

OCTOBER 2023

LAZARD | 175

GEOPOLITICAL ADVISORY

RESEARCH BRIEF

# Geopolitics of Artificial Intelligence



# Lazard Geopolitical Advisory

## Senior Advisors



Gen. John Abizaid (ret.)  
Senior Advisor



Jami Miscik  
Senior Advisor



Adm. William McRaven (ret.)  
Senior Advisor



Sir Stephen Lovegrove KCB  
Senior Advisor



Dante Roscini  
Expert Advisor

## Senior Leadership



Theodore Bunzel  
Head & Managing Director



Siddharth Mohandas  
Director



Paul Norwood  
Director

## Geopolitical Advisory Team



Daniel Jevremovic  
Vice President



Abraham Axler  
Vice President



Carlos Petersen  
Associate



Aily Zhang  
Associate



TJ Nzewi  
Associate



Sienna Tompkins  
Analyst  
*Lead Author*



Trenton Stone  
Analyst



Robert Bailey  
Analyst



## About Geopolitical Advisory

Lazard Geopolitical Advisory blends leading geopolitical insights with unmatched advisory expertise, advising clients on how geopolitical trends translate into business impact.

To discuss this report or how Geopolitical Advisory could support your firm, please contact [geopoliticaladvisory@lazard.com](mailto:geopoliticaladvisory@lazard.com)

New York  
30 Rockefeller Plaza  
New York NY 10112  
United States  
+1 212 632 6000

Singapore  
One Raffles Place  
#29-63 Tower 2  
1 Raffles Place  
Singapore 048616  
+65 6534 2011

Paris  
175 Bd Haussmann  
75008 Paris  
France  
+ 33 1 44 13 01 11

London  
50 Stratton St  
London W1J 8LL  
United Kingdom  
+44 20 7187 2000

San Francisco  
4 Embarcadero Center  
24<sup>th</sup> Floor  
San Francisco CA 94111  
United States  
+1 415 623 5000

Austin  
200 West 6<sup>th</sup> St  
Suite 1650  
Austin TX 78701  
United States  
+1 512 652 2600

# Table of Contents

## EXECUTIVE SUMMARY

### I GEOPOLITICS OF ARTIFICIAL INTELLIGENCE

1	AI ON THE FRONTLINES OF GEOPOLITICAL COMPETITION	7
2	REGULATING AI	9
3	GEOPOLITICAL BOTTLENECKS IN THE AI VALUE CHAIN	12
4	BUSINESS IMPLICATIONS	17
5	LOOKING AHEAD	19

# Executive Summary

The artificial intelligence (AI) boom invites a geopolitical question with profound implications: who will benefit and how? Previous general-purpose technologies, like electricity and computers, drove surges in productivity, altered social structures, and shifted the international balance of power. For its part, AI is projected to add an annual 3.3% productivity boost, or up \$25.6 trillion, to the global economy.<sup>1</sup> Political systems are already being transformed as AI changes our understanding of knowledge and services such as healthcare and education are expected to experience vast improvements. It will also change how warfare is conducted and intelligence collected. AI-driven software will cut decision-making windows down sharply, help engineer cyberattacks, and scale personalized disinformation, while autonomous tanks and AI-enabled drone swarms will become routine in the course of battle.

The scramble to develop and deploy AI is, therefore, one of the frontiers of accelerating geostrategic competition. Countries are competing to secure the economic, political, and military advantages of AI in an increasingly fragmented and polarized geopolitical environment. While there is common concern about the potential dangers posed by AI, we expect limited global cooperation given competitive dynamics, and are seeing policy both to promote and place guardrails on AI primarily at the national level and within smaller, more politically manageable international forums. Over time, these dynamics will trend towards more fragmented and incompatible AI ecosystems. Businesses will need to navigate increasing regulatory complexity caused by this fragmentation as well as the heightened risk of being targeted by rival states or malicious non-state actors over strategic technology unbound by any international rules of the road.

This research brief provides an overview of the geopolitical dynamics impacting countries' approach to AI, the policy responses and how they interact with bottlenecks in the AI value chain, as well as the business implications for the technology, healthcare, financial services, and energy sectors.

## Key findings

- **AI is pivotal to the unfolding, and end state, of US-China competition:** The compounding economic and national security benefits of leadership in AI will arguably have a determinative impact on the outcomes of US-China rivalry
- **Geopolitical bottlenecks in the AI supply chain currently favor the US but its leadership in AI is not predetermined:** The US' structural advantages in computing power, talent, and energy bolster Washington's ability to gatekeep AI development and apply geopolitical pressure to competitors (e.g., China) across the AI value chain; however, much depends on enacting policies to bolster those advantages going forward
- **Distinct commercial and regulatory AI ecosystems will emerge:** As the US and China solidify their leads and tighten control over necessary inputs, countries have reluctantly started to align with the US or China to ensure access to increasingly indispensable AI
- **Middle / great powers (i.e., Canada, France, Israel, the UK) can leverage AI to punch above their weight:** Advanced economies with strong education and innovation ecosystems can compensate for smaller population sizes and declining geopolitical influence by leveraging AI in their economies
- **Less developed countries will fall behind in the current race for AI:** Without access to expensive computing power, physical infrastructure, and large AI talent pools, less developed countries will increasingly need to trade market access in exchange for access to powerful AI

## Executive Summary (cont'd)

- **New international governance frameworks on the horizon:** Proposals for new agencies and models of governance are proliferating and will begin to turn into more concrete policy from the end of 2023 onward

As companies consider the transformative impact AI may have in their sector, it is also worth assessing where AI's interaction with geopolitics affects its deployment and impacts businesses. Companies should assess where they are exposed across the four geopolitical bottlenecks in the AI value chain (computing power, data, talent, physical infrastructure) as well as opportunities to engage countries as they seek to advance their respective AI agendas.



## **I Geopolitics of Artificial Intelligence**

# 1. AI on the Front Lines of Geopolitical Competition

Leadership in AI—and emerging technologies more generally—has become the frontier of US-China geostrategic competition. AI is critical not only to the defense of countries (e.g., through next-generation autonomous weapons), but also their political functions as AI changes how the creation and distribution of information is understood. AI-generated content and deep fakes significantly lower the cost of influence operations by both domestic and foreign actors and will influence, and even disrupt, democratic processes. Above all, the vast economic gains made possible by AI are driving the centrality of AI competition in the global policy agenda.

The US is, as a result, racing to disentangle its AI ecosystem from China's in a bid to cement the US's strong, but not insurmountable, lead in AI development. This marks a sea change from the role US technology companies initially played in anchoring and developing China's dynamic AI ecosystem. Export controls already block the transfer of vital US semiconductor technology to China, while recently announced, novel outbound investment rules aim to stem the flow of US capital and knowledge to Chinese AI companies. These measures are significantly changing the business landscape for US technology firms and investors. Within this new status quo, businesses need to track existing compliance as well as periodic tightening of restrictions and attempts to close perceived loopholes. The first set of follow-up restrictions to semiconductor export controls were announced in mid-October and introduce tighter performance thresholds for chips that can be exported to China while requiring approval to export chips below the threshold by the Commerce Department.

Meanwhile, China's leadership has long been committed to cultivating its AI industry and the foundational infrastructure enabling its development. Along with other key policy initiatives, Beijing announced artificial intelligence as a priority growth area as early as 2017 in its "New Generation Artificial Intelligence Development Plan" alongside the signature "Made in China 2025" initiative. China spends tens of billions of dollars on implementing these strategies.<sup>2</sup> At least two Chinese regional governments have committed to investing \$14bn each in AI development, while Beijing's \$45bn semiconductor fund, known as the "Big Fund," supports self-reliance for the hardware required to enable AI development. It is increasingly apparent that both the US and China are mobilizing to reap the economic, military, and political benefits of AI capabilities ahead of the rest.

AI is not only a two-way race between the US and China. The UK, Canada, France, Singapore, India, South Korea, and Israel, among others, have become prominent AI players. Russia also harbors ambitions to be an AI leader and has sought to deploy it for influence operations in the West, though the war in Ukraine and US sanctions have hindered efforts at the cutting edge. The US and China top most global AI power rankings, but other countries are implementing strategies to bridge the gap by developing sovereign large language models (LLMs), funding "national champion" AI companies, creating AI hubs, improving their digital infrastructure, and strategically protecting and using data. The UK, for instance, has allocated an initial \$1.1bn to improve access to computing power, and \$125mn to its new Foundation Model Taskforce, an expert taskforce to help build and adopt generative AI. France has invested in national champions, such as generative AI company Mistral AI, to compete with predominantly US-based LLM leaders. Strong AI capabilities pose an opportunity for so-called "middle powers" (e.g., Canada, the UK, France, Israel) to remain economically competitive and geopolitically influential in an international order increasingly shaped by rivalry between the US and China.

Developed countries are at an advantage in this instance. AI adoption is likely to be faster where wages are higher and the economic feasibility of integrating automation occurs earlier. Less developed countries meanwhile are at risk of falling behind in AI development and may end up forced to trade their population's data and market access in exchange for essential AI services, becoming what *The Economist* termed "AI vassal states."<sup>3</sup>

The EU, meanwhile, is attempting to exert itself as a regulatory superpower in the evolution of AI. The multilateral

Countries beyond the US and China Are Investing in and Attempting to Regulate AI		
Country	National AI Strategy	Select Government Funding Initiatives for AI
Canada	✓	Pan-Canadian Artificial Intelligence Strategy (\$93mn)
France	✓	AI for Humanity (\$1.6bn); IA-Clusters (\$523mn)
Germany	✓	Federal Artificial Intelligence Strategy (\$3.2bn)
India	✓	National Strategy for AI (\$944mn)
Israel	✓	N/A
Japan	✓	Included in New Energy and Industrial Technology Development Organization Fund (\$875mn)
Russia	✓	National Strategy for AI Development (\$6.1bn)
Singapore	✓	Included in Services and Digital Economy Program (\$366mn)
South Korea	✓	Artificial Intelligence R&D Strategy (\$1.95bn)
United Arab Emirates	✓	G42 Expansion Fund (\$10bn)
UK	✓	AI Sector Deal (\$1.2bn)

Source: Stanford AI Index 2023, OECD.ai, and government announcements.

body has forged ahead on regulation that aims to replicate the influence its data privacy rules achieved. The General Data Protection Regulation (GDPR) introduced in 2018 has driven the passage of privacy laws in about 120 countries inspired by GDPR. The introduction of regulation relies not on the dynamism of the EU's own commercial AI ecosystem but rather on the enticement of its 450mn-strong potential customer base. There are differing views, however, on the benefits of the EU's regulatory efforts. Recent economic studies have pointed to negative impacts of enhanced privacy rules on the financial performance of companies targeting European consumers.<sup>4</sup> The French government's recent advocacy for slow rolling regulatory efforts to allow the European AI ecosystem time to grow reflects these concerns.

Governments across the board are grappling with the tension between the imperative to develop strong AI capabilities and the need for guardrails that minimize possible harms. Yet, geostrategic competition complicates attempts to respond to this conundrum as countries view slowing down their own AI deployment as a "zero-sum" loss absent guarantees that others will follow this same approach. As a result, most regulatory responses are occurring primarily at the national and local level, while those at the international level are a patchwork of overlapping and competing frameworks from smaller, more politically manageable forums.



## 2. Regulating AI

A total of approximately 120 AI-related bills have been passed globally since 2016, but none are comprehensive frameworks specific to AI. Only a handful of countries are proceeding with comprehensive regulation of the risks posed by the adoption of AI. The EU is, unsurprisingly, leading in this regard. It has forged ahead with its AI Act, now in final negotiations, which bans the highest risk applications of AI (e.g., real-time biometric identification) and imposes testing and reporting requirements for lower risk categories (e.g., spam filters). Brussels’ calculation is in part to establish itself as the regulatory leader on AI and hope to replicate the “Brussels effect” of its data privacy rules which had significant global impact. Critics argue, however, that the EU’s regulation will quickly be out-of-date given the rapid evolution of AI technologies and especially given that it will only come into force in 2026.

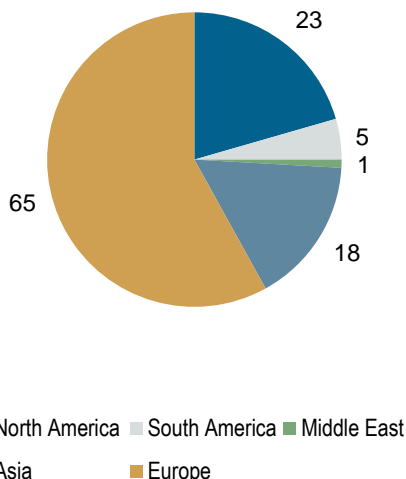
To date, government policy focused on AI and associated parts of the supply chain can be broadly divided into three categories:

- **“Promote” policies** (i.e., R&D funding, flexible immigration policy, manufacturing / other subsidies)
- **“Protect” policies** (i.e., export controls on key inputs, bans on outbound investment in specific AI applications)
- **“Principles” policies** (i.e., domestically focused safety and ethics guidelines to steer AI development)

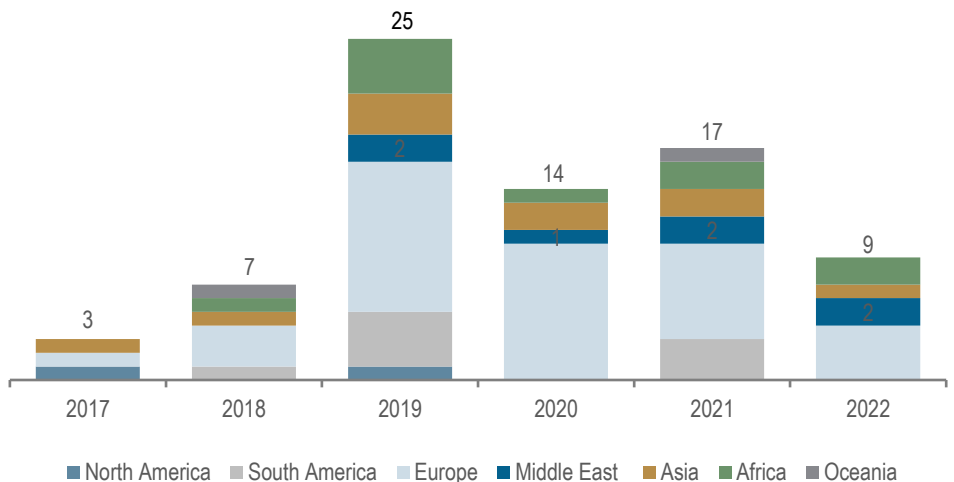
The US has primarily been focused on the first two categories of policy—enacting strong technology industrial policy in areas key to AI development while restricting Chinese access to advanced US technology, managerial expertise, and capital. US “protect” policies have arguably had the most noticeable, and profound, real-world impact. Restricted access to advanced chips has forced China to direct substantial flows of capital, talent, and government bandwidth to technological self-sufficiency efforts. Chinese AI companies have scrambled to stockpile or circumvent the sanctions. Even recent breakthroughs, such as China’s Semiconductor Manufacturing International Corporation (SMIC)’s 7nm chip, still relied on Western machinery—a vulnerability that may be exploited as the Biden administration considers whether to expand the scope of its existing restrictions. It is less clear how successful US industrial policy will be given the challenges of reshoring highly globalized and complex industries like semiconductors.

### Government Emphasis on AI-Related Policy Has Steadily Increased since 2017

Number Of AI-related Bills Passed Into Law (2016-22)



Number Of National AI Strategies Released By Region



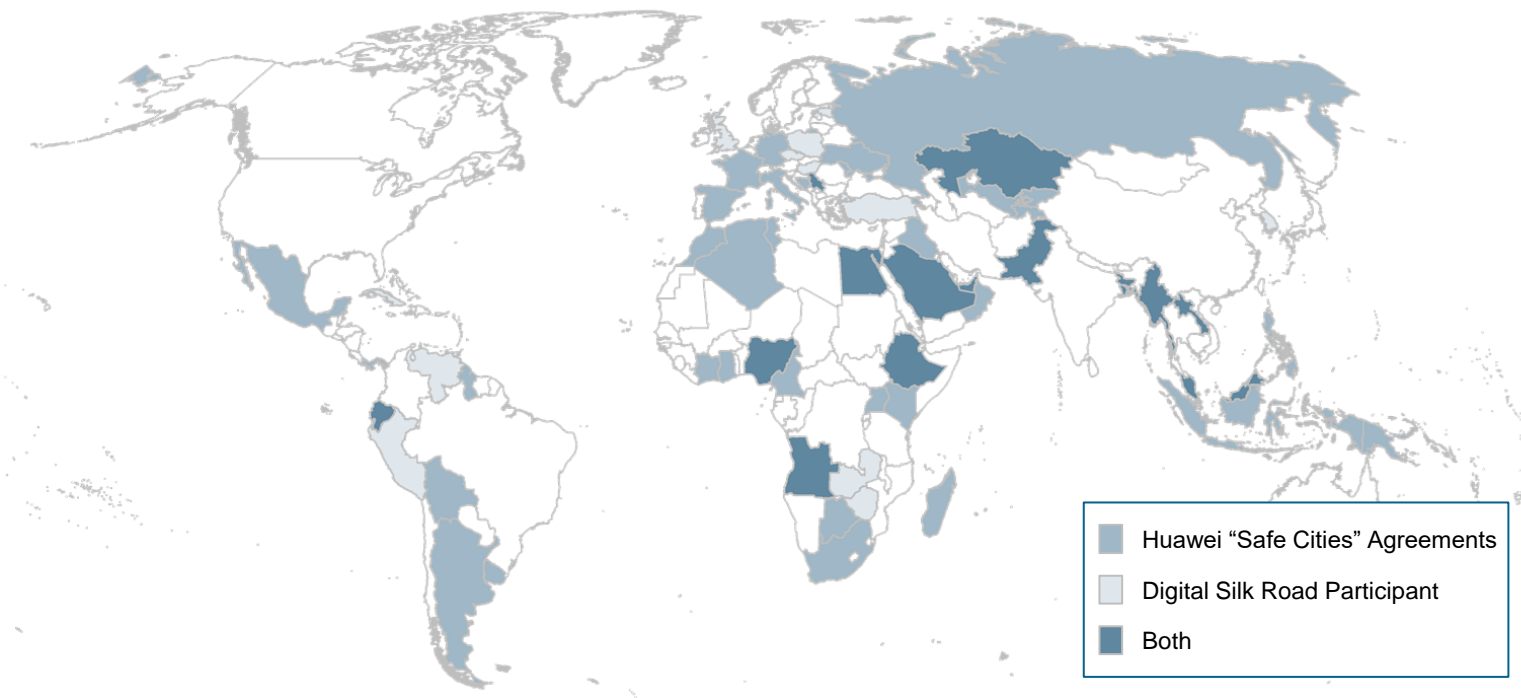
Source: Stanford AI Index 2023

## 2. Regulating AI (cont'd)

Domestic political focus on comprehensive AI regulation in the US has accelerated since the release of OpenAI’s ChatGPT. The Biden administration has made progress on expanding AI “principles” policies via federal agencies and executive power. The National Institute of Standards and Technology produced an AI Risk Management Framework (pre-dating the generative AI boom), while the White House announced an AI Bill of Rights and Voluntary Principles signed by seven leading AI companies. However, recent attempts at legislation (e.g., Senator Schumer’s “Security, Accountability, Foundations, Explainability” innovation framework for AI policy or Senators Warren and Graham’s Digital Consumer Protection Commission Act) have not advanced in a divided Congress. As a result, industrial policy, such as the CHIPS and Science Act, and trade restrictions will likely remain the most used, and effective, tools for the US in AI competition moving forward.

China has been forthcoming with its own AI regulation, including policies on recommendation algorithms and draft rules on generative AI (though focused on corporate uses of AI and data rather than the Chinese government’s). Like the EU, China has also been attempting to export its approach to AI. However, China’s emergent efforts have emphasized its AI-driven surveillance capabilities which have, as of 2019, been sold by Chinese AI companies in at least 73 agreements across 52 countries, especially in emerging economies.<sup>4</sup> This emphasis on “promote” policies with a global dimension has helped cement China’s position in the AI value chain of these emerging markets early on, further bolstered by Digital Silk Road infrastructure projects. Interventions at such early stages in countries’ digital development help to encode Chinese technical standards and establish long-lasting commercial relationships. These ties will likely deepen as the US-China competition intensifies and AI ecosystems gradually bifurcate.

### China’s Involvement in Digital Infrastructure Development Influences Market Access and Technical Standards



Source: CSIS, Council on Foreign Relations.

## 2. Regulating AI (cont'd)

Meanwhile, recent gains in AI capabilities are catalyzing efforts at the international level. The cross-border nature of AI products and the impact that AI development can have beyond the jurisdiction in which it is developed will require governance efforts at the international or intergovernmental level. There are calls for the UN to create a new agency to support collective AI governance efforts based on precedents set by the International Atomic Energy Agency, the International Civil Aviation Organization, or the Intergovernmental Panel on Climate Change.

Japan has been playing a leading role through their initiation of the G7 Hiroshima Process and aims to produce agreement among G7 members on a set of principles for all organizations using and creating AI tools. In October, Prime Minister Kishida announced that a set of guidelines would be agreed by the end of the year and recent reporting indicates that a draft plan, including a code of conduct with voluntary standards on limiting misuse and cybersecurity investments, has been agreed. While only member countries will be party to the initial agreement, it may form the basis for broader international principles moving forward.

The UK, determined to become a “science and technology superpower” post Brexit, is similarly attempting to convene a range of stakeholders for a Global AI summit in November 2023 and internationalize its AI safety efforts. Deliverables under discussion include the creation of a global AI Safety Institute building on the UK’s Frontier AI Taskforce and producing a joint communique on the risks of AI models.

Nevertheless, all the proposals are in their infancy and little exists in concrete terms regarding AI safety implementation, oversight, or certification and licensing. New intergovernmental institutions that could evolve over time include: international agreements on AI use and non-proliferation that would monitor compliance through inspector visits to frontier AI labs (organizations producing advanced large-scale models exceeding the capabilities of existing systems) and controlling AI inputs like computing power; a commission on frontier AI to build scientific consensus on the opportunities and risks from advanced AI; and an international AI collaborative to facilitate legitimate and equitable access to powerful AI.

While these international initiatives evolve and produce multiple sets of overlapping regulations, national-level policies will be the most powerful in promoting and restricting access to AI in the short term.

### 3. Geopolitical Bottlenecks in the AI Value Chain

National-level policies and their impact on the global scramble for AI depend in part on the distribution of structural advantages necessary to power AI development. **Computing power, talent, data, and physical infrastructure are widely recognized as the key building blocks for AI development and adoption.**<sup>6</sup> So far, the US has most prominently deployed its strength in computing power. Yet, the other three factors will also increasingly be weaponized in the AI race.

Building Block	Geopolitical Bottlenecks	Leading Countries	Leading Firms / Organizations
<p><b>Computing Power</b> Chips, and the data center infrastructure they are deployed in, are fundamental to powering model training &amp; inference</p>	High ■■■	US, Taiwan, Japan, South Korea, Netherlands	Semiconductor players (NVIDIA, TSMC, etc.), cloud computing companies (Amazon Web Services, Azure, Google Cloud)
<p><b>Talent</b> The limiting factor across all other key building blocks. The US, India, and Europe have a meaningful head start, but China is catching up</p>	High ■■■	US, China, Europe, India	Universities and research centers, Google DeepMind, OpenAI, Anthropic, etc.
<p><b>Data</b> Data is vital to AI, but its advantage is likely to be constrained to narrow applications</p>	Medium ■■	China, India, US, Indonesia, non-state corporate actors	Leading global technology players (e.g., Meta, Google, ByteDance, Amazon), financial institutions
<p><b>Physical Infrastructure</b> Cheap energy and abundant water resources help determine where data center infrastructure necessary for AI training and inference is built</p>	Low ■	Indonesia, Brazil	Amazon Web Services, Microsoft Azure, Google Cloud, Alibaba Cloud, IBM, Salesforce

### 3. Geopolitical Bottlenecks in the AI Value Chain (cont'd)



#### Computing power

Computing power (or compute) is the engine for both training models and using them in real time to make inferences. Exponential increases in processing power has been a driving force of AI for machine learning systems enabling them to process exponentially larger volumes of data in shorter time frames. Studies have found that increases in computing power were the major driver of AI progress between 2010 and 2018.<sup>6</sup> While recent research has shown that LLMs were previously trained with suboptimal uses of compute and more modest resources might produce similar capabilities, compute remains the most impactful bottleneck for the time being.<sup>7</sup>

The US is well positioned across most of the building blocks of AI, but in computing power especially it can act as a gatekeeper to AI development by controlling access in two key ways: (a) access to advanced semiconductors and (b) access to cloud computing. The US Commerce Department's October 7 2022 export controls package leveraged historical US dominance in the semiconductor sector to restrict China's, as it had Russia's, access to the most advanced chips. Among US chip designers, NVIDIA confers a unique advantage to the US as a result of its broadly-used, proprietary software development platform (known as CUDA) for AI tasks. More broadly, Taiwan, South Korea, the Netherlands, and Japan all play roles in the chip supply chain that grant them outsized influence over access to key AI hardware. Semiconductors are widely recognized as the lifeblood of the modern economy beyond the development of AI. A total of \$620bn in manufacturing subsidies has been announced to that end by the US, Japan, South Korea, EU and others to bolster their semiconductor manufacturing capabilities.

China is also making progress towards semiconductor self-sufficiency in spite of US restrictions. Most recently, China's leading foundry, SMIC, reportedly manufactured chips at the 7nm process node level and is expected to develop its own AI chips over time. Meanwhile, Chinese AI companies, while restricted from purchasing NVIDIA's most advanced chips (the best available chips to handle AI's intensive processing tasks) were, until recently, still able to access slightly lower performance chips and can still use AI-as-a-service through cloud providers.

US companies' dominance in cloud computing and providing AI-as-a-service also places the US in a strong position in controlling access to computing power. The Biden administration is, in fact, exploring closing a perceived loophole in its October export controls relating to cloud providers that continue to provide AI services to geopolitical adversaries. Many of these companies operate globally, including contracts with foreign governments, and will find their client base curtailed and will face stricter know-your-customer provisions in the near future.

US cloud companies' likely outsized role in spreading access to AI across sectors will also present a difficult issue for Brussels. Leveraging these companies to accelerate AI adoption in Europe and reaping the associated economic benefits will exacerbate concerns that Europe has an unhealthy dependency on US technology platforms. This will likely re-invigorate proponents of "digital sovereignty" (a state's ability to regulate digital services and technologies) and more protectionist policies and the promotion of European technology champions.

Meanwhile, developing countries with no role in the semiconductor or cloud computing value chain will struggle without domestic computing power capacity. This will be exacerbated by the increasingly exorbitant costs of computing power. OpenAI's GPT-3 is estimated to cost approximately \$105mn in graphics processing units (GPUs) and electricity costs per training run, and up to \$700,000 a day in computing costs.<sup>7</sup> These costs as well as constrained supply of semiconductor chips (which is reportedly outstripped by demand by a factor of 10) will result in accessibility increasingly restricted to the most well-resourced countries and companies.<sup>8</sup>

### 3. Geopolitical Bottlenecks in the AI Value Chain (cont'd)



#### Talent

Talent is key to keeping algorithms, data, and computing hardware competitive. Historically, countries' success in adapting to revolutionary technologies has been a matter of whether its institutions are organized to widen the base of engineering skills associated with the technology to ensure its diffusion across as many sectors in the economy as possible.

Of all the building blocks of AI, human talent—and the time it takes to develop—is the limiting factor in scaling AI advancement. To date, the US, China, and Europe have the strongest AI research communities. While researchers at Chinese institutions produce the highest number of total AI publications, US and European AI research is regarded as higher quality. US papers are cited roughly 30% more than European papers are and 70% more than Chinese ones. That said, the quality of Chinese research has been improving steadily over time, not to mention the fact that industry analysts suspect that cutting-edge Chinese research is increasingly being kept under wraps.

Middle / great powers also recognize the importance of cultivating talent as a key factor for AI development. Multiple national AI strategies stress the importance of developing their AI workforces: South Korea's AI strategy set a goal of awarding 4,500 AI scholarships by 2022, while the UAE awards 120 AI internships per year for Emirati students. Meanwhile, India already produces 16% of the world's AI talent pool and 12% the "most elite" AI researchers received their undergraduate degrees in India, making it second only to the US.<sup>9</sup> However, most emigrate to the US or Europe for graduate and post-graduate education. Canada, the UK, Israel, and South Korea also perform well in terms of AI talent pipelines.<sup>9</sup>

Importantly, AI talent is highly mobile. One of the US's leading advantages is that it is home to the highest-quality research universities and institutions, as well as a highly attractive labor market. More than half of Chinese undergraduates studying AI left for the US, of which 90% chose to stay and work in the US after graduation since 2005.<sup>10</sup> The trajectory of US-China scientific cooperation, and immigration policy for highly skilled workers from China, could increasingly become politicized and restrict US access to a broad pool of international talent. Middle / great powers could also narrow US access to talent by increasingly drawing STEM graduates away from the US through more generous immigration policies

China's response has been to try to attract back highly skilled talent that can translate key US or Western IP into technological advances in China. An undergraduate AI major is now offered at 440 Chinese universities, all approved by China's Ministry of Education.<sup>11</sup> Since 2008, the state-sponsored "Thousand Talents" program has focused on recruiting Chinese and non-Chinese experts and academics ostensibly to promote international cooperation on science, but is instead strategically focused on filling key gaps in China's technological capabilities. The "Thousand Talents" program is thought to contribute to "informal" technology transfers.

In the semiconductor sector, there have been cases of explicit theft of high-value IP as well as tacit knowledge transfers through the poaching of star engineers. Chinese chip design firms are reportedly willing to pay Taiwanese engineers 500% of their salaries in Taiwan if they relocate to mainland China to work for Chinese firms.<sup>12</sup> Poaching of top employees and intensifying corporate espionage will become more prevalent risks for companies across the AI value chain in the near-to-medium term.

### 3. Geopolitical Bottlenecks in the AI Value Chain (cont'd)



#### Data

Data is a key input for AI applications across the board because of its importance in training more accurate algorithms. Typically, the greater the volume and relevance of training data, the higher the effectiveness of the machine learning system. Companies are faced with the technical and organizational questions of how best to collect, organize, store, and make accessible data for AI training. Legal and regulatory hurdles—especially around privacy—add another layer of complexity which constrain the assembly of large datasets.

Much is made of China’s “data advantage.” This “advantage” is drawn from the large troves of data collected on China’s large and highly digitized population with relatively few regulatory restrictions on data protection. The Chinese government has classified data as the “sixth factor of production” and attempted to create operational data trading exchanges. Importantly, however, data is not fungible across applications and so large data assets may be more useful for certain AI applications (e.g., facial recognition) over others (e.g., military AI). In general, countries are increasingly aware of the national security and economic value of data, especially as it relates to AI. As a result, countries are attempting to ensure control over data produced within their borders and enacting policies that reflect data nationalism and data sovereignty trends.

The EU’s emphasis on “digital sovereignty,” a concept promoted especially by French President Emmanuel Macron, has provided momentum for a raft of data governance policies designed to take advantage of the vast data collection occurring across the bloc. The recently passed Data Governance Act encourages companies to pool and share data in sector-specific “data spaces.” Meanwhile, India, Saudi Arabia, Indonesia, and others have been accelerating efforts to assert their sovereignty over data produced by their citizens. Between 2017 and 2021, the number of laws, regulations, and government policies that require digital information to be stored in a specific country more than doubled to 144.<sup>15</sup> India has been especially vocal about so-called “data colonialism,” the extractive appropriation of big data in developing countries, where the volume of data harvested from users is least reflected in the quantum of investment in digital infrastructure by those monetizing that data. New Delhi used its G20 Presidency to secure consensus on a “G20 Framework for Systems of Digital Public Infrastructure”. The Framework encourages the development of data and digital infrastructure built by the public and private sectors as a public good.

In 2022, to meet increasing customer demand, Microsoft announced a product custom built to meet governments’ national security and privacy concerns by including data localization options. Other cloud providers quickly followed suit. Data localization is an imperfect tool for improving privacy and security of data. It is also not necessary to conduct AI training or inference through local data centers. However, these regulations have forced foreign cloud providers to invest in local data infrastructure, thus beginning to reduce countries’ reliance on others such as the US and China and possible leverage in the event of a geopolitical dispute. Nevertheless, such infrastructure investments are likely only worthwhile for larger emerging markets such as India and Indonesia, leaving smaller countries attempting to leverage their data resources for AI development further behind the curve.

### 3. Geopolitical Bottlenecks in the AI Value Chain (cont'd)



#### Physical infrastructure

The environmental footprint of cloud providers' data center infrastructure is increasingly a determinant of where data centers are built and where computing power is made available for AI development and especially for state-of-the-art models. For countries anxious to ensure self-sufficiency in a key factor of the AI value chain (computing power), their energy and water resources will become important variables in the economic and political viability of building data centers domestically.

The global electricity consumption footprint of computing is projected to reach up to 21% by 2030 up from 1% to 2% in 2018. Generative AI models in particular consume exponentially higher amounts of energy especially in the model training stages. A typical large AI model consumes between 100-200 MWh of energy during training (10-20 times the yearly usage of an average single-family home in the United States) while ChatGPT by some estimates is thought to consume as much electricity as a mid-size city of 175,000 people on a monthly basis.<sup>14,15</sup> Projected uses of computational AI will require unprecedented deployment of new digital infrastructure reaching up to tens of gigawatts in energy demand while energy supply chains are dramatically transforming to enable decarbonization. The energy-intensive nature of AI will therefore link it indirectly to global energy dynamics and put it at odds with decarbonization goals central to the agenda of many advanced economies. The energy demands of data centers are already prompting issues at the local level as power outages caused by overwhelmed grids have disrupted local communities. The disparity between capacity and resiliency expectations for servers and existing renewables capacity will drive cloud providers to use more hydrocarbon-based energy sources to meet exponential AI-driven demand.

The cooling mechanisms inside data centers also consume staggering volumes of water. Training GPT 3 in Microsoft's state-of-the-art US data centers directly consumes 700,000 liters of clean freshwater over one training run (a process which takes several weeks), a figure that would have tripled if training were done in Microsoft's data centers in Asia where cooling tower efficiency and uses of recycled water are not as advanced.<sup>16</sup> As a result, access to water will also constrain countries' ability to attract investments in their digital infrastructure, especially in the context of ESG commitments made by major cloud providers (e.g., most US cloud providers have pledged to be powered by 100% renewable energy by 2030 and to use less freshwater). As emerging economies struggle to make themselves attractive destinations for digital infrastructure investment, this could re-invigorate momentum for data localization policies which would force the building of local data centers, ostensibly for data security and national security reasons, but in reality designed to boost self-reliance in computing power.

The physical data center infrastructure and associated environmental resources are in the earliest stages of importance as geopolitical bottlenecks that could impact countries' ability to develop AI. These constraints may not become significant until more mature stages of development when the costs of building out a domestic AI sector powered by local resources become a substantial burden to less wealthy governments.



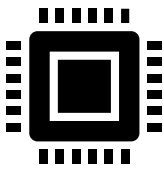

## 4. Business Implications

As the US and China solidify their leads in AI and tighten control over the inputs necessary for its development, companies will find themselves torn between diverging regulatory and commercial approaches for AI. Globalized business models will be under fire as governments increasingly assert the importance of geopolitical and ideological alignment in the sale of AI services. Companies operating in this area, either as fundamental enabling cogs in the AI supply chain or as industries set to be significantly disrupted by the rise of AI, will face several critical strategic considerations.





First, as the global AI marketplace fragments in response to geopolitical competition, businesses will face restrictions on their global customer bases. Ongoing operational and commercial ties to China will attract political / regulatory scrutiny in the US / Europe. Depending on a company’s importance within the AI value chain, policies such as export controls, investment screening, tariffs, sanctions, and subsidies will be deployed by the US or China against strategically important firms. These will involve restrictions on which companies and countries one can do business with or invest in. It is worth considering how one’s global customer base would be restricted according to geopolitical alignment and begin mitigating any existing dependency on government contracts in markets that might jeopardize revenue elsewhere.

Second, strategically important companies in the AI value chain will likely face intensified corporate espionage. Companies in this position should consider what mitigation methods are available across a number of attack vectors, including talent poaching, cyber espionage, and explicit knowledge transfers required by regulation.

Finally, while US-China competition will likely add to companies’ compliance burdens, it will also create opportunities in third-country markets. As US and Chinese companies are increasingly restricted from buying and selling to one another, third countries that are either well positioned to support AI development or primed for AI adoption could provide opportunities for expansion. It is worth looking beyond the US and China to assess which other countries will have advantages across each of the AI bottlenecks. Companies should also consider which countries have existing strong ties to Beijing or digital infrastructure built via the Digital Silk Road that make them less viable, or more siloed, alternative markets.

Sector / Industry	Possible Implications / Considerations
 <p><b>Semiconductor &amp; related equipment</b></p>	<ul style="list-style-type: none"> <li>• Additional tightening of existing export restrictions and tightening of any perceived loopholes allowing China to advance in AI development</li> <li>• Ongoing government support via subsidies, though with strings attached (e.g., restrictions on greenfield investments / capacity expansion in China)</li> <li>• Rising costs of doing business as a result of reshoring to more developed economies with higher talent and energy costs</li> <li>• Intensifying and possibly state-sponsored corporate espionage against highest-value IP (e.g., advanced tooling, design, packaging)</li> </ul>
 <p><b>Cloud computing, data centers</b></p>	<ul style="list-style-type: none"> <li>• Governments may curtail total addressable market and require burdensome “know-your-customer” framework (similar to financial services)</li> <li>• Rise in popularity of “sovereign cloud” products</li> <li>• Increasing protectionist pressure to build data centers in-country and enter JVs with local industry players</li> <li>• Push to cordon off discounted computing power for national research institutions / non-profit community</li> </ul>

## 4. Business Implications (cont'd)

Sector / Industry	Possible Implications / Considerations
 <p><b>Infrastructure software</b></p>	<ul style="list-style-type: none"> <li>• AI-enabled tools to bolster cybersecurity will receive huge investment as AI will also empower cybercriminals by lowering barriers to entry (e.g., automated malicious code, convincing phishing, etc.)</li> <li>• Infrastructure software will become necessary for managing the different data governance regimes across markets</li> </ul>
 <p><b>Pharmaceuticals</b></p>	<ul style="list-style-type: none"> <li>• Export controls on biotechnology enhanced by AI with possible dual-uses, including synthetic biology and genome editing, with the potential to be repurposed to develop synthetic or bioengineered viruses, chemical weapons, and toxic compounds</li> <li>• Stringent safety standards for biotech models, including pre-release evaluations, localized biological, genomic, and clinical trial datasets, as well as restrictions on the sources of computing power, and cybersecurity requirements</li> <li>• Restrictions on international transfer of digital biological data for use in training AI models (e.g., genomic data, cell data, clinical test data, epidemiological data)</li> <li>• Human capital restrictions for research projects on essential / cutting-edge treatments</li> </ul>
 <p><b>Financial services</b></p>	<ul style="list-style-type: none"> <li>• Additional government mandated consumer safety and anti-discrimination measures for AI deployed for sensitive applications with human impacts (e.g., loan / credit rating decisions, roboadvisors)</li> <li>• Macroprudential policies to reduce tail risks of AI-driven instability in financial systems (e.g., AI causing market crash)</li> <li>• Higher costs to deploy AI-driven tools to combat exponentially higher fraud activity given increased scalability of scams</li> <li>• May be required to source computing power locally (i.e., through domestically located data centers) to increase security around sensitive payments / transaction / other data</li> </ul>
 <p><b>Energy</b></p>	<ul style="list-style-type: none"> <li>• Unprecedented deployment of new digital infrastructure will outpace renewables capacity and drive greater consumption of hydrocarbon-based energy sources</li> <li>• Overburdening of local energy resources required for AI training and deployment will increasingly spark political backlash and regulatory scrutiny for energy security and / or environmental justice reasons</li> <li>• Increased cybersecurity costs to secure critical digital infrastructure as cheaper, reliable power may be in jurisdictions with lower security standards</li> </ul>

## 5. Looking Ahead

As companies and countries compete for the political, economic, and military benefits of AI, much remains uncertain about who will come out ahead and how long that may take. While the US leads comfortably in most of the key building blocks of AI, recent Chinese breakthroughs in semiconductor technologies have bolstered prospects for their technology self-sufficiency goals.

Much will depend on how the US chooses to respond. Investing in R&D, developing new industrial policy, coordinating with like-minded allies and partners, tightening loopholes or expanding the scope of export restrictions could all influence both China's path forward and the global order around it. As of October 2023, the US administration's initial reaction to China's breakthrough at the 7nm process node has been to respond cautiously by tightening existing restrictions while signaling possible additional actions on the horizon.

Meanwhile, the EU will measure its success by the influence of its upcoming AI Act beyond its own borders. The AI Act will also be judged by whether it supports the EU's "digital sovereignty" aspirations or undermines them. The tension between the need for a dynamic current AI ecosystem and Europe's dependency on large US technology platforms will continue to complicate successful AI development for EU policymakers.

Competition will continue to play out across the four bottlenecks in the AI supply chain. At first, computing power and talent will remain the primary domains of activity in AI competition. Many policymakers are broadly aware of the importance of computing power, especially since the October 7 semiconductor export controls and subsequent refining of rules a year later. The cloud computing sector will likely be the next in the crosshairs from the US which is considering restrictions on AI-as-a-service tools and has asked for public comment on introducing "know-your-customer" provisions for cloud providers. Other AI contenders seeking self-sufficiency in a key building block of AI will similarly consider their strategic interest in the cloud computing sector. While more sensitive, talent and related scientific cooperation and immigration policy will also become more prominent subjects of debate. The US-China 1979 Science and Technology Cooperation Agreement is facing increasing opposition, while the Netherlands is considering legislation to screen foreign Ph.D. students who plan to study in technical fields with national security implications. The impact of data and infrastructure on AI development will unfold more gradually and less conspicuously but will similarly influence which countries are able to monetize their data resources and build self-sufficient AI supply chains.

This period will also be one of maximum risk. In the absence of internationally agreed rules and regulation, practical norms will be figured out in the course of real-life use. Conflicts will be proxy technological testing grounds pitting US, Chinese, Russian, and other players' military AIs against each other - a phenomenon already underway in the Russia-Ukraine war. This poses severe risks relating to AI catastrophes spiraling out of control (e.g., release of an AI-identified bioweapon, or an AI-enabled cyberstrike, etc.).

In the weeks and months ahead, there will be multiple signposts of progress on AI regulation as well as indicators of which countries are best deploying their structural advantages to get ahead in the AI race. Navigating the geopolitical dynamics impacting AI development will require close attention to the progress of international cooperation efforts on AI such as the outcomes of the upcoming British AI Summit in early November and a finalized G7 code of conduct, Chinese success in technological self-sufficiency efforts including semiconductor breakthroughs such as the erosion of NVIDIA's software capabilities, rising AI stars in technological ecosystems outside the US and China, and third countries' choices about alignment with the US or China, among other factors.

## Disclaimer

These materials have been prepared by Lazard for general informational purposes only, and they are not intended to be, and should not be construed as, financial, legal, or other advice.

In preparing these materials, Lazard has assumed and relied upon the accuracy and completeness of any publicly available information and of any other information made available to Lazard by any third parties, and Lazard has not assumed any responsibility for any independent verification of any of such information. These materials are based upon economic, monetary, market, and other conditions as in effect on, and the information available to Lazard as of, the date hereof, unless indicated otherwise. Subsequent developments may affect the information set out in this document, and Lazard assumes no responsibility for updating or revising these materials.

These materials may include certain statements regarding future conditions and events. These statements and the conditions and events they describe are inherently subject to uncertainty, and there can be no assurance that any of the future conditions or events described in these materials will be realized. In fact, actual future conditions and events may differ materially from what is described in these materials. Lazard assumes no responsibility for the realization (or lack of realization) of any future conditions or events described in these materials.

Nothing herein shall constitute a commitment or undertaking on the part of Lazard to provide any service. Lazard shall have no duties or obligations to you in respect of these materials or other advice provided to you, except to the extent specifically set forth in an engagement or other written agreement, if any, that is entered into by Lazard and you.