened to a modern-day Venice, to the remote reaches of the Arctic. Dominance over data centres translates into control over the digital commons, enabling states to reap substantial economic gains while also leveraging data as a strategic asset for military and security purposes. Furthermore, such control offers governments greater authority over their domestic digital environments, which are increasingly being challenged by the rapid proliferation of disruptive technologies.

While much of the current techno-political discourse[2] has centred on semiconductors, the enduring logic of geopolitics remains rooted in the nexus between geography and

---

1 Andy Power, "Quantifying the Value of Data Centres: Report Key Takeaways," *Digital Reality,* Accessed December 15, 2024, https://www.digitalrealty.be/resources/articles/qualifying-the-the-value-of-data-centres.

2 Dieter Ernst, "Supply Chain Regulation in the Service of Geopolitics: What's Happening in Semiconductors?" (CIGI Papers no. 256, Centre for International Governance Innovation, Waterloo, 2021), https://www.econstor.eu/handle/10419/299728.

power. In this context, understanding where data centres are located, and which states possess the capital, infrastructure, and regulatory capacity to host them, is essential. A deeper examination of their spatial distribution and strategic significance[3] can enrich contemporary debates that have thus far focused predominantly on semiconductors, 5G,[4] and AI, offering a more holistic view of techno-politics.

This paper adopts a novel approach by exploring a relatively underexamined dimension of techno-politics: the geopolitics of data centres. It situates this inquiry within the broader context of intensifying strategic competition, particularly between the US and China, where the race to control data infrastructure has become increasingly pronounced. The central argument posits that data centres represent the next frontier of great power competition and states that successfully build, host, and secure advanced data centres will gain substantial technological and geopolitical advantage.

The study is structured into three sections. The first employs the theoretical lens of offensive realism to conceptualise the geopolitical significance of data centres. The second presents comparative case studies of the US and China, analysing their respective strategies in developing and controlling data infrastructure. The final section addresses the key infrastructural, geopolitical, and environmental challenges associated with the global expansion of data centres, offering insights into the implications for international security and digital governance.

Theoretical Framework

Given the importance of data centres in shaping the contemporary global order, this study employs John J. Mearsheimer's theory of *Offensive Realism* to analyse the dynamics of data centre geopolitics. Offensive Realism, which posits that great powers are inherently driven to maximise their relative power under conditions of anarchy, provides a compelling framework for understanding why states compete to dominate critical digital infrastructure. Through this lens, the pursuit of control over data centres is not merely a function of technological advancement, but a calculated strategy to secure long-term geopolitical leverage in an increasingly data-driven world.

According to Mearsheimer, in the absence of a supranational authority capable of regulating state behaviour,[5] the international arena becomes a self-help system where the security of one state often comes at the expense of another, producing a persistent security dilemma. Under such conditions, great powers not only seek to accumulate capabilities but also maintain offensive military potential to counter peer competitors,

3 Michael A. Peter, "Semiconductors, Geopolitics and Technological Rivalry: The US CHIPS & Science Act, 2022," *Educational Philosophy and Theory* 55, no. 14 (2023): 1642-1646.

4 Mustafa Bilal, "5G Geopolitics: Securitisation, Sino-US Competition and Technological Dependence for Developing States," *Journal of Aerospace & Security Studies* 3 (2024): 97-121.

5 John J. Mearsheimer, *The Tragedy of Great Power Politics* (New York: W.W. Norton, 2001), 30.

particularly in moments of heightened tension or conflict. This drive is not impulsive but strategic: Offensive Realism posits that states are rational actors, guided by the logic of long-term self-interest and survival. Consequently, their pursuit of dominance, whether territorial, technological, or economic, is rooted in structural imperatives shaped by the anarchic nature of the international system.[6]

In the contemporary era, power maximisation increasingly involves development of state-of-the-art technologies to maintain an edge over adversaries. While military strength remains central to realist thinking, the rise of AI, quantum computing, IoT, and 3D manufacturing has placed technology at the core of great power competition. These capabilities are vital for enhancing national security and asserting influence. However, their effective deployment depends on modern physical infrastructure. In this context, data centres have emerged as critical geopolitical assets enabling and sustaining technological operations.

Jared Cohen notes that future conceptions of geography and power will be shaped by control over data infrastructure.[7] Through initiatives like Stargate, the US aims to consolidate data centres on its mainland to reinforce its role in the global tech ecosystem. Currently, it hosts approximately 51% of the world's data infrastructure,[8] with presence in regions such as Southeast Asia and the Arctic. This not only provides a significant technological advantage over rivals but also enables deployment of advanced technologies critical for enhancing military and strategic capabilities. China has also ramped up its investments in developing data infrastructure to compete with the US in this realm. Through the nexus of state-owned enterprises, it is making strides in developing advanced data centres and computing capabilities. With companies like Huawei and AliBaba, China is operating a high-performance cluster of data centres on its mainland and abroad.

Dominance in data centres will allow great powers to launch technological offensives, securing data supremacy and limiting access for smaller states. As technology becomes central to geopolitics, data centres are likely to fuel a 'techno-security dilemma' driving a competitive race in digital infrastructure. These dynamics reflect an increasingly anarchic techno-political realm where states are compelled to maximise power through control of data centres.

---

6 Mearsheimer, *The Tragedy of Great Power Politics.*

7 Jared Cohen, "The Next AI Debate is About Geopolitics," *Foreign Policy,* October 28, 2024, https://foreignpolicy.com/2024/10/28/ai-geopolitics-data-center-buildout-infrastructure/.

8 "Leading Countries by Number of Data Centres as of March 2024," *Statista,* March 2024, https://www.statista.com/statistics/1228433/data-centres-worldwide-by-country/.

Data Centres: Evolution and Significance

Historically, data centres have transformed from basic computational facilities into critical nodes of global power. Evolving from mainframe systems to fibre-optic networks, they now underpin the global technological revolution. The 21st Century marked a huge shift with the rise of cloud computing, driven by Big Data and AI, which rendered traditional IT infrastructure increasingly obsolete.

In 2006, industry leaders like Google and Amazon Web Services (AWS) pioneered hyperscale data centres, characterised by vast storage capacities, advanced cooling systems, and reliable infrastructure. By 2015, proliferation of AI and emerging technologies led to development of AI-driven data centres, where ML systems managed data operations and optimised energy and cooling efficiency.

The expansion of edge computing in 2020 further integrated the IoT and 5G, enabling real-time processing and decentralised data handling. Most recently, by 2023, incorporation of sustainable energy sources, particularly small modular nuclear reactors and advanced smart grids, became a defining feature, powering next-generation data centres with greater resilience and efficiency.

Amid rapid technological advancements, the future points toward the emergence of quantum data centres and autonomous data ecosystems. These centres will dramatically enhance data processing capabilities, far surpassing current limitations, while autonomous ecosystems, powered by AI and renewable energy, are poised to evolve into self-sustaining infrastructures with virtually limitless scalability. By harnessing the principles of quantum mechanics, these centres will be capable of solving complex equations, supporting industrial automation, and driving innovation in sectors such as defence. As noted by Ilana Wisby, quantum data centres differ fundamentally from conventional models by enabling breakthroughs in renewable energy and contributing to climate change mitigation through optimised energy generation and usage.[9]

In this backdrop, countries hosting these data centres will gain political, economic, and military leverage over the peer ecosystem. However, establishing quantum data centres requires a strong industrial baseline, massive finances, and a formidable supply chain of rare earth minerals such as gallium and germanium.

To build on the historical evolution of data centres, from mainframes to AI- and quantum-powered systems, it is essential to understand their growing significance. As the information revolution accelerates, control over data has become a foundational element of technological supremacy. This shift is increasingly evident in the official strategies of major powers. The US military doctrine underscores the centrality of data

[9] "Bringing Quantum Computing to Data Centers," *McKinsey Digital,* December 20, 2023, https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/tech-forward/bringing-quantum-computing-to-data-centers.

in future warfare,[10] while China's 'National Defence in the New Era' reflects its transition toward 'intelligent wars,'[11] where AI, Big Data, and quantum computing play a pivotal role in national defence.

In this new era, data centres are no longer mere repositories: they are strategic assets. Nuclear-powered data centres, in particular, represent the frontier of this competition, offering not only energy resilience but also technological sovereignty in an increasingly interdependent world.[12] Moreover, integration of AI and quantum systems into these infrastructures is redefining decision-making processes across sectors, shifting from conventional command structures to real-time, data-driven models. This transformation is reshaping national security frameworks, financial markets, industrial operations, and sustainability efforts.

As Laura DeNardis notes, internet infrastructure has become a proxy for controlling information flows.[13] In this context, countries with active investments in advanced data infrastructure are better positioned to meet the demands of emerging technologies. In an increasingly 'datafied' global order, geopolitical dominance will hinge on a state's ability to secure, manage, and regulate its digital backbone. Consequently, states are being compelled to recalibrate their priorities, ensuring that data centres form the core of their national power projection in a complex, multipolar world.

Great Power Competition in Data Centres

As data emerges as the 'new oil' of the 21st Century, the US and China are redirecting substantial resources towards the establishment and expansion of data centre infrastructure. While conventional military capabilities, such as frigates, submarines, fighter jets, and hypersonic weapons, remain essential, both powers increasingly understand that technological supremacy hinges not only on hardware but also on control over data. Failure to secure this domain risks vulnerability, with far-reaching consequences for political leverage, economic competitiveness, and military efficacy.

This section critically examines the respective strategies and initiatives undertaken by the US and China to assert dominance in the global data infrastructure race.

---

10 Office of the Chief Information Officer, *Army Data Plan,* report (U.S. Department of Defense, 2022), https://www.army.mil/e2/downloads/rv7/about/2022_army_data_plan.pdf.

11 State Council Information Office of the People's Republic of China, *China's National Defense in the New Era*, report (Beijing: Foreign Languages Press, First Edition, July 2019), https://www.chinadaily.com.cn/specials/whitepaperonnationaldefenseinnewera.pdf.

12 Bill Kleyman, "Welcome to the Era of the Nuclear-Powered Data Centre," *Data Centre Knowledge,* May 8, 2024, https://www.datacentreknowledge.com/next-gen-data-centres/welcome-to-the-era-of-the-nuclear-powered-data-centre.

13 Laura Denardis, *The Global War for Internet Governance* (New Haven and London: Yale University Press, 2014), 9.

United States of America

Technological Dominance

The US has historically led in the development and integration of general-purpose technologies, from the Industrial Revolution to the post-Cold War era. With greater focus on leadership in innovation and control over secure supply chains, data centres have become central to US policy planning, aimed at preserving its technological edge. These shifts represent 'novel dimensions of power,' where control over subsea, undersea, and data infrastructure is critical.[14]

So far, the US maintains a commanding position in cloud computing. With leading cloud giants such as AWS, Microsoft Azure, and Google, it accounts for 66% of the cloud market where these giants have market share of 31%, 24%, and 11%, respectively. According to Statista estimates, global cloud infrastructure spending has surged to USD 84 billion, marking a 15% increase from the previous year, where these 'big three' dominate.[15] The rest of the actors including Alibaba, IBM, and Oracle cloud services account for single-digit percentages.

The US also maintains a commanding lead in the global data centre sector, hosting 5,381 facilities, accounting for approximately 51.6% of the world's total data infrastructure.[16] Despite China's growing ambitions in the digital domain, disparities remain in the scale of investment between the two powers, particularly in the AI-cloud-data centre nexus. In 2023, US tech giants invested approximately USD 45 billion in AI-related infrastructure, compared to just USD ten billion by Chinese firms.[17] This investment gap reflects not only a resource imbalance but also reinforces the US's lead in global data infrastructure.

US Data Centres in Southeast Asia

The US is taking transformative steps to maintain its technological ascendency by building data infrastructure across the world. Southeast Asia has become one of the central grounds for data centre competition. In Southeast Asia, Microsoft Azure and AWS hold nearly 60% of the market share when it comes to providing cloud

14 Zbigniew Brzezinski, *The Grand Chessboard: American Primacy and its Geostrategic Imperatives* (New York: Basic Books, 1998), 1.

15 Felix Richter, "Amazon Maintains Cloud Lead as Microsoft Edges Closer," *Statista,* November 1, 2024, https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers/.

16 "Leading Countries by Number of Data Centres as of March 2024."

17 Tsubasa Suruga and Akito Tanaka, "Southeast Asia's Digital Battle: Chinese and U.S. Big Tech Face Off over $1tn Market," *Nikkei Asia,* November 15, 2023, https://asia.nikkei.com/Spotlight/The-Big-Story/Southeast-Asia-s-digital-battle-Chinese-and-U.S.-Big-Tech-face-off-over-1tn-market.

infrastructure services.[18] Countries such as Singapore and Indonesia dominate the data centre market in Southeast Asia. Singapore, in particular, serves as a key maritime entrepôt and is deeply embedded in worldwide fibre-optic networks, including major undersea cable systems. Its position is further strengthened by multiple digital cooperation agreements with leading global powers, solidifying its role as a regional hub for digital infrastructure. In 2023, Singapore issued a national tender to expand its data centre infrastructure.[19] The bidding process attracted major US tech firms alongside Singapore's own Singapore Telecommunications, as well as Chinese contenders. Ultimately, the contracts were awarded to two US companies, Microsoft and Equinix, and two Chinese entities: ByteDance-led Consortium and GDS Holdings.[20] While Chinese firms competed primarily on pricing, they were unable to match the US companies in terms of overall quality and cost-effectiveness, reaffirming the competitive edge of American tech giants in this domain.

On the other hand, Indonesia has also emerged as a key regional player for data centres-realpolitik between the US and China. Following Alibaba's entry into Indonesia's cloud market, Google followed suit by creating a cobweb of data centres across the country. In 2021, AWS entered the market with a commitment to investing USD 5 billion for building new data centres over the next fifteen years.[21] Furthermore, Microsoft constructed its first data centre in West Java, the most densely populated province of Indonesia.[22] These developments not only reflect the deepening footprint of US tech firms in Southeast Asia.[23]

Under the broader push to expand US data centre presence in Southeast Asia, 2023 marked a shift as emerging regional players - Vietnam, Malaysia, and Thailand - entered the digital infrastructure race with comparative advantages in land availability and energy resources. In a significant move, these three countries formed a regional nexus, committing USD 8.46 billion to establish a comprehensive data infrastructure network in Thailand.

---

18 Felix Richter, "Amazon and Microsoft Stay Ahead in Global Cloud Market," *Statista,* February 27, 2025, https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers/.

19 IMDA, "Four Data Centre Proposals selected as Part of Pilot Data Centre Call for Application," July 14, 2023, https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/press-releases/2023/four-data-centre-proposals-selected-as-part-of-pilot-data-centre-call-for-application.

20 Alex Capri, *The Geopolitics of Modern Data Centers,* report (Hinrich Foundation, 2024), https://shorturl.at/knM4p.

21 Leon Spencer, "AWS Launches Indonesia Cloud Region, Pledges $5B Investment," *Channel Asia,* December 14, 2021, https://www.channelasia.tech/article/1266775/aws-launches-indonesia-cloud-region-pledges-5b-investment.html.

22 Jakarta Post, "Indonesia to house Southeast Asia's second Microsoft data hub," February 26, 2021, https://www.thejakartapost.com/news/2021/02/26/microsoft-to-establish-first-data-center-region-in-indonesia.html.

23 Febis, "The Race to Build Data Centres in Southeast Asia," May 24, 2024, https://www.febis.org/2024/05/24/the-race-to-build-data-centres-in-southeast-asia/.

Collaborating with major US cloud providers such as AWS and Microsoft Azure, Malaysia has also committed to developing new data centre facilities to enhance its digital infrastructure. Meanwhile, Vietnam is also emerging as a key player, with Google announcing plans to establish a hyperscale data centre there.[24] These developments underscore the growing role of Southeast Asia in the US-led expansion of global data infrastructure, as regional states position themselves as critical nodes in the evolving digital geopolitical order.

US Data Centres in the Polar North

The Polar North has recently gained attention in the geopolitical lexicon due to its changing climactic conditions. The abundance of renewable energy resources notably wind and hydropower, natural cooling, infrastructural space, and political stability provides an attractive avenue for establishing data centres there. In 2009, Google launched an ambitious project to convert an abandoned paper mill in Hamina, Finland, into an environmentally sustainable data centre.[25] Located along the Gulf of Finland, the facility repurposed an existing 450-metre tunnel to draw in seawater for server cooling. This innovative method reduces the electricity typically required for conventional cooling systems, demonstrating Google's commitment to energy-efficient and sustainable data infrastructure. In 2019, Google invested an additional USD 670 million demonstrating how innovative technologies and ecological considerations can be included to optimise the operation of data centres.[26]

Likewise, a US-Norwegian startup 'Kolos' is planning to build the world's largest data centre in Ballangen, Norway. The data centre is expected to initially require 70 megawatts of power, with plans to scale up to 1,000 megawatts within the next ten years, surpassing Amazon's data centre in Virginia.[27] According to the CEO Havard Lillebo, the data centre will be powered by renewable energy sources including proximate hydrocarbon dams and wind farms. The construction is planned to be developed over several years, with the site being completely built out in the next 11 years.[28]

Currently, there are no direct subsea cables connecting the Arctic with the US. Therefore, the US plans to direct investments to the region due to its conducive

---

24 Vietnam Investment Review, "More Investments planned for Vietnam's Hyperscale Data Centres," September 30, 2024, https://vir.com.vn/more-investments-planned-for-vietnams-hyperscale-data-centres-115056.html.

25 Cade Metz, "Google Reincarnates Dead Paper Mill as Data Center of Future," *Wired,* January 26, 2012, https://www.wired.com/2012/01/google-finland/.

26 Leo Laikola and Natalia Drozdiak "Google Invests $670 Million to Expand its Data Centre in Finland", *Bloomberg,* May 27, 2019, https://www.bloomberg.com/news/articles/2019-05-27/google-invests-670-million-to-expand-its-data-centre-in-finland.

27 Leo Kileon, "Record-sized Data Centre Planned Inside Arctic Circle," *BBC,* August 14, 2017, https://www.bbc.com/news/technology-40922048.

28 Callum Rivett, "Kolos to Build World's Largest Data Centre in Arctic Circle, *Technology Magazine,* May 17, 2020, https://technologymagazine.com/cloud-and-cybersecurity/kolos-build-worlds-largest-data-centre-arctic-circle.

landscape for setting up larger data centres. In this regard, Alaska presents a pressing opportunity for the US to establish a data centre ecosystem due to ample water reservoirs and renewable energy sources. Although the harsh environment poses a mounting challenge to such an initiative, it can be overcome by connecting the secluded frontier with the rest of the world.

Data Centres under the U.S. Department of Defense

The U.S. Department of Defense (DoD) recognises data as a 'strategic asset.'[29] Currently, it operates a wide array of data centres to fulfil its needs and objectives. According to Dave Powner, Director of IT Management at the Government Accountability Office (GAO), the number of data centres owned by the DoD is around 3065. The U.S. Air Force (USAF) is the leading entity in tri-services which holds around 1400 data centres followed by the Army's 1200 and 300 and 450 Navy and other defence agencies, respectively. The U.S. Army is poised to become more data-centric to prevail in future military operations. In this regard, the Army has outlined a set of 11 objectives. Notable among them is establishing scalable data infrastructures to enable the military to store and process data in wartime conditions; governing the data infrastructure required to support critical missions; and facilitating seamless assimilation of operations/intelligence. Furthermore, the plan stresses establishing flexible operational data centres that are force-structured and geographically dubious to sustain multidomain and theatre-specific operations.[30]

In addition, AWS has also announced development of a modular data centre designed for operational use of the US military. The project aims to maintain huge storage capacities and support bulky workloads in remote and challenging terrains. More specifically, these modern capabilities are aimed at enabling the US military to operate in Disconnected, Disrupted, Intermittent, or Limited (DDIL) places where strong communication links with central data servers are limited or not guaranteed. The project was conceived during the contract titled *'Joint Warfighting Cloud Capability (JWCC)'*, enabling the DoD to take advantage of cloud abilities in undertaking critical missions.[31]

According to DoD's *'Strategic Management Plan, 2022-2026'*, the Department will focus on five priorities. Amongst them, the second priority is directed towards transforming the foundations of future military forces. In this regard, the DoD is gearing up to initiate Cloud and Data Centre Optimisation, aimed at the closure of

---

29 U.S. Department of Defense, "DoD Data Strategy," October 30 2020, https://media.defense.gov/2020/Oct/08/2002514180/-1/-1/0/DOD-DATA-STRATEGY.PDF.

30 Office of the Chief Information Officer, "Army Data Plan," Accessed December 13, 2024, https://www.army.mil/e2/downloads/rv7/about/2022_army_data_plan.pdf.

31 U.S. Department of Defense, "Department of Defense Announces Joint Warfighting Cloud Capability Procurement," December 7, 2022, https://www.defense.gov/News/Releases/Release/Article/3239378/department-of-defense-announces-joint-warfighting-cloud-capability-procurement/.

vulnerable data centres and facilitating a seamless transition to cloud-enabled operations.[32]

Like other services, the U.S. Navy is also planning to establish data infrastructure networks to overcome two-pronged challenges: how to deal with large swaths of data and understanding if the Navy has the correct data to inform leaders' decision-making during a crisis. One example is 'Jupiter Today', a platform that makes the Navy's data visible, accessible, and usable across the naval enterprise. It also bolsters naval decision-making capabilities by providing military and civilian planners with data visualisations and analytics for naval data force actionable insights, decisions, and outcomes. Currently, the U.S. Navy is planning to build a 'multi-story communications centre facility' in Guam. The estimated cost of the data centre will be around USD 500 million, which includes an information facility to conduct naval information operations.[33]

People's Republic of China

As a potential contender to the unipolar hegemony of the US, China is also hedging its bet to become a dominant player in the geopolitics of data centres. As discussed earlier, the ability to control and disseminate data guarantees technological and strategic ascendancy. China is eager to capitalise on this opportunity by building a physical infrastructure of digital data while at the same time developing the regulations to enable global data flow towards Beijing. Due to a favourable domestic environment, Chinese companies, supported by the government, are poised to build global data centres and emerge as key players in this digital geopolitical grail.

Chinese industrial planners see data as a new factor of production. However, currently, China does not possess an upper hand in data infrastructure vis-à-vis the US or other global actors. This is evident from the broader regional picture in Asia where Singapore is working towards gaining a competitive advantage by leveraging its talent pool, geopolitical stature, and connectivity. Nonetheless, China's domestic market size and capacity grant it a structural edge over its regional peers to build advanced data infrastructure.

China's Push for Data Centres

China's growing interest in data centres is a part of its long-term data strategy. In 2013, the Ministry of Industry and Information Technology (MIIT) published a guideline titled 'Guiding Opinions on the Layouts of Data Centre Construction' which outlined the laws for regulating data centres in the country. Back then, nearly 70% of

[32] U.S. Department of Defense, "DoD Strategic Management Plan: Fiscal Years 2022-2026," April 12, 2024, https://media.defense.gov/2024/Apr/12/2003438601/-1/-1/1/FY25_DOD_STRATEGIC_MANAGEMENT_PLAN_2024_FINAL.PDF.

[33] Georgia Butler, "U.S. Navy to Build Data Centre at Camp Blaz base in Guam," *Data Centre Dynamics,* October 29, 2024, https://www.datacentredynamics.com/en/news/us-navy-to-build-data-centre-at-camp-blaz-base-in-guam/.

China's data centres received government support which has been increasing over the years.[34] The Chinese government has been working with commercial service providers to develop cloud governing systems. In 2015, the MIIT and the National Energy Administration released a joint working plan for establishing 'National Green Data Centres.'[35] In 2016, the MIIT issued a 'Big Data Industry Development Plan (2016-2020)', with policy guidelines for local governments and enterprises to lay down the framework of data centre construction.[36] By 2018, the Central Economic Work Conference's focus on building new infrastructures became a lynchpin in China's pandemic recovery investment.[37]

China's digital strategy is calibrated to rely on inexpensive energy sources to make it a unique player in the data centre landscape. In 2020, the Politburo Standing Committee placed the creation of data centres under the notion of 'new infrastructures' as a priority of the government.[38] The term 'new infrastructure' refers to physical centres such as telecommunication base centres, industrial internet systems, and data centres. In 2022, the data centres were mentioned as a national priority in the National Development and Reform Commission (NDRC) Implementation Plan for the 14th five-year plan to enlarge domestic demand.[39] This entails a focus on data localisation and cross-border flow, showing its proactive approach by enacting domestic data localisation regulations to guard vital domestic data and redirect international data flow towards China.

In the past two years, China has invested more than USD 6.1 billion in data centres. The country has increased its investments in data infrastructures to circumvent export controls imposed by the US in the wake of trade wars. According to estimates by the NDRC, around eight data centre clusters could see an investment of USD 63 billion per annum.[40]

---

34 "China: MIIT Releases Guiding Opinions on Development of Industrial Big Data," *DataGuidance*, Last Modified May 13, 2020, https://www.dataguidance.com/news/china-miit-releases-guiding-opinions-development.

35 Peter Judge, "Chinese Government Calls For Green Data Center Catch-Up," *Data Center Dynamics,* March 24, 2015, https://www.datacenterdynamics.com/en/news/chinese-government-calls-for-green-data- center-catch-up/.

36 Centre for Security and Emerging Technology, "14th Five-Year Plan for the Development of the Big Data Industry," February 10, 2022, https://cset.georgetown.edu/publication/14th-five-year-plan-for-the-development-of-the-big-data-industry/.

37 The State Council Information Office, "China Kicks Off Central Economic Work Conference for 2018," December 19, 2017, http://english.scio.gov.cn/topnews/2017-12/19/content_50111291.htm.

38 Emily De La Bruyere and Nathan Picarsic, *China's Quest for Asymmetric Dominance in Data Centers,* report (Hinrich Foundation, 2024).

39 The People's Government of Fujian Province, "Outline of the 14th Five-Year Plan (2021-2025) for National Economic and Social Development and Vision 2035 of the People's Republic of China," August 9, 2021, https://www.fujian.gov.cn/english/news/202108/t20210809_5665713.htm.

40 Georgia Butler, "China has Spent $6.1bn Building Data Centres in the Past Two Years," *Data Centre Dynamics,* September 3, 2024, https://www.datacentredynamics.com/en/news/china-has-spent-61bn-building-data-centres-in-the-past-two-years/.

Besides USD 6.1 billion investment by the Chinese government, the cluster has attracted nearly USD 28 billion in investment from the private sector. So far, 1.95 million data server racks have been installed by the Chinese government, and out of them 63% are operational. These data centres are located in Inner Mongolia, Southwest Guizhou, Gansu, Beijing-Tianjin-Heibei, Guangdong Hong Kong-Macua Greater Area, Yangtze River Delta, and Chengdu Chongqing Economic Circle. Besides these, the government also plans to build an additional ten smaller data centre hubs across the country.[41]

China is clearly focused on developing a nationwide network of internet data centres—an initiative indicative of its broader strategy for data centre development. According to a senior government official, through these centres, Beijing aims to accelerate the synergy of informatisation and industrialisation by constructing advanced 5G infrastructure and information facilities, thereby enhancing the global competitiveness of Chinese technology brands.[42]

Data Localisation

Data localisation is of utmost significance for China due to its entrenched aim of achieving data asymmetry with global competitors. This will also allow the state to exert its influence on domestic and international tech entities. As discussed earlier, their AI+ framework has placed data-centre-backed national integrated computing networks at the forefront.[43] Chinese industrial policy is conducive to creating real-world infrastructure to harness the actual potential of AI and other emerging technologies.

China's approach to data localisation aligns with the instrumentalisation of surveillance capitalism, reflecting a model where data control serves both state surveillance and economic objectives. Accordingly, the state capitalises on the vast amount of data collected from users within the confines of internal analytics and programming.[44] This allows the state to observe, monitor and monopolise control on data crucial for national defence strategies, military calculations, and financial operations. On the other hand, flow of data is one of the most formidable and complex tasks where free-flowing data poses pressing challenges to geopolitics, national security, privacy protection, industrial capabilities, and financial markets. Hence, cross-border data flow may also override the government's enforcement capacity over the digital industry.[45]

---

41 Butler, "China has Spent $6.1bn Building Data Centres in the Past Two Years."

42 Tu Lei, "China Prepares to Pilot Opening-up of Internet Data Centers," *Global Times,* March 8, 2024, https://www.globaltimes.cn/page/202403/1308482.shtml.

43 Bruyere and Picarsic, *China's Quest for Aymmetric Dominance in Data Centers.*

44 Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (New York: Public Affairs, 2019).

45 Alibaba Cloud, "AliBaba Shines as Center of Innovation with Research Presented at SIGCOMM 2019," September 25, 2019, https://www.alibabacloud.com/blog/alibaba-shines-as-center-of-innovation-with-research-presented-at-sigcomm-2019_595391

There are reports that caution that data sovereignty strategies of the US and Europe are 'offensive' in nature, where Atlanticist powers promote control of cross-border data flows to claim access to data outside a country's jurisdiction. China's localisation of data infrastructure strategy is, hence, part of broader, forward-thinking that understands data asymmetry between China and its Western counterparts.[46] Furthermore, it allows Beijing to consolidate control over domestic and international companies.

Unlike Western academics, Chinese discourse views the 'state' as a core architect of governing information and data flow on external and internal fronts.[47] China's extensive datafication has prompted a comprehensive regulatory strategy to manage its domestic economic landscape and transnational data flows.[48] Part of China's push for data sovereignty stems from its comparative disadvantage to the US in ultra-large-scale data centres.[49] Despite this gap, China holds second position globally due to its rapid growth potential. This competitive positioning has motivated efforts to scale up data aggregation while safeguarding national security through controlled data governance. China's expansive legal framework on cross-border data flows should strive for a balanced approach ensuring both data protection and secure outflows. Chinese scholars advocate that critical industry and enterprise data ought to be stored, processed, and routed domestically to uphold national security.[50] However, such localisation ambitions depend on the development of a secure and resilient data infrastructure. As such, China's strategy hinges on constructing and operating data centres under domestic control to manage and regulate data flows effectively.

Tesla offers a prominent example of China's push for data localisation. In April 2024, the China Association of Automobile Manufacturers approved new data privacy and security requirements centred on local data storage. Tesla secured approval to operate as an international brand in the Chinese market by complying with these regulations, most notably through the establishment of its first data centre in the country.[51]

---

46 Chinese National Development and Reform Commission, *Guidelines for National Data Infrastructure Construction,* report (Washington D.C., 2024), https://cset.georgetown.edu/wp-content/uploads/t0608_data_infrastructure_EN.pdf

47 Min Tang, "The Challenge of the Cloud: Between Transnational Capitalism and Data Sovereignty," in *The Geopolitics of Chinese Internets,* ed. Jack Linchuan Qiu, Peter K. Yu and Elisa Oreglia (London: Routledge, 2024), 75.

48 Chi Zhang, "China's Privacy Protection Strategy and its Geopolitical Implications," *Asian Review of Political Economy* 3, no. 6 (2024): 1-17.

49 Peter Harrell, "Managing the Risks of China's Access to US Data and Control of Software and Connected Technology, *Carnegie Endowment for International Peace,* January 30, 2025, https://carnegieendowment.org/research/2025/01/managing-the-risks-of-chinas-access-to-us-data-and-control-of-software-and-connected-technology?lang=en.

50 Xinyi Du and Aijiao Liu, "Security and Openness: China's Cross-Border Data Flow Scheme," *Pacific International Journal* 6, no. 1 (2023): 138–141, https://doi.org/10.55014/pij.v6i1.326.

51 "As Musk Visits China, Tesla Wins Key Data Security Clearance," *Bloomberg News,* April 28, 2024, https://www.bloomberg.com/news/articles/2024-04-29/as-musk-visits-china-tesla-wins-key-data-security-clearance.

The Tesla case is just a tip of the iceberg. China requires similar data localisation measures from personal data users in online applications. These measures have led to the establishment of several partnerships between Western tech titans Amazon, Apple and Microsoft, and Chinese data giants such as Guizhou-Cloud Big Data.

China's PLA and Data Security

When it comes to global competition, the People's Liberation Army (PLA) remains the epicentre of Chinese grand strategy. Considering the global geopolitical dynamics, PLA is adapting to changing realities by investing heavily in new technologies including AI, quantum computing, Big Data, and IoT. This is evident in the shift of Chinese military doctrine from 'informatisation' (*xixinhua*) to 'intelligentisation'. Chinese military strategists are convinced that the first war is likely to be dominated by algorithms and ML, where information and data processing will play a key role in informing the decisions of policymakers.

In this regard, establishing data centres is a prerequisite for the PLA to store, regulate, and process data in wartime conditions. Using data both for offensive and defensive measures is central to the PLA's military planning.

The *Science of Campaigns*, often described as the cornerstone of China's military doctrine,[52] places information warfare at the forefront of operational activity. Alongside kinetic actions such as long-range strikes on data centres and information infrastructure, it emphasises electronic and cyber warfare. Equally, the PLA prioritises safeguarding its own data and network systems to ensure *'operational security.'*[53]

Chinese President Xi Jinping has been a proponent of a Military-Civil Fusion (MCF) strategy to harness the expertise of industry, academia, and entrepreneurs to turbocharge the strength of the PLA. A notable example is establishment of Wuhan University under the administration of the State Administration of Science, Technology, and Industry for National Defence, and overseen by the State Council's Central Commission for Integrated Military and Civilian Development.[54] By strategically aligning academic research with national defence priorities, the university is well-positioned to leverage its international collaborations to contribute to the PLA's modernisation drive. This reflects China's broader vision of harnessing civilian technological capacity to augment military innovation and self-reliance. For instance, the university is affiliated with the International GNSS Services, a federation comprised

---

52 People's Liberation Army, *Science of Campaigns*, trans. China Aerospace Studies Institute (Montgomery, AL: China Aerospace Studies Institute, 2020); and, Wang Houqing and Zhang Xingye, eds., *Science of Campaigns* (Beijing: National Defence University Press, 2000), https://www.airuniversity.af.edu/Portals/10/CASI/documents/Translations/2020-12-02%20In%20Their%20Own%20Words-%20Science%20of%20Campaigns%20(2006).pdf.

53 Ibid., 175-82.

54 Samuel Strickland, "How China's Military Plugs into the Global Space Sector," *Strategist,* October 26,2022, https://www.aspistrategist.org.au/how-chinas-military-plugs-into-the-global-space-sector/.

of a cluster of 350 organisations across 118 states, with a mission to provide open-access data products on navigational satellites for the benefit of the members and international community.[55]

Geopolitical Implications

The contestation between China and the US carries profound implications for the global technological order, shaping the direction of innovation, standards-setting, and control over emerging technologies.

Data Sovereignty and Digital Colonialism

The US-China competition raises critical concerns about data sovereignty and evokes parallels with historical patterns of data colonialism. In an era of unrestricted global data flows, the question of who controls data remains central. The presence of US and Chinese data centres on foreign soil raises concerns about the potential compromise of sensitive information, including government records and financial data of host countries. Apart from the European Union's General Data Protection Regulation (GDPR), most countries lack comprehensive national frameworks for data privacy and regulation, leaving them vulnerable to the influence of tech giants that often operate beyond the jurisdiction of domestic legal systems.

Geopolitical Complications

Growing divisions in the global digital sphere risk fragmenting the world into competing technological blocs. This emerging bifurcation presents a dilemma for middle powers and smaller states, which must tackle intensifying pressures while striving to safeguard their national interests and technological sovereignty. In this context, the US and China are not only investing in digital infrastructure and networks for connectivity, but also to assert control, consolidate influence, and expand the reach of digital surveillance. Both are also vying for footholds in emerging regions such as Southeast Asia and the Nordic Arctic. The establishment of data centres in Finland and Norway reflects Washington's attempt to secure a first-mover advantage in one of the world's most remote yet strategically vital frontiers. Similarly, the digital competition unfolding in Southeast Asia highlights the urgency with which both powers seek to expand their influence across the Asia-Pacific, using digital infrastructure as a conduit for long-term leverage.

Threat of Escalation over Data Infrastructure

The modernisation of data infrastructure brings with it heightened risks of sabotage, espionage, physical damage, and cyber-attacks targeting data centres. Recently, incidents of subsea infrastructure attacks raised alarms in the strategic community,

[55] International GNSS Service, "About the IGS," Accessed May 20, 2025, https://igs.org/about/#.

e.g., in November 2024, two undersea cables C-Lion1 and BCS East-West Interlink were damaged in the Baltic Sea.[56]

Challenges

Data centres now lie at the heart of global geopolitical competition but their rise comes with a minefield of challenges. Some of the most pressing include:

Cyber-Attacks and Digital Espionage

Data centres are an attractive avenue for hackers to conduct cyber-attacks and digital espionage. Events like the Yahoo cyber-attack[57] and 'WannaCry' ransomware attacks[58] are stark reminders that relying solely on one source for data comes with serious vulnerabilities. In the same vein, data centres are vulnerable to cyber-attacks and digital espionage, risking citizen privacy, government files, and financial records. In this regard, relying on externalities, including major powers and tech titans, could be perilous as it puts the country's data security at the discretion of a few while overshadowing its domestic efforts to consolidate data control.

Role of Small and Middle Powers

As next-generation technologies take centre stage in global geopolitical discourse, a widening divide is emerging between technological 'haves' and 'have-nots.' The establishment and maintenance of data centres demand extensive political, financial, and technological resources which remain out of reach for many small and middle powers. This disparity exposes these states to a growing reality of technological dependency, where dominant powers can leverage their digital supremacy to influence policymaking. A striking example lies in the cases of Stargate and China: the former's centralised data infrastructure and the latter's stringent data localisation policies both illustrate how concentrated control over digital ecosystems can entrench asymmetric dependencies among less technologically advanced nations.[59]

The weaponisation of data centres compels smaller states to align with great power preferences, effectively forcing them to take sides in an increasingly techno-polar world. As both the US and China adopt more inward-looking approaches to

---

56 Ryan Browne, "Undersea Cable Cuts in the Baltic Sea are Stoking Geopolitical Tensions- What's Going On," *CNBC,* November 28, 2024, https://www.cnbc.com/2024/11/28/explainer-baltic-sea-undersea-cable-cuts-stoke-geopolitical-tensions.html.

57 Nicole Perlroth, "All 3 Billion Yahoo Accounts Were Affected by 2013 Attack," *New York Times,* October 3, 2017, https://www.nytimes.com/2017/10/03/technology/yahoo-hack-3-billion-users.html.

58 BBC News, "Cyber-Attack: US and UK Blame North Korea for WannaCry," December 19, 2017, https://www.bbc.com/news/world-us-canada-42407488.

59 Shaheer Ahmad, "Stargate: A Trojan Horse for Global Technological Dependency," *Centre for Aerospace & Security Studies,* March 5, 2025, https://casstt.com/stargate-a-trojan-horse-for-global-technological-dependency/.

technological development and control, small and middle powers face mounting pressure to recalibrate their foreign policies simply to maintain access to the latest digital infrastructure. In this context, the notion of 'technological neutrality' is becoming increasingly untenable. The confinement of advanced technologies within great power spheres of influence presents these states with a stark choice: *embrace it or lose it*.

Supply Chain Vulnerabilities

From minuscule semiconductors to critical rare earth elements, a wide array of technological components is being weaponised amid the intensifying US-China competition. Flashpoints such as Taiwan represent acute geopolitical risks, where conflict could instantly disrupt global supply chains. A disruption in semiconductor production, in particular, would severely undermine the world's capacity to develop and sustain advanced computing systems striking at the core of data centre functionality and the broader digital ecosystem.

Data Bifurcation

China and Russia are actively implementing measures to reduce the influence of foreign actors in critical technological sectors. A recent example is China's release of *Document 79*, which outlines plans to eliminate foreign data dependencies in key industries such as finance and energy by 2027.[60] Notably, the document references a 'delete America' directive signalling the intent to replace Intel and AMD microprocessors with domestically produced alternatives. In parallel, the US has intensified its regulatory posture, including restrictions on the transfer of sensitive genomic data to China.[61] These reciprocal actions reflect an accelerating trend towards the geopolitical bifurcation of data systems, laying the groundwork for emerging 'data blocs' defined by alliances, regulatory divergence, and digital sovereignty.

Erosion of State Control

Data is intrinsically transnational. Regardless of how rigorous policies are to localise data, it will likely continue to flow across the border. This transnational feature of data challenges the state's illusion of control, posing complex questions about national security, individual privacy, industrial aptitude, and financial capabilities.

---

60 Liza Lin, "China Intensifies Push to 'Delete America' from its Technology," *The Wall Street Journal,* March 7, 2024, https://www.wsj.com/world/china/china-technology-software-delete-america-2b8ea89f.

61 The White House, "Fact Sheet: President Biden Issues Executive Order to Protect Americans' Sensitive Personal Data," February 28, 2024, https://www.whitehouse.gov/briefing-room/statements-releases/2024/02/28/fact-sheet-president-biden-issues-sweeping-executive-order-to-protect-americans-sensitive-personal-data/.

Environmental Cost

While data centres have become essential to the digital economy, their construction and operation come at an environmental cost. One of the most pressing challenges is their high energy consumption. Rough estimates suggest that data centres account for approximately 2% to 3% of global electricity usage. This is an increasingly unsustainable figure as demand for digital infrastructure continues to rise.[62] According to the International Energy Agency, this figure is expected to double by 2026.[63]

The US has aging energy grids,[64] which are under intense pressure due to rising electricity demand, extreme weather conditions, and a shift to renewable energy sources.[65] Data centres are projected to consume 8% of total US electricity by 2030,[66] reflecting a broader global trend of escalating energy demands. In parallel, data centre power consumption is expected to more than double, from 17 gigawatts in 2022 to 35 gigawatts by 2030, underscoring the growing energy intensity of digital infrastructure.[67]

Energy and Water Usage

As noted earlier, data centres consume vast amounts of energy, with a large portion dedicated to cooling systems essential for preventing hardware failure. Among the common methods, water-based cooling is often preferred for its efficiency. However, this approach demands large volumes of water, placing considerable strain on local resources, especially in regions already facing scarcity.[68] This can also result in

---

62 "Understanding the Power Consumption of Data Centres," *Socomec,* Accessed December 12, 2024, https://emea.socomec.com/en/solutions/business/data-centres/understanding-power-consumption-data-centres#:~:text=How%20much%20electricity%20do%20data,to%20the%20International%20Energy%20Agency.

63 Matthew Gooding, "Global Data Centre Electricity Use to Double by 2026 - IEA Report," *Data Centre Dynamics,* January 26, 2024, https://www.datacentredynamics.com/en/news/global-data-centre-electricity-use-to-double-by-2026-report/.

64 Evan Halper, "Nation at Risk of Winter Blackouts as Power Grid Remains under Strain," *Washington Post,* November 8, 2023, https://www.washingtonpost.com/business/2023/11/08/power-grid-blackouts-texas/.

65 Evan Halper and Caroline O' Donovan, "AI is Exhausting the Power Grid. Tech Firms are Seeking a Miracle Solution," *Washington Post,* June 21, 2024, https://www.washingtonpost.com/business/2024/06/21/artificial-intelligence-nuclear-fusion-climate/.

66 "AI is Poised to drive 160% Increase in Data Centre Power Demand," *Goldman Sachs,* May 14, 2024, https://www.goldmansachs.com/insights/articles/AI-poised-to-drive-160-increase-in-power-demand.

67 International Energy Agency, *Electricity 2024: Analysis and Forecast to 2026,* report (International Energy Agency, 2024), https://www.iea.org/reports/electricity-2024/executive-summary.

68 Matt O' Brien, "Artificial Intelligence Technology behind ChatGPT was Built in Iowa – With a Lot of Water," *AP News,* September 9, 2023, https://apnews.com/article/chatgpt-gpt4-iowa-ai-water-consumption-microsoft-f551fde98083d17a7e8d904f8be822c4?utm_source=sg&utm_medium=email&utm_campaign=article_email&utm_content=article-11231.

diversion of water from other critical sectors such as agriculture and public supplies. Moreover, when water used in data centre cooling systems is discharged back into local reservoirs, it may pose environmental risks. The thermal load and potential saturation with harmful chemicals can hurt aquatic ecosystems and threaten marine life, raising concerns about the ecological sustainability of current data centre operations.

Apart from direct environmental impacts, there are also a minefield of indirect impacts. The manufacture of advanced hardware components, particularly servers, depends heavily on semiconductor chips. This involves extensive mining of rare earth minerals which cause pollution and habitat decimation. Moreover, rapid advancements in technology renders previous equipment obsolete, generating a significant amount of electronic waste. The presence of toxic chemicals, such as lead and mercury, from such waste taint the soil and water if mismanaged.

Recommendations

Despite geopolitical ebbs and flows, data centres are critical to maintain technological dominance. The following recommendations are essential for consideration at the national and international level:

Build and Diversify Data Infrastructure

To strengthen national infrastructure, regulators must craft frameworks that both enable rapid data-centre deployment and incentivise investment in ancillary systems (power, cooling, security). Securing access to ground-breaking semiconductor chips, microprocessors, and server hardware is vital for scaling capacity. In light of China's data localisation requirements and the US's export-control regimes, middle and small powers ought to develop a geographically and supplier-diverse portfolio of data-centre sites, undersea cables, and edge-computing nodes. Finally, they must underpin these facilities with high-bandwidth, low-latency networks ensuring efficient data exchange between users, centres, and cloud platforms.

Encourage Innovation

Governments and industry stakeholders should accelerate innovation in data-centre development by incentivising modular, prefabricated designs for rapid, scalable deployment; supporting R&D and pilot projects in advanced cooling (such as liquid-immersion and AI-driven thermal management) alongside on-site renewables and storage; championing AI-powered infrastructure management and digital-twin simulations for predictive maintenance and capacity planning; enabling regulatory sandboxes for edge and micro-data-centre roll-outs to serve low-latency applications; and fostering open standards and interoperability through industry consortia to reduce vendor lock-in and spur competitive, sustainable advances across the ecosystem.

Innovation in energy management is critical for next-generation data centres: leveraging AI-driven analytics can optimise power distribution and predict load fluctuations to minimise consumption, while partnerships between government and industry, exemplified by both American and Chinese initiatives to develop ultra-efficient microprocessors are essential for reducing hardware energy draw; complementing these efforts with on-site renewable generation, smart grid integration, and advanced energy-storage solutions will further decarbonise operations and ensure resilient, low-carbon data-centre power systems.

Prioritise International Cooperation

Prioritising cooperation over conflict can enable major powers to equitably share the technological burden and foster a more stable global digital order. Collaborations with emerging economies like Brazil, Vietnam, Thailand, Indonesia, and The Philippines, have the potential to cultivate a more inclusive and harmonious digital environment, mitigating mistrust and alleviating underlying technopolitical tensions. Similarly, Gulf States are well-positioned to serve as regional connectivity hubs by supporting development of data centre infrastructure, thereby contributing to a more balanced digital ecosystem and bridging the divide between the Global North and Global South.

Development of Domestic Legislation

The regulation of data infrastructure is a fundamental prerequisite for responding effectively to the intensifying digital contention between major powers. Drawing lessons from the EU's GDPR provides a valuable framework for monitoring the behaviour of data subjects and ensuring accountability in data processing. For middle powers such as Pakistan, development of domestic legislation on data governance is equally critical. Such policies not only enable oversight of technology companies and foreign enterprises operating within national borders, but also enhance digital sovereignty, safeguard citizen privacy, and position these countries as credible actors in the evolving global digital order.

Conclusion

Data centres have become central to contemporary great power competition, with the ability to store, process, and control data underpinning political authority, financial stability, and military capability. The competition between the United States and China increasingly revolves around securing global dominance in data infrastructure mirroring historical shifts driven by railroads and telecommunications that once redefined geopolitical influence. As the backbone of the next industrial revolution, data centres will play a defining role in shaping future global power hierarchies.

A pragmatic response hinges on forging effective public-private collaborations, channeling investment into homegrown technological development, and enacting

policies that reinforce digital sovereignty. Coherent regulatory frameworks and secure data ecosystems will be critical for Pakistan and comparable middle powers to reduce external dependence and secure genuine digital autonomy.

At the same time, the global expansion of data infrastructure brings risks such as deepening the digital divide, exacerbating technological dependency, and exposing nations to cyber vulnerabilities and environmental stress. Therefore, promoting cooperative interdependence, particularly through inclusive engagement with small and middle-income countries, is vital. Reducing the technology and connectivity disparity between advanced and emerging economies can unlock new economic opportunities in under-served regions while strengthening the resilience and security of global digital networks.

ABOUT THE AUTHOR

Shaheer Ahmad *is a Research Assistant at the Centre for Aerospace & Security Studies (CASS), Islamabad, with prior experience at the Institute of Strategic Studies, Islamabad, and the Consortium of Indo-Pacific Researchers in New Jersey, USA. His research focuses on the intersection of international relations, geopolitics, military strategy, and emerging technologies, with regional emphasis on the Asia-Pacific, Arctic, and South Asia. He holds a Bachelor's degree in International Relations from the National Defence University (NDU), Pakistan.*

ABOUT CASS

The Centre for Aerospace & Security Studies (CASS), Islamabad, was established in 2018 to engage with policymakers and inform the public on issues related to aerospace and security from an independent, non-partisan and future-centric analytical lens. The Centre produces information through evidence-based research to exert national, regional and global impact on issues of airpower, emerging technologies and security.

VISION

To serve as a thought leader in the aerospace and security domains globally, providing thinkers and policymakers with independent, comprehensive and multifaceted insight on aerospace and security issues.

MISSION

To provide independent insight and analysis on aerospace and international security issues, of both an immediate and long-term concern; and to inform the discourse of policymakers, academics, and practitioners through a diverse range of detailed research outputs disseminated through both direct and indirect engagement on a regular basis.

CORE AREAS OF RESEARCH

Aerospace

Emerging Technologies

Security

Strategic Foresight

CASS www.casstt.com
CENTRE FOR AEROSPACE & SECURITY STUDIES, ISLAMABAD
Independence | Analytical Rigour | Foresight

Old Airport Road, Islamabad, Pakistan
+92 51 5405011
cass.thinkers@casstt.com
www.casstt.com
@CassThinkers
Centre for Aerospace & Security Studies
cassthinkers
cass.thinkers