The Technopolar World:
Do Tech Companies Matter as Geopolitical Actors?

By: Eliana Aiken, Peyton Allen, Alice Baudin, Jared Finkel, Emma Fischer, Lauren Goldberg, Jazilah Salam, Randall Schmollinger

Columbia University, SIPA, Capstone Project

May 16, 2025

Table of Contents

Key Insights

- In the geopolitical landscape, technology companies can take three main roles – objects, arenas, and actors – each reflecting a varying degree of agency wielded by the company. Hence, we conclude that firms can still shape world affairs even without acting deliberately.

- Given certain enabling conditions related to the firm's profile and its relationships with governments, tech companies can behave as geopolitical actors. Nonetheless, their ability to do so is inherently subject to the domestic regulations under which they operate and constrained by foreign governance structures. In other words, certain tech companies *can* behave as geopolitical actors if they *choose* to do so until governments decide otherwise.

- We predict that, in the long run, tech companies will be compelled to cede their geopolitical agency to states with the regulatory leverage to preserve state primacy in global affairs. In other words, the balance of power between states and tech companies will remain tilted in favor of states, making a technopolar world unlikely.

Introduction

On January 20, 2025, Donald Trump was inaugurated for his second term as President of the United States. The ceremony was attended by members of the Trump family, Congressional representatives, and cabinet nominees.[1] The closed-door event required a $1 million donation from participants. Seated directly behind the President were billionaire CEOs of the tech companies Meta, Amazon, X, Google, Apple, and TikTok.[2] This show of financial and political support raises critical questions about the emerging dynamics between tech companies and the state.

Large tech companies in the U.S. and China have grown at an unprecedented scale, surpassing most nation-states' gross domestic product and populations in terms of market value and user reach, respectively.[3] Tech companies are characterized by three main product types: digital infrastructure, data, and platforms. Their ownership and operation of networks, data, and algorithms have made them key players in contemporary societies. They have aided war efforts, such as SpaceX's provision of telecommunication infrastructure to support Ukraine against Russia's invasion; they have facilitated public movements, like the Arab Spring; and they have been banned by countries in the name of national security, such as TikTok and Meta. While their implications in world events span a broad spectrum, they are undeniably present in global affairs.

Tech companies are constrained by regulatory environments that shape their capacities and abilities to operate, determining the roles they play in global affairs. Anu Bradford, Columbia Law professor and author of *Digital Empires: The Global Battle to Regulate Technology*, outlines three dominant regulatory models: the U.S. (market-driven), China (state-driven), and the

European Union (rights-driven).[4] In the U.S., minimal government interference is exemplified by Section 230 of the Communications Decency Act of 1996, which shields platforms from liability for user-generated content, giving them the freedom to manage how their platforms are used. On the other hand, China's regulatory model emphasizes state control, requiring tech companies to implement surveillance and censorship in line with the Chinese Community Party's policies. In contrast, Europe's regulatory approach prioritizes the protection of rights and democratic values, ensuring that technological innovations comply with these principles first.[5] The ability of tech companies to act in geopolitics is dictated by their capacity to make independent choices under domestic and foreign governance structures. Domestic regulation can also compel a company to behave under specific guidelines internationally through trade regulations and laws such as import controls and sanctions. Furthermore, while foreign governments do have the ability to constrain tech companies, this depends on the country and its respective characteristics, such as its economic wealth or population size. Given that the largest tech companies are in the U.S. and China, the scope of this paper will focus on the regulatory models in these two respective nations.

Due to governance structures, tech companies are limited in the roles they can take on in geopolitics. They can become proxies of state interest, provide an infrastructural role, or take on an active role in geopolitics – sometimes even going against the foreign policy objectives of their domestic governments. Beyond the regulatory environments, tech companies' ability to exert agency is determined by company-specific variables, from their ownership of advanced technology to their national security link and ownership structure. Together, these enabling conditions define tech companies' geopolitical agency trajectory over time.

This report attempts to answer the following research question: "The Technopolar World: Do Tech Companies Matter as Geopolitical Actors?" We address this question in three sections:

- **Section I** presents a conceptual framework for understanding the various roles tech companies can play in the geopolitical landscape. Both contemporary examples of tech companies and historical comparisons of oil and financial giants are provided to illustrate the framework and assess the novelty of tech companies' presence on the international scene.

- **Section II** delves into the variables that determine a company's geopolitical action potential, namely a company's firm profile and its respective relationships with domestic and foreign governments. First, an empirical analysis serves to identify patterns and relationships between the variables. Then, the empirical analysis is used to develop a scoring index that quantifies a tech company's geopolitical action potential.

- **Section III** builds on the conceptual framework and scoring index to map U.S. and Chinese tech companies' trajectory of geopolitical agency over time. These trajectories inform our base case scenario on the balance of power between tech companies and governments.

Definitions

To ensure clarity and consistency, we define the following key terms to underpin our discussion of tech companies and geopolitics.

Agency: The capacity and willingness of an actor to independently make choices, implying freedom and control over one's actions.[6]

Tech Company: Tech companies have a massive global footprint and have dominated the industry for years in terms of size, influence, and financial success. They are known for amassing and processing vast amounts of data. Additionally, they are distinguished by their innovative use of cutting-edge technologies like AI and cloud computing. The term "Big Tech" often refers to the "Big Five," Amazon, Apple, Facebook (Meta), Google (Alphabet), and Microsoft, as well as other large tech firms such as Alibaba, Tencent, Huawei, and Tesla.[7]

Geopolitics: Geopolitics involves three qualities. First, it is concerned with questions of influence and power over space and territory. Second, it uses geographical boundaries, often of states, to make sense of world affairs. Third, it includes an interstate component. Geopolitical actors are those who exert agency in each of these three spheres.

Influence: Influence refers to the ability to manipulate the environment to achieve a desired outcome. It is an actor's exertion of power to achieve a specific outcome. It is predicated by the necessary presence of power and is activated by intentions and motivations to make an impact.[8]

Non-State Actor: Organizations that are not formally governmental or intergovernmental actors. This includes organizations with ties to the government. NSAs must be actors in the sense that they can plausibly exert agency.[9]

Power: In its classic relational sense, power is the capacity of one actor (A) to get another actor (B) to do something B would not otherwise do.[10]

Sovereignty: The ability of a state to make and enforce a regulatory structure within a territory.[11]

Section I. Agency Framework: What Roles Do Tech Companies Play in Global Affairs?

Insight 1: In the geopolitical sphere, tech companies can take three main roles – objects, arenas, and/or actors. Tech companies can matter in geopolitics even if they do not exert agency as an actor.

The Agency Framework sheds light on the various roles tech companies can play in global affairs, demystifying the belief that when tech companies are involved or named in geopolitical issues, they necessarily behave as actors pursuing geopolitical interests. These roles can be defined under three larger umbrella terms: "objects," "arenas," and "actors," capturing different levels of geopolitical saliency. These terms are not mutually exclusive and often overlap as the underlying case studies used for illustration are context-dependent. Historical comparisons of private companies are provided to assess the novelty of private sector presence on the international scene.

Tech companies can take on three roles in geopolitics:

- As an **object**, tech companies are targets of geopolitical competition between state and non-state actors because of the instruments of power they possess. In this role, someone else is exerting agency *on* the tech company, which then, *de facto*, becomes entangled in interstate affairs.
- As an **arena**, tech companies play an infrastructural role through the services they provide. State and non-state actors utilize tech products to serve their domestic and foreign policy interests. In this role, state and non-state actors exert their agency *through* the tech company.
- As an **actor,** tech companies exert *their own* agency on geopolitical issues through their services and products.

Each role will be presented with three contemporary examples from technology companies and one historical example from other large companies with the aim of identifying similarities and differences.

i. Tech Companies as "Objects" of Geopolitics

As *objects,* tech companies are caught in interstate rivalries and either targeted as strategic assets that bolster states' national power or as vulnerabilities to be exploited by adversaries. In such cases, states utilize tech companies to serve their geopolitical interests. Tech companies are used as strategic assets that can be moved and banned by governments irrespective of the tech companies' will. There is also a historical precedent of large private sector companies being seen as *objects* of state interest, a common role that companies continue to play in global affairs. This subsection presents contemporary cases of Chinese and U.S. tech companies being subject to bans, forced divestitures, tariffs, and data-flow restrictions, as well as the historical case of the Seven

Sisters, whose Gulf oil concessions were seized and repurposed by OAPEC during the 1973 Arab Israeli War.

The Ban of Chinese Companies by Geopolitical Adversaries

TikTok, a social media platform owned by the Chinese firm ByteDance, has repeatedly faced scrutiny and threats of being banned in the U.S. due to concerns that the Chinese government could access American user data on the platform. At the start of his second presidential term, President Trump issued an executive order threatening to prohibit the use of the app unless ByteDance dilutes its shares of its U.S. operations to non-Chinese entities.[12] Trump's initial decision to ban the platform was met with unfavorable public reception. The administration has since extended the buyout deadline multiple times, initially by 75 days and then by 90.[13] Since then, the Trump administration has implemented tariffs on Chinese goods, stating that a TikTok deal negotiation would go a long way toward reducing the tariffs.[14] This is a prime example of how a tech company is used as a bargaining chip or an *object* in geopolitics. This phenomenon is not specific to the relationship between the U.S. and China. Similar measures have emerged worldwide – from India's nationwide ban on device-only restrictions across Europe – motivated by the concern that, under Chinese law, TikTok may be compelled to share user data with the Chinese government and align its content policies with Chinese authorities.[15] Similarly, the Chinese government has enacted the Great Chinese Firewall, which blocks U.S. companies like Facebook and Microsoft from functioning in the country.[16]

ZTE and Huawei, Chinese digital infrastructure companies, are also treated as objects of geopolitics, primarily because they serve as key facilitators of China's Belt and Road Initiative (BRI),[17] which involves rolling out telecommunications networks and digital infrastructure across numerous countries. Their prominence in expanding Beijing's technological footprint has, however, led other governments – particularly in the U.S., the UK, and India – to ban or heavily restrict their 5G and networking equipment on grounds of national security. As a result, these two Chinese companies are targets of international technology regulations. They are perceived as proponents of China's global ambitions under the BRI, attracting foreign scrutiny from those wary of Beijing's potential surveillance and cybersecurity threats.

The Courting of TSMC by Taiwan and Allies

Taiwan Semiconductor Manufacturing Company's (TSMC) status as a linchpin of Taiwan's national defense highlights its critical role in global power dynamics. Often referred to as the island's "silicon shield," TSMC's semiconductor manufacturing capabilities have motivated the U.S. and its allies to support Taiwan's autonomy actively as they seek TSMC's advanced chips for their own technological and military needs.[18] Meanwhile, the Taiwanese government maintains a significant ownership stake, viewing TSMC not merely as a commercial enterprise but as a strategic asset to be safeguarded. This shared understanding – that TSMC's survival is intertwined with Taiwan's security – positions the company as a vital resource in the eyes of foreign governments, who vie to secure TSMC's favor and investment. In doing so, they bolster Taiwan's

broader defense posture, turning TSMC into both an object of external strategic courtship and a guarantor of the island's continued safety.

The Leveraging of American Tech Companies by Russia and the EU

American social media platforms have also been utilized as tools within larger state-led strategies to secure national interests and control the digital space. During the Russian invasion of Ukraine, the Russian government escalated its targeting of Western platforms by designating Meta as a "terrorist" organization and imposing bans on several U.S. technology services, aiming to control its domestic information environment and counter external pressures.[19] By banning American platforms for allegedly spreading anti-Russian sentiment, Moscow not only exerted indirect pressure on the U.S. government but also tightened domestic information control by limiting citizens' ability to share content.

More recently, as part of the ongoing global trade war triggered by President Trump's April 2, 2025, "Liberation Day" tariffs, the EU has threatened digital-advertising levies on major U.S. tech firms, including Meta, Google, and Amazon, as a bargaining chip. The EU Commission President, Ursula von der Leyen, warned that "the EU could tax Big Tech if Trump's trade talks fail," signaling that American companies are being used as negotiating chips to restore normal transatlantic trade and secure the rollback of the 20 percent duties on European exports.[20]

Historical Comparison: OAPEC, Nationalization, & the Embargo

In response to U.S. support for Israel at the onset of the 1973 Arab-Israeli War, Iraqi Oil Minister Sa'dun Hammadi demanded the "total nationalization" of all assets of American oil companies in the Middle East, the withdrawal of all Arab funds from the United States, and for all Arab states to break diplomatic relations with the United States.[21] Following this push for the nationalization of American oil interests, the Organization of Arab Petroleum Exporting Countries (OAPEC) initiated a nationalization and embargo campaign against many countries that were seen as supportive of Israel during the war, including the United States. The campaign was designed to punish oil companies operating within those countries in the hopes that the respective oil companies would be compelled to pressure their home countries to reverse policy on Israel. In effect, the OAPEC countries used the oil companies to wage economic warfare against Israeli allies such as the U.S.[22]

As objects caught in geopolitical rivalries, tech companies alike are increasingly targeted by state-led bans, ownership pressures, and regulatory constraints, underscoring their strategic importance in global affairs. This is similar to the early example of state-led corporate capture by OAPEC, where private actors were targeted by states for the resources they owned, and their assets were seized to extract political concessions without the use of military force.[23] In these cases, states are exercising geopolitical agency on tech companies; the companies themselves do not act as geopolitical players but are used as geopolitical objects.

However, they matter in geopolitics because states intentionally leverage tech companies' instruments of power on the international stage.

ii. Tech Companies as "Arenas" of Geopolitics

The classification of a tech company as an *arena* indicates a higher level of influence than that of a passive *object*; in this case, other actors exert their agency *through* the platforms provided by the tech companies. Ownership and control of critical infrastructure, such as social media platforms, data centers, and algorithmic systems, grant tech companies a form of structural agency, often exercised indirectly, through the systems they design and maintain. Social media platforms exemplify this dynamic. Both state and non-state actors have leveraged their user-maximization models to influence social movements, sway elections, disrupt regimes, and shape conflicts. The infrastructural power of today's tech companies parallels that of financial institutions like J.P. Morgan in the Gilded Age, when network control over capital flows was essential to economic development. However, the digital infrastructure offered by tech companies, through app stores, search engines, and cloud computing, enables control over both the flow of information and economic transactions. Unlike the relatively bounded and regulated financial infrastructure of the nineteenth century, tech companies' influence is also augmented by their unprecedented speed, global reach, and deep integration into the daily behaviors, social interactions, and personal data of billions of users.

Digital Infrastructure & Society: The 2011 Arab Spring

One of the earliest and most notable examples of the geopolitical impact of social media was during the 2011 Arab Spring. In the nascent phases of social media, platforms like Facebook and Twitter served as critical arenas for organizing protests and disseminating information.[24] Their popularity surged in the Middle East, particularly in countries under authoritarian rule, where they were used for political organizing and mobilization.[25] Unlike traditional local media, which authoritarian regimes could tightly control, social media allowed for decentralized information sharing, helping to mobilize mass demonstrations. These platforms provided a young and digitally connected population with a forum to coordinate and spread dissent.

In the aftermath of the Arab Spring, many authoritarian governments responded by tightening digital regulations, implementing internet shutdowns, ramping up surveillance, and pressuring platforms to engage in stricter content moderation in an effort to reassert control over their populations and their communications.[26] The Arab Spring not only marked a watershed moment in grassroots digital mobilization but also signaled the rise of social media platforms as *arenas* where geopolitical change is exercised and contested.

Digital Infrastructure & Election Interference: 2016 U.S. Elections

In the 2010s, state-sponsored propaganda, disinformation campaigns, and online influence operations became increasingly prevalent. Authoritarian regimes, for example, have been observed deploying troll armies, amplifying state-controlled narratives, and manipulating algorithms to

shape domestic and international discourse. During the 2016 U.S. election, Russia launched a wide-ranging digital interference campaign aimed at influencing American voters, as revealed by the Mueller Report. The Russian Internet Research Agency (IRA) built a vast disinformation network using fake social media accounts, reaching an estimated 126 million Facebook users and engaging millions more via Twitter and Instagram.[27] These accounts spread propaganda, amplified content through bots, and ran targeted ads.[28] The Russian campaign against U.S. elections highlighted the vulnerability of open social media platforms to foreign influence and marked a turning point in state and public recognition of digital infrastructure as a critical arena for democratic manipulation.

Digital Infrastructure & War: 2022 Russian Invasion of Ukraine

Since Russia's 2022 invasion of Ukraine, social media companies have emerged as an information battlefield on digital platforms. Often referred to as the first "social media war," Ukraine and Russia have leveraged Western platforms to maintain a moral high ground by spreading viral videos, real-time battlefield updates, and official government messaging.[29] Although major tech companies such as Facebook, Google, TikTok, and YouTube have taken active steps to combat known Russian propaganda through content moderation policies and de-platforming known Russian disinformation networks, Russia continues to run covert operations on these platforms while restricting its own population to Vkontakte and Yandex, domestic tech companies supporting Russia's information ecosphere.[30] Looking ahead, the rise of generative AI adds another layer to this landscape, making it even easier to produce realistic deep fakes and synthetic propaganda at scale.[31] While strategic propaganda campaigns are not new to warfare, the shift toward social media as the primary distribution channel is transforming how information warfare is waged, turning platforms designed initially for commerce and entertainment into key instruments of modern geopolitics.

Historical Comparison: J.P. Morgan & The "Gilded Age"

During the "Gilded Age" (approximately 1865-1902), an era of rapid industrialization and economic expansion, powerful business magnates emerged to control critical industries, including oil, steel, railroads, and finance. Figures like John D. Rockefeller, Andrew Carnegie, and J.P. Morgan wielded significant power, often blurring the lines between private enterprise and public interest.[32] Just as President Trump finds himself surrounded by CEOs such as Elon Musk, Mark Zuckerberg, Jeff Bezos, Tim Cook, and Sundar Pichai, then-President McKinley was similarly surrounded by leading industrialists of his time. J.P. Morgan stood out for providing an intangible yet vital form of infrastructural service – credit and financial intermediation – akin to today's tech companies that offer digital platforms, data flows, and cloud services.

Much like modern tech companies that transcend national borders, Morgan's banking empire operated on a global scale with minimal constraints by providing intangible services deeply embedded within economic and social systems. Morgan's company was a critical piece of financial infrastructure in the absence of a central bank. In fact, J.P. Morgan bailed out the U.S. Treasury in

the depression of the mid-1890s, saving the gold standard by selling bonds in exchange for gold in Europe.[33] Additionally, it ended the Panic of 1907 – a U.S. banking and stock-market collapse triggered by a failed attempt to corner United Copper, which sparked widespread runs on New York trust companies – by acting as lender-of-last-resort.[34] Similarly, technology platforms are indispensable infrastructure in digital commerce and communication, controlling the flow of information and transactions through app stores, search engines, and cloud computing services. These tech companies serve as surveillance intermediaries and quasi-regulators of speech and maintain influential ties with the government through lobbying and policy advising. The public perception of these companies is also reflected in each era: the Gilded Age's "robber barons" are mirrored today in the "techlash" against monopolistic practices and privacy intrusions, triggering regulatory backlash and antitrust scrutiny.[35]

However, essential differences distinguish the power of tech companies from that of J.P. Morgan during the Gilded Age. A tech company's influence is characterized by unprecedented speed, scale, and scope. Beyond J.P. Morgan's financial leverage, tech companies exercise a unique form of influence through control over digital platforms that shape public opinion, electoral processes, and even policy debates.[36] Hence, the stakes in contemporary conflicts involving tech companies (privacy, democracy, and autonomy) extend far beyond the economic concerns that were primarily present during J.P. Morgan's time. Furthermore, while J.P. Morgan's instrument of power, capital flows was readily understood by lawmakers and the broader public, tech companies' tools of power, especially emerging technologies like AI, are algorithmically opaque, limiting regulatory oversight.

Despite differences in speed, scale, and scope, J.P. Morgan and contemporary tech companies function as central arenas that affect the geopolitical behavior of both state and non-state actors. Today, the digital services tech companies offer have evolved into arenas of real-time geopolitical contestation. While tech companies own and operate these platforms, they do not exert geopolitical influence themselves, as actual influence requires the deliberate intent and goal of achieving specific geopolitical outcomes. Instead, privately owned companies are primarily driven by financial incentives, with their platforms being leveraged by others with geopolitical agendas. State-owned companies, which operate under more rigid regulatory structures, are more explicitly motivated to have a role in a geopolitical context, but government directives often shape their actions. Regardless of the regulatory structures, tech companies have built user-engaging, profit-driven colosseums where future geopolitical power struggles will continue to be waged.

iii. Tech Companies as "Actors" of Geopolitics

Under certain conditions, tech companies can be geopolitical actors, wherein they independently impact international affairs. In some cases, a tech company may make decisions that are independent of – or even in conflict with – the foreign policy strategies of their home

country. In this case, technology companies make stand-alone decisions that have an impact on foreign countries beyond commercial interests. This phenomenon is most observed in more libertarian, market-driven regulatory environments, such as that of the United States. As a result, tech companies in the U.S. are not restrained, which, in turn, increases their capacity to engage in political actions. Indeed, this can also depend on the relative strength of the foreign government with which they are interacting and the capacity of the respective foreign government to allow them to operate in a favorable or adversarial manner.

Asserting Agency: Starlink Provides Internet Services in Ukraine

One prominent example of a tech company wielding geopolitical agency is Starlink, a satellite internet service operated by SpaceX. Thanks to its unique satellite-based connection, rather than underground internet cable, Starlink is one of the only options for internet connectivity in remote areas, disaster zones, and active war zones. Starlink began operations in Ukraine following the 2022 ViaSat cyberattack of Russia on Ukraine, which turned off its key satellite networks. Over 42,000 terminals have since been deployed across Ukraine to service the military, hospitals, businesses, and aid organizations.[37] However, in response to information about Starlink being used by the Ukrainian military to operate drones, in February 2023, SpaceX President Gwynne Shotwell clarified that Starlink "was never meant to be weaponized,"[38] and that military application was not in the original agreements. She emphasized that Starlink's contract was solely intended for humanitarian purposes.[39] Unlike traditional defense contractors, Starlink remains a commercial product,[40] which gives the company a level of independence that may not always align with U.S. foreign policy objectives. Gregory C. Allen, a former Defense Department official, noted, "It's certainly been a long time since we've seen a company and an individual openly act in ways that conflict with U.S. foreign policy, especially in the midst of a war."[41]

Starlink's ability to provide critical infrastructure during a war, not merely as a passive service provider but as an active and selective enabler of communication, demonstrates the company's influence over national defense capabilities. Elon Musk's public statements and decisions about service continuity have direct implications for Ukrainian military operations and diplomatic relations.[42]

Asserting Agency: Starlink Circumvents Internet Shutdowns in Iran

Starlink again played a significant role during the 2022 anti-government protests in Iran. The Iranian government, which can control the country's internet access, slowed and eventually cut off service in response to mass nationwide protests.[43] On September 23, 2022, after protests erupted in Iran in response to the death of Iranian national Mahsa Amini in police custody, as well as regressive laws against women and human rights overall, the Biden Administration lifted sanctions to allow U.S. communications companies to operate in Iran. That same day, Musk announced, "Starlink is now activated in Iran. It requires the use of terminals in-country, which I suspect the government will not support, but if anyone can get terminals into Iran, they will work."[44] Within days, human rights activists were able to formulate an underground operation spanning continents

and use private funds to smuggle the terminals and connect the network of protestors. After realizing the Iranian government could no longer control all methods of communication in the country, they accused SpaceX of violating its sovereignty.[45]

This is a striking case of a private company intervening in a sovereign state's internal affairs. By providing uncensored internet access in defiance of the Iranian government's shutdown, Starlink not only empowered activists but also undermined the state's control over information and communication infrastructure. This act, facilitated by changes in U.S. sanctions policy and carried out through a transnational activist network, demonstrates how tech firms can disrupt state authority from the outside.

An Unsuccessful Attempt to Assert Agency: X and Brazil

During Brazil's recent election cycle, the government requested that X (formerly Twitter) limit the reach of specific users and pieces of content to curb potential manipulative information operatives. Elon Musk refused, citing his commitment to protecting free expression on the platform, to assert the platform's agency. Justice Alexandre de Moraes of Brazil's Supreme Court then warned that X could be blocked nationwide if the company did not appoint a local representative and comply within 24 hours.[46] When X still resisted, the court enforced its order and barred the platform from doing so. Faced with the shutdown and mounting legal pressure, Musk ultimately backed down and allowed the specified accounts to be blocked.[47]

The Brazil-versus-X episode is a case study of the evolving power dynamic between global tech platforms and sovereign states. By refusing Brazil's takedown order, Elon Musk signaled that content-moderation decisions are no longer framed merely as operational questions of "community guidelines;" they amount to overt political stances. A platform the size of X shapes what millions of voters can see amplifies or mutes particular narratives, and thus wields an agenda-setting power comparable to a major media network. Choosing free-speech maximalism in an election context, therefore, places the company squarely in the political terrain, whether it intends that or not.

The Brazilian case highlights a significant limitation to corporate autonomy: states retain ultimate coercive authority over tech companies. Governments command legal tools such as licensing regimes, bandwidth throttling, financial penalties, criminal liability for local executives, and outright blocking to force compliance. Justice de Moraes invoked exactly that leverage, threatening X with a nationwide ban unless it followed court orders and appointed an in-country representative. Once the block materialized, the economic and reputational costs rose sharply for X, leading the company to capitulate and block the specified accounts.

Historical Comparison: British East India Company

The British East India Company (EIC) stands as one of the most striking historical precedents for corporations acting as geopolitical actors. Unlike modern-day tech companies, which operate within regulatory frameworks imposed by nation-states, the EIC governed millions of people,

administered justice, and even waged wars in pursuit of its commercial interests. While modern tech companies wield influence over economies and societies, the EIC exerted this influence to a more substantial degree, possessing the formal trappings of state power, including the ability to levy taxes and maintain an army.

However, critical differences set the EIC apart. The most significant is its direct exercise of agency. While modern tech companies influence policy through lobbying and market dominance, the EIC functioned as a governing authority. It issued its diem, entered diplomatic negotiations, and maintained private armies: actions no contemporary corporation can legally undertake. Moreover, the British Crown dissolved the EIC in 1874 and assumed direct control of its territories.[48] As such, the EIC did not enjoy full sovereignty, as it was beholden to the will of the British Crown. That is, the EIC was sovereign only to the extent that the British Crown allowed it to be.

Perhaps the most instructive parallel lies in the relationship between corporate power and state oversight. The EIC's ability to operate as a geopolitical force was eventually curtailed when its actions threatened imperial stability. While tech companies currently do not possess the power EIC enjoyed, their ability to shape public discourse, economic trends, and even national security strategies suggests that they are moving toward a new form of corporate geopolitics – one that, like the EIC, blurs the boundaries between business and statecraft.[49]

The British East India Company is a vital historical reference point exemplifying that a corporation, with its sovereignty ultimately limited by the state, can still become a powerful geopolitical actor. However, like that of their predecessors, the influence of tech companies is contingent on the boundaries imposed by sovereign states. Whether through contract termination, sanctions, or legal mandates, governments retain the ultimate authority.

Key Takeaways of the Agency Framework

By shedding light on the different roles that tech companies play in global affairs – as objects, arenas, and actors – the Agency Framework reveals not only *how* tech companies matter in geopolitics but also *why*. Whether they are targeted or utilized by state and non-state actors to advance their geopolitical agendas or act independently to serve their interests, the roles tech companies play in geopolitics are complex and context-dependent. Tech companies can be geopolitical actors only when they exert their agency, using their tools of power to influence geopolitical issues. Nevertheless, tech companies can also indirectly shape geopolitical dynamics as objects and arenas, given the powerful tools at their disposal. Hence, if agency, read on a spectrum, is a necessary condition for becoming an actor, intent must accompany it for a company to use the tools it possesses to influence geopolitical issues deliberately. With limited agency and no intent, tech companies can still matter by providing an arena for interstate competition. Finally, as objects without agency or intent, tech companies do not act geopolitically, but they are nonetheless caught up in geopolitical dynamics due to their undeniable value. It is worth noting that a tech company providing an infrastructure in global affairs due to the services they provide,

such as Meta, can serve as arenas (e.g., during the Arab Spring) but also as objects (e.g., when Russia designated Meta a terrorist organization during the Russia-Ukraine war). The degree of agency and intent determines which role they assume.

While the tools and domains have shifted from ships and steel to servers and code, our Agency Framework reveals that the underlying dynamic remains: corporations that control foundational infrastructure, whether physical or digital, *can* significantly influence the course of global affairs by intervening in specific geopolitical issues, *contingent* on governments allowing them to do so. The "Tools-Issues" matrix below illustrates this argument **(Figure 1)**.

The "Tools-Issues" matrix filters case studies that we suspect to have some geopolitical dimension and relevance to our analysis. Tools, listed on the left-hand side, are meaningful aspects of a tech firm's business that grant it power (including digital infrastructure, big data, and government partnerships) (see Annex, 3). Geopolitical issues, listed at the top, are areas of interstate power contestation (including elections, public movements, and wars). We selected the cases using open-source research, primarily drawing our examples from news articles and academic publications. These cases show tech companies exercising varying degrees of power and influence over key geopolitical issues, positioning them on a spectrum of geopolitical agency: from low (when they are merely objects), through medium (when they serve as arenas), to high (when they act as actors). We have color-coded the cases based on our interpretation of where they fall on this spectrum.

Figure 1: Tools-Issues Matrix

	Geopolitical Issues						
Tools of Power	**Unclassified**	**Elections**	**Public Movements**	**Wars**	**National Security**	**Pandemic Response**	**Economic Crisis**
Digital Infrastructure	ZTE and Huawei facilitate China's BRI		Starlink & Internet Shutdowns in Iran Facebook and Twitter tools in the Arab Springs	Starlink in Ukraine	Microsoft moved data to EU servers U.S. bans Huawei China bans META and Google Global TikTok bans U.S. TikTok ban META provides an AI model to DoD TSMC provides advanced chips to the Global North		
Big Data							EU threatened levies on major U.S. tech firms TikTok used as leverage in U.S.-China tariffs
Government Partnerships	Microsoft Digital Geneva Convention TSMC & U.S. chip manufacturer Facebook provides Internet in Africa Huawei and Ethiopian partnership						
Content Moderation Policies		X and Brazil quarrel 2016 Russian interference in U.S. elections	Facebook facilitation of genocidal rhetoric in Myanmar		Meta as a "terrorist" designation by Russia	META pandemic content moderation policy pressured by gov	
Ownership of Emerging Technologies				Meta removes deep fakes of Ukrainian President Apple complies with British law			
Mass Membership	TikTok issues pro-Trump message	Russia-Ukraine "social media war"	U.S. TikTok ban extension				

Level of agency

Object **Arena** **Actor**

Section II. Enabling Conditions for Companies to Be Geopolitical Actors

Insight 2: A company's action potential on the geopolitical stage is a function of the firm's profile, and its relationships with the domestic and foreign governments. Hence, a tech company *can* behave as a geopolitical actor, until *governments* decide otherwise.

Empirical Analysis

In the Agency Framework case analysis, we identified the companies which are most present in the geopolitical sphere through the Tools-Issues matrix, organizing the cases as geopolitical "objects," "arenas," or "actors." Section II analyzes the mechanisms that allow companies to be actors in geopolitics. Given that tech companies' potential for geopolitical action is inherently constrained by the regulatory environment in which they operate, it is essential that we understand the relationship each company has with governments and the patterns of their engagement.

We identify three major variables that affect geopolitical action:

- **Firm Profile:** This condition looks at the company itself, including the power that it may wield due to its products and ownership structure. The products a tech company provides allows them to leverage their power against domestic and foreign governments and are the source of their influence. The ownership structure of the company is classified by private, public, or government ownerships. Their position on this ownership spectrum shapes the accountability mechanisms in place that determine their potential action.
- **Relationship with Domestic Government:** This condition outlines the interactions the tech company has with its domestic government, including government contracts, personal friendships, and public-private partnerships. The regulatory environment in which a company operates determines its ability to pursue its own political ends.
- **Relationship with Foreign Governments**: This condition identifies the actions these companies have pursued abroad which have prompted interaction with foreign governments. For a tech company to qualify as a geopolitical actor, it must act on a foreign government. This ability and willingness to act depends on the relative strength of the government in question – a company may be less likely to behave as a geopolitical adversary to a country where it has strong economic incentives, for example. For the sake of this analysis, we aggregated these observations as a trend and did not look at the specificities of each respective foreign governance structures.

From the case study analysis, the tech companies that emerged as most pertinent were X, SpaceX, Meta, Microsoft, Apple, TSMC, TikTok, Huawei, and ZTE. The United States and China emerged as the clear leaders in environments fostering influential tech companies. Figure 2 below provides an analysis of each of these companies as well as how they interact with the three variables listed above: "Firm Profile," "Relationship with Domestic Government," and "Relationship with Foreign Governments."

Figure 2: Tech Company Analysis

Company	Country	Products	Ownership Structure	Relationship with Domestic Government	Relationship with Foreign Governments
X	U.S.	Social media	Private, (owned by X Corp)	• Reinstated Trump's account • Paid $10 million to settle Trump lawsuit over prior suspension at a big discount • Served Trump's political campaign	• Disputes with Brazil over free speech • 10-day ban on X in Venezuela by Maduro • Blocked in Pakistan over national security concerns during the election
SpaceX	U.S.	Satellites, spacecraft	Private	• Contracted by the U.S. government (NASA and DoD) for space exploration, national security, and satellite launches • Received ~$7B from NASA, $1B+ from DoD, and regulatory approvals from FAA/FCC	• Commercial satellite launch services with Turkey, Germany, South Korea, and Israel • Agreements with Ukraine, Japan, Brazil, Indonesia • Restricted by China and Russia
Meta	U.S.	Social media	Public	• Provides DoD with the special Llama model • Donated $1 million to the Trump inauguration • Aligned social media content moderation policies with Trump's views • Prosecuted by the FCC under antitrust laws • Aligned with White House requests to censor COVID content	• Canada: dispute overpaying news channels for the content posted on the platform • Australia: dispute over Australian policy that would make platforms pay for news • Europe: dispute over the use of citizen data to train AI
Microsoft	U.S.	Cloud computing, Data center, Personal computing	Public	• Provides the U.S. government with cloud-based solutions for federal programs • Provides U.S. government special data centers and workers with security clearance • Important cybersecurity partner to the U.S. • Donated $1 million to Trump inauguration • $10b contract to provide services to the U.S.	• Airband initiative - helps countries develop broadband capabilities • India: open AI center of excellence in line with national AI strategy and $3 billion investments • $298m investment in South Africa • Kenya: additional $1b with G42 • Abu Dhabi: invest $1.5b in G42
Apple	U.S.	Personal computing, Software development	Public	• Investing $500 billion in the U.S. over the next 4 years	• Reliant on China for supply chains and manufacturing • Shifting supply chain to India amid US-China tension
TSMC	Taiwan	Semiconductors	Public, (Taiwan's Executive Branch as largest shareholder)	• Largest company in Taiwan • Central link in the semiconductor supply chain • Key to Taiwanese security & national defense (known as the "silicon shield")	• U.S. companies are largest consumers of its chip output[9] • TSMC is the likely sole reason for Taiwan receiving a billion in U.S. military aid • Netherlands sole manufacturer of high-end lithography equipment integral to TSMC's production pipeline • Challenge for China and the Chinese American relationship due to strong ties to the Taiwanese gov.
TikTok	China	Social Media	Private, (Chinese gov. owns 1% "golden share" in ByteDance)	• Chinese government oversight on cybersecurity, data laws, and censorship policies • ByteDance Internal CCP Committee • Imposed government restrictions on exporting ByteDance AI algorithms	• Scrutinized over data privacy concerns (U.S., EU, India) • Backed by global firms such as Sequoia and SoftBank • Banned by India in 2020 • Threat of ban in the U.S. • Receives state-linked funding in Singapore and Japan
Huawei	China	5G, Manufacturing, Personal Computing, Cloud	Private*, (Employee ownership model)	• *Reported as unaffiliated with the Chinese government, but this is contentious among other countries • Implementation partners of the BRI	• Banned across the world • Limitations by France, the Netherlands, Norway, Japan • Agreement to build a $3.5m data center in Nepal • Large-scale investment from Brazil • Ethiopia as a partner for digital strategy • Thailand deal for data centers and 5G infrastructure
ZTE	China	5G, Manufacturing, Cloud	Public, (Partially state-owned)	• Reported as state-owned and privately run • Strong ties to the Chinese state	• Banned by the U.S. • Partnership with 160 countries • 5G DigiSchool in South Africa

The data presented in this table yields several important findings and patterns in the relationship between the variables. Firms whose offerings relate to national-security infrastructure, like satellites, 5G gear, or advanced semiconductors, become quasi-strategic assets to the state. SpaceX thrives on multibillion-dollar NASA and U.S. Department of Defense (DoD) contracts; TSMC counts Taiwan's executive cabinet among its largest shareholders; Huawei and ZTE, formally employee-owned or state-owned, still move with Beijing's industrial policy. Because these companies benefit from strong backing at home, they trigger mirror-image reactions abroad, attracting barriers to imports, outright bans, or security reviews from foreign governments that view their technology as a vector of influence. Ownership acts as a built-in policy lever. The tighter the state grip, whether through golden shares, cabinet stakes, or state ownership, the more predictable domestic alignment becomes. This leads to more acute backlash overseas. Conversely, public companies such as Apple, Microsoft, and Meta, as well as privately held firms like X and SpaceX, possess nominal independence yet still find governments exerting pressure through procurement windfalls, regulation, or antitrust actions. That leverage shapes platform behavior.

Scoring Index

Building on this empirical analysis, we create a scoring index that allows us to assign a numerical value to the geopolitical action potential of a company at a given point in time. Our scale ranges from a score of 1 to 8. First, we identify observable characteristics for each enabling condition of geopolitical action potential. Then, based on the Tech Company Analysis, we establish the direction of the correlation between each observable characteristic and geopolitical action potential, identifying which elements promote geopolitical action potential and which elements restrain it. Finally, we attempt to quantify geopolitical action potential by creating a point system for each of the enabling conditions.

To create a scoring index around the relationship between the enabling conditions and geopolitical action potential, we identify observable characteristics on which to base the analysis. This allows us to identify specific characteristics of the enabling conditions.

Figure 3: Enabling Conditions and Their Characteristics

Enabling Conditions	Observable Characteristics
Firm Profile	• Ownership of advanced technology • National security link • Ownership structure
Relationship with Domestic Government	• Regulatory regime • Government contracts
Relationship with Foreign Governments	• Investment in digital infrastructure • Legal disputes

After identifying the observable characteristics of each enabling condition, we seek to understand the mechanisms by which they affect a given company's potential for geopolitical action. Drawing from the lessons of our tech company empirical analysis, we identify the effect of each observable characteristic.

Figure 4: Enabling Conditions' Effect on Geopolitical Action Potential

Enabling Conditions	Observable Characteristics	Effect on a Company's Geopolitical Action Potential
Firm Profile	Ownership of Advanced Technology	As the pace of innovation increases, the government's ability to regulate at the same speed decreases, which, in turn, increases geopolitical maneuvering on the company's behalf. Therefore, if a company owns cutting-edge technology in a lax regulatory environment, it will have greater geopolitical action potential.
	National Security Link	Suppose a company has a product that becomes of national security interest to the government. In that case, the government will become more interested in overseeing its actions, and the company will lose geopolitical action potential.
	Ownership Structure	If the company is privately owned, it has more operational maneuverability. Its accountability mechanism concerns only itself and its incentives. If the company is publicly owned, it has operational maneuverability. As it is traded publicly, its accountability mechanisms are related to market dynamics. If it is government-owned, it also benefits from business incentives and alignment with the government's policies. If the company is private or public and the government owns a symbolic share, it will likely operate in line with government policies.
Relationship with Domestic Government	Regulation	As regulations determine a company's capacity to operate, companies have less room to act in their geopolitical interests, and they lose the potential for geopolitical action.
	Government Contracts	As companies acquire more government contracts, they become increasingly tied to the government and lose their geopolitical action potential.
Relationship with Foreign Governments	Investment in Digital Infrastructure	As companies invest in foreign countries, they gain maneuverability in that country and gain geopolitical action potential.
	Legal Disputes	If a company faces legal disputes in a foreign country, it is likely less able to operate with complete agency and lose geopolitical action potential.

We then seek to create a simple quantifying algorithm for tech companies' geopolitical action potential where:

- The value is ϕ if it does not contribute to geopolitical power potential
- The value is ✓ if it contributes to geopolitical power potential

In the case of company ownership, the values range from 0 to 2. This is to capture the difference between government ownership, public ownership, and private ownership. This quantitative analysis results in each company being attributed a score between 1 and 8. The higher a company scores in the evaluation, the greater its potential is to become a geopolitical actor, resulting in it

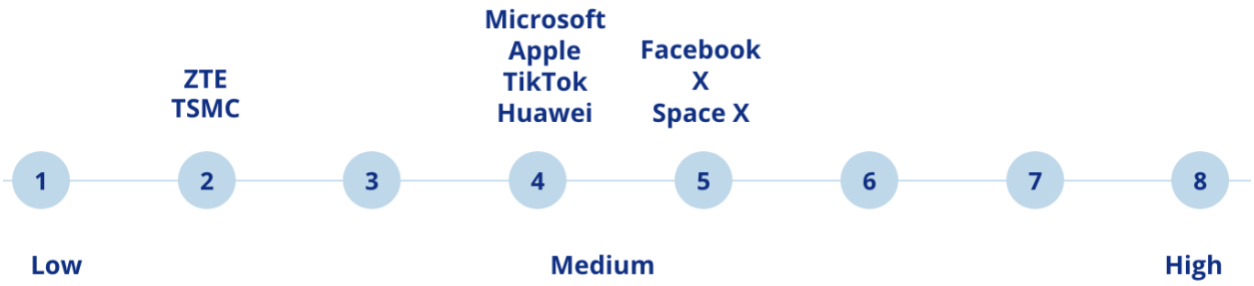
meeting more enabling conditions. This quantification serves as an index to compare companies at a given moment and track the evolution of a company over time; however, the values are meaningless taken out of context.

Figure 5: Geopolitical Action Potential of Studied Companies

			U.S.					China and Taiwan			
Enabling conditions	**Observable characteristics**	**Actions**	**SpaceX**	**X**	**Microsoft**	**Facebook**	**Apple**	**ZTE**	**TSMC**	**TikTok**	**Huawei**
Firm Profile	Product Type	Owner of the most advanced technology in their product type (✓) No (ϕ)	✓	ϕ	ϕ	ϕ	ϕ	✓	✓	ϕ	✓
		It is not in the national security interest (✓) **It is** in the national security interest (ϕ)	ϕ	✓	✓	✓	✓	ϕ	ϕ	✓	ϕ
	Ownership Structure	Privately owned (✓✓) Publicly owned (✓) Government-owned (ϕ)	✓✓	✓✓	✓	✓	✓	ϕ	ϕ	✓	✓✓*
Relationship With the Domestic Government	Legal Regime	Light (✓) Rigid (ϕ)	✓	✓	✓	✓	✓	ϕ	ϕ	ϕ	ϕ
	Government Contracts	No (✓) Yes (ϕ)	ϕ	✓	ϕ	✓	ϕ	ϕ	ϕ	✓	ϕ
Relationship With Foreign Governments	Investments in Digital Infrastructure	Yes (✓) No (ϕ)	✓	ϕ	✓	✓	✓	✓	✓	✓	✓
	History of Legal Disputes	No (✓) Yes (ϕ)	ϕ	ϕ	ϕ	ϕ	ϕ	ϕ	ϕ	ϕ	ϕ
Total			**5**	**5**	**4**	**5**	**4**	**2**	**2**	**4**	**4**

*NB: Huawei is officially owned by its employees. However, there are suspicions that it is owned by the Chinese government. Given this contention, we assign it a score of 2 following the company's disclosures. To some audiences, this elevates the score of Huawei beyond what would be intuitively anticipated. However, the subject of Huawei's effective ownership structure is beyond the scope of this paper.

Figure 6: Spectrum of Geopolitical Action Potential



These results match what we would intuitively expect from the quantification. We see that ZTE and TSMC are at the lower end of the scale, reflecting their position as instruments of power leveraged by their governments, while Facebook, X, and Space X are on the highest end of the spectrum, reflecting their relative independence from governmental agencies due to technological innovation. Those in the middle of the spectrum are those who have legacy technology that, over time, has become regulated by the government. While the quantification itself is flawed, the model identified the variables that were important to the analysis and that were a good starting point for future research.

This quantification is a basic model with limitations:

- All observable characteristics are independent and are weighted equally, except for ownership structure. These are simplifying assumptions that necessitate further research to develop greater complexity.
- The ownership structure is measured on a scale of 0-2. This explicitly weighs ownership structure more than the other variables. This is to allow for more complexity in the ownership structure analysis, but it can create distortions in the final score.
- Since all other observable characteristics are weighed equally, this enables substitution between them, which might not reflect reality.
- There might be some endogeneity where the decision to go into a certain product line linked to national security would inherently bring the company to be more linked with the government.
- There are deep structural differences between the U.S. and Chinese markets, which are not reflected in the table.

To further develop this quantitative model, more research is needed to determine the interdependencies between the variables and the relative weight of each observable characteristic.

Section III. Projections

Insight 3: We predict that, in the long run, tech companies will be compelled to cede their geopolitical agency to states with the regulatory leverage to preserve state primacy in global affairs. In other words, the balance of power between states and tech companies will remain tilted in favor of states, making a technopolar world unlikely.

Our Agency Framework (Section I) reveals that the role of tech companies in geopolitics is layered, and their ability to act geopolitically is subject to the tools of power they possess, as well as the regulatory mechanisms within which they operate. In other words, tech companies can behave as geopolitical actors if they so choose until governments perceive their actions as an infringement on their sovereignty. Beyond the legal regime of the domestic government in which the tech company is based and the history of legal disputes with foreign governments, our tech company analysis (Section II) examines additional enabling factors that determine tech companies' potential for geopolitical action, such as product type, ownership structure, government contracts, and investments in digital infrastructure. Putting this research into perspective, we develop projections on the geopolitical agency trajectory of both U.S. and Chinese tech giants, informing our base case scenario of the balance of power between tech companies and governments. We also consider the main watchpoints and their impacts on our projections.

Base Case Scenario

In our base case scenario, the geopolitical agency of high-potential tech firms follows a distinct arc: it rises as their technologies scale and diffuse but eventually tapers as external constraints intensify. This trajectory reflects the cumulative effects of the enabling conditions discussed above. Crucially, the time component of this curve is not tied to a fixed calendar but is relative to each company's stage of technological and geopolitical maturity. As a firm's influence grows, it reaches a critical inflection point, a threshold at which heightened government oversight, regulatory intervention, or geopolitical entanglement begins to reshape or slow its upward trajectory. The exact timing and nature of this inflection depend on the firm's sector, its user base, and the sensitivity of its core technology. For instance, companies like Google, which provide foundational internet infrastructure and have long operated at scale, are likely positioned at or beyond the first inflection point, where their geopolitical power is now modulated by mature regulatory frameworks. By contrast, a company like OpenAI, whose central product, a large language model, has only recently emerged as geopolitically salient, remains earlier on the curve, with significant growth potential but less formalized oversight. Importantly, this geopolitical agency trajectory diverges under different governance regimes. In the market-driven U.S. model, firms retain more leeway before encountering state constraints, while in China's state-led model, firms are more closely integrated with or subordinated to state objectives at earlier stages. Despite these variations, our base case assumes that states continue to serve as the dominant geopolitical

actors, ultimately shaping and bounding the agency of even the most globally influential tech companies.

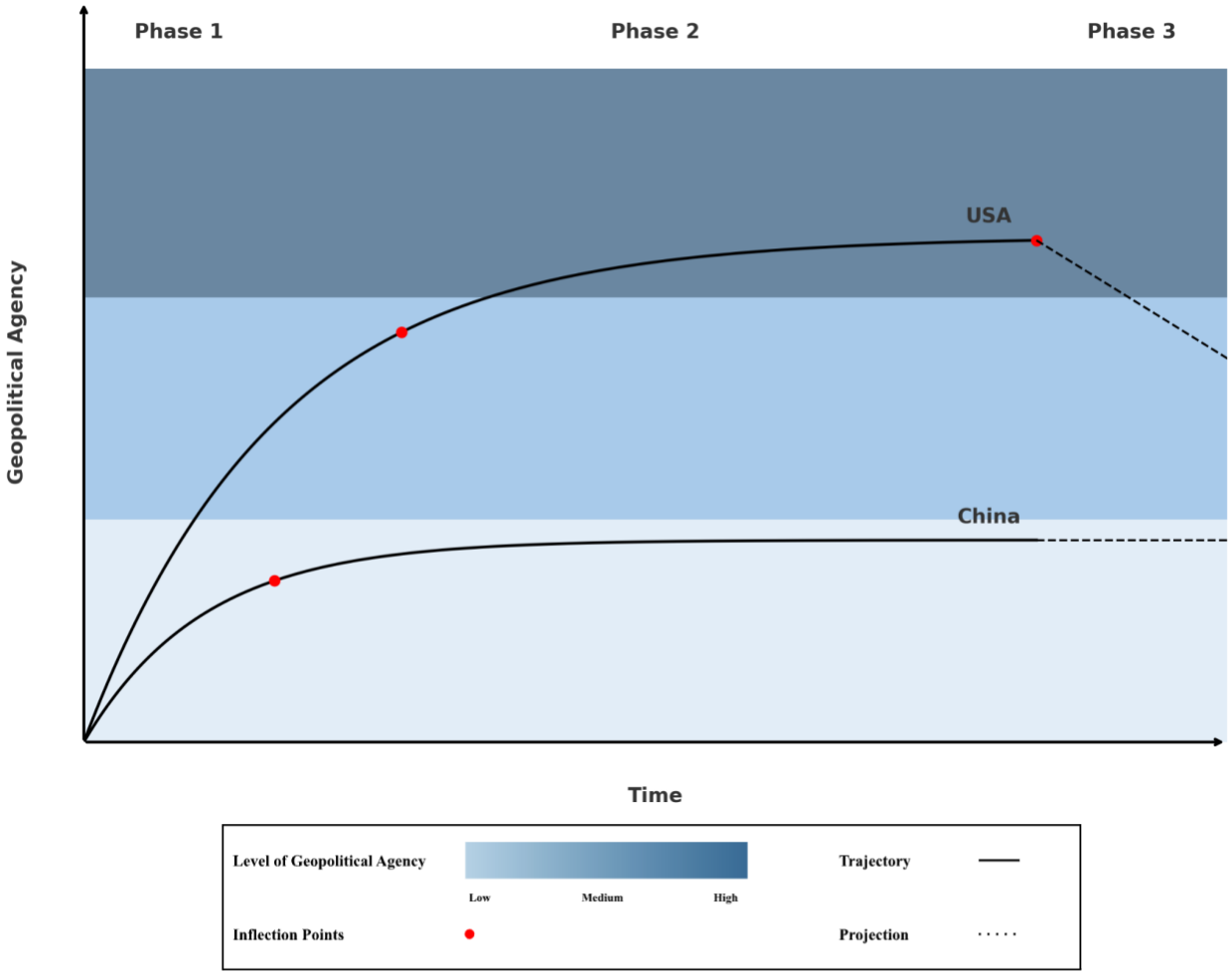
American tech companies' geopolitical agency trajectory follows three phases:

- *Phase 1*: American tech companies have the leeway to exert geopolitical agency, bolstered by certain characteristics of their firm profile and relationships with domestic and foreign governments. In this phase, the companies with the steepest trajectory are the ones that are privately owned and produce an advanced tech product that governments do not perceive as a product of national security interest. Typically, these companies do not have government contracts with their home governments, have not been involved in legal disputes with foreign governments, and expand their reach abroad through foreign investments.
- *Phase 2*: As American tech companies increasingly exert geopolitical agency, they attract both foreign and domestic governments' oversight, constraining their ability to act geopolitically (inflection point 1). In this second phase, tech companies still exert agency, but their growth flattens as they fall under the radar of governments. At this stage, the relationship with the domestic government strengthens, reaching such a level of influence that they become of national security interest and attract the scrutiny of foreign governments.
- *Phase 3*: Under the radar of governments, American tech companies exerting influence in geopolitics ultimately face regulatory actions (inflection point 2). At home, the government attempts to mitigate their power and influence by issuing antitrust lawsuits. Abroad, they face legal disputes with foreign governments that try to protect their power and influence within their borders.

Inherently constrained by the Chinese state-led model, Chinese tech companies' geopolitical agency trajectory follows three phases:

- *Phase 1*: Chinese tech companies have the leeway to exert geopolitical agency, bolstered by certain characteristics of their firm profile and relationships with domestic and foreign governments. Due to China's rigid legal regimes, Chinese companies quickly face government scrutiny, reducing the growth rate of their geopolitical agency trajectory. In this phase, the companies with the steepest trajectory are the ones that are privately owned and produce an advanced tech product that is not perceived by their home and foreign governments as a product of national security interest. Typically, these companies do not have government contracts with their home governments, have not been involved in legal disputes with foreign governments, and expand their reach abroad through foreign investments.
- *Phase 2*: As Chinese tech companies increasingly exert geopolitical influence, they attract government oversight (inflection point 1) and quickly become Chinese state-enabled strategic assets, used either as objects or arenas to serve the Chinese government's geopolitical agenda.
- *Phase 3*: Considered by the home government to be of national security and public interest, the company will maintain a flat trajectory, constrained by their country's rigid legal posture to remain in a low geopolitical agency zone.

Figure 7: Geopolitical Agency Trajectory of Tech Companies



Given these trajectories, we predict that, in the long run, tech companies will be compelled to cede their geopolitical agency to states, which have the regulatory leverage to preserve state primacy in global affairs. In other words, the balance of power between states and tech companies will remain tilted in favor of states, making a technopolar world unlikely.

States will remain the principal actors in geopolitics, constraining tech firms' ability to exert geopolitical agency. Nevertheless, tech companies will maintain – and steadily gain – significance in geopolitics as the tools they possess, such as digital infrastructure, big data, and massive user bases, become national security assets that increasingly define the contours of interstate competition. This competition has been perceived as a "tech cold war" as the U.S. and China compete over semiconductors, artificial intelligence, and other emerging technologies, which are critical to maintaining their supremacy.[50] The weapons of this new tech cold war are not nuclear bombs but rather instruments of economic statecraft, such as export controls, investment screening, and industrial policy, deployed by governments, not companies. While tech firms create the products being coveted, this competition is between sovereign states. This doesn't disregard the

fact that tech companies themselves are competing to create the most advanced products but are mainly motivated by economic rather than political reasons.

Main Watchpoints

- **Domestic regulatory environment (e.g., U.S. antitrust lawsuits)**. Ongoing antitrust actions and broader competition-policy debates in Washington reinforce our base case scenario that states ultimately constrain tech companies' geopolitical agency. Each new lawsuit or rulemaking round shortens the window in which firms can translate scale into geopolitical leverage, nudging their agency curve downward. While litigation rarely strips firms of all influence, it reallocates bargaining power to regulators.

- **Governments move toward technology self-reliance (e.g., Matrix protocol)**. Tech companies are entrusted with billions of personally identifiable information – a reliance that creates a single point of failure and increases the risk of cyber intrusions, leaks, or outages. As a result, countries have already engaged in initiatives to claim digital sovereignty. One such example is the Matrix protocol, an open standard for an end-to-end encrypted, interoperable, and decentralized real-time communication network for messaging, voice over IP (VoIP), and other forms of communication. This has been adopted by the French government, Luxembourg government, and the German Armed Forces as an official messaging network and service. Initiatives like the matrix protocol show that governments have already taken steps to have more direct ownership over their tech infrastructure, though it may not be adopted by the wider public. When governments adopt open standards like the Matrix Protocol or fund sovereign communications and space infrastructure, they dilute tech-company gatekeeping power and create fallback systems that lessen dependency on private platforms. This strategic "re-internalization" of critical digital utilities compresses the area under firms' agency curves in both the U.S. and China, confirming the base case in which states retain decisive leverage – especially in crises when they can simply migrate to state-controlled alternatives.

- **Intensifying U.S.-China trade war (e.g., use of export controls on chips and critical minerals)**. Bilateral restrictions weaponize tech companies' supply chains, forcing companies to align with national policy and curbing their freedom to operate globally. The result is a sharper divergence between the two regulatory models and a narrower gap between their respective agency curves because American tech companies' access to key inputs (critical minerals) necessary to win the AI race is suddenly constrained. This dynamic reinforces state primacy but also heightens firms' strategic value as pawns. This tech competition is not only between the U.S. and China but also between states worldwide as they attempt to claim digital sovereignty. As the world fragments between the two tech ecosystems created by the U.S. or China, countries may not be able to remain neutral, pressured to either align with the former or create their own autonomous tech ecosystem, which is not accessible to all. This pressure to claim sovereignty is driven by concerns over data privacy and national security.

- **Major technological breakthroughs (e.g., foundation-model AI or quantum computing).** Disruptive advances can temporarily boost a firm's leverage by creating new, scarce capabilities; our trajectories would bulge upward in the short term. Yet once states grasp the strategic salience, they move to regulate, subsidize, or nationalize the know-how, pulling the curve back toward the baseline. Breakthroughs thus inject volatility into the timeline but do not overturn the long-run outcome: states reassert control after an adjustment lag.

Section IV. Conclusion

Does the rise of tech companies herald a technopolar era in which companies eclipse states as the primary actors of world politics? Our analysis suggests not. Tech companies certainly matter, but their influence is conditioned by – rather than independent of – state power. Tech companies will increasingly gain significance in geopolitics as the tools they possess become national security assets that increasingly define the contours of interstate competition. Nonetheless, their maneuverability to exert agency is contingent upon a set of enabling conditions that inherently constrain their ability to behave as geopolitical actors. Section I showed that companies oscillate among three roles: *objects* of interstate competition, *arenas* through which others project power, and, under specific conditions, *actors* that pursue their own agendas. Section II traced those conditions to a company's technological assets, ownership and security profile, and its relationships with home and host governments; an index of these factors indicates that agency is highest for privately owned, advanced-technology firms operating in light regulatory environments and lowest for companies tightly linked to national-security mandates or direct state ownership. Section III projected these patterns forward, showing that tech companies' influence tends to expand until governments intervene with regulations, contracts, or legal actions that limit further autonomy. Accordingly, tech firms will continue to matter in global politics, but their geopolitical agency will always be contingent on the constraints that states choose to impose. This report has focused deliberately on tech companies – legal entities whose rights and obligations are ultimately circumscribed by state law. Yet the forces reshaping geopolitics extend beyond the firm. Breakthroughs in AI or quantum computing can reorder strategic balances on their own, and charismatic technologists can wield influence that outstrips any single corporate charter. Recognizing that wider universe of "technology" and "technologists" invites further inquiry into how, and how far, power may flow outside the corporate structures analyzed here.

Two caveats temper our conclusions. First, many transactions, lobbying efforts, and informal ties between tech firms and governments are opaque, limiting the precision of any assessment of corporate influence. Second, our study relies on qualitative case analysis; without quantitative tests, the causal weight for each episode cannot be established. Future research that combines richer data on state–firm interactions with quantitative methods would sharpen our understanding of how, when, and to what extent technology companies can act geopolitically; but always within limits set by sovereign states.

Annex

1. Acknowledgments

The Columbia SIPA Capstone team would like to extend our gratitude to our mentors and advisors who made our research possible. At SIPA, we are particularly grateful to Professor Markus Jaeger, Adjunct Professor of International and Public Affairs, whose vision, advice, and feedback proved invaluable throughout our research and writing process. The team is incredibly grateful for the freedom and creativity that Professor Jaeger enabled us to implement. We would also like to thank our client, Eurasia Group. We are especially thankful to Sebastian Strauss, Director of Global Macro at Eurasia Group, who guided us on avenues for research and scope.

2. Historical Comparison Tables

	Similarities	**Differences**
1973 Oil Embargo (Seven Sisters)	● Private firms transformed into state instruments ● Leverage control over critical assets (oil then, data/services now)	● Methods of tool capture (direct expropriation vs indirect regulation)

Annex Figure 1: Historical Comparison of Private Firms as Objects

	Similarities	**Differences**
J.P. Morgan	● Intangible products ● Chokepoint power ● Proximity to the home government ● Public perception ● Trans-national presence	● Speed of innovation ● Scale of private power ● Scope of influence

Annex Figure 2: Historical Comparison of Private Firms as Arenas

	Similarities	**Differences**
British East India Company	● Monopoly control over trade ● Entanglement with state interests ● Control over critical economic infrastructure	● Direct territorial rule ● Levied taxes and waged wars ● Functioned as a quasi-sovereign entity

Annex Figure 3: Historical Comparison of Private Firms as Actors

3. Tech Companies' Tools of Power

A tool is any meaningful aspect of a tech firm's business that is possessed by tech companies and may grant the ability to exert power in global affairs. The following list of tools presented is an inventory of these items, which serves as the foundation for the frameworks developed in this paper. This is in no way meant to be an exhaustive or definitive list but rather serves as a basis for future research on the topic.

Digital Infrastructure

Before the 21st century, public physical infrastructure – such as roads, electricity, water, and plumbing – was essential to economic and social development. Today, digital infrastructure and systems manage and support digital identity, payments, and data exchange systems, with funding and creation coming from governments, philanthropies, transnational organizations, and the private sector. [51] Frischmann defines infrastructure as "shared means to many ends," viewing it as a holistic concept that encompasses not only physical elements but also social, institutional, and digital aspects. He emphasizes its communal nature and the wide range of potential uses, including services and other goods. When people refer to "digital infrastructure," many still think of the physical telecommunications systems that support the digital age, such as internet cables, data centers, and transmission networks. Others think of it in terms of the internet. The internet stands as a prominent example of how software (such as instructions and protocols), combined with hardware (like computers and cables), forms digital infrastructure. With access to a device and a reliable connection, individuals, businesses, and organizations can use the internet for research, communication, commerce, gaming, and countless other activities. Although the governance of this infrastructure is a subject of ongoing debate and change, there is widespread agreement that both the physical infrastructure and the protocols of the internet qualify as forms of infrastructure.

Big Data

Due to their client-facing position in the market, technology companies collect enormous amounts of data. This data includes personally identifiable information (PII) – name, date of birth, address, credit card number – and general data – demand for a certain good, environmental data, etc. At the aggregate level, the private sector, specifically tech companies, holds the largest data sets on people around the world. From this, they can use data analytics to understand society and make business decisions. The amount of data these companies possess can be utilized as a tool to yield political power. First, they can create partnerships with the government to share valuable data-driven insights on issues the government would not have otherwise. Second, they can use this data to train state-of-the-art large language models, which are increasingly becoming a cornerstone of national strategies. These two secondary effects of Big Data ownership give technology companies a strategic position in the geopolitical landscape, which can be leveraged to meet their interests. For example, in 2025, the U.S. attempted to ban TikTok, citing the Chinese government's access

to TikTok data on U.S. citizens as a national security issue. This entails that the data being collected by a tech company, TikTok, directly threatened the national security of another country, the United States.

Mass Membership

One of the major advantages of power tech companies, which benefit from their mass membership, is their enormous user base, aggregated worldwide. Mechanisms of influence tied to mass membership include agenda-setting and norm-shaping, referring to the ability of platforms to amplify certain information or values to global audiences, shaping what issues people perceive as necessary. Another important mechanism of influence is network mobilization, which refers to the ability to rally large user bases for collective action. Hence, the influence of mass membership is not only top-down, from company to users, but also bottom-up, where the existence of a vast user community itself becomes a geopolitical asset. Companies having employed user mobilization include Uber, Airbnb and most recently TikTok, urging its users to oppose government's proposed legislation to ban the application in the U.S.[52] Hence, tech companies can leverage this vast network not only to set agendas directly but also to exercise "latent influence" when traditional inside lobbying is weakened by high public salience. In other words, platform companies may use their unique relationship with consumers to indirectly influence policy outcomes, a case of regulatory capture occurring through the cognitive capture of citizens. This challenges the consensus in academia, according to which firms often get their way in politics during periods of quiet politics.

Content Regulation Policy

Social media platforms can use self-regulation as a tool to project their geopolitical goals. Companies such as Facebook and X have taken recent measures to regulate their content, and in the process, have platformed or de-platformed certain individuals and constituencies. For example, in early January, Meta announced the decision to end their fact-checking program, and many see this as a gift to Trump and his allies.[53] It is interpreted as providing a platform to conspiracists and extremists to voice themselves without regulatory consequence. This is just one example of how a company may choose not to regulate their platform to empower a certain audience, however, there are also examples of companies regulating content to disempower individuals and impact key geopolitical issue areas. The best example of this came after January 6 in the United States. X and Facebook quickly deplatformed Donald Trump after rioters sieged the U.S. Capitol, taking down posts that highlighted Trump's extremist rhetoric. Facebook and X did not make these decisions for financial gain, but rather as an appeal to their own stakes in a key political issue: the U.S. Presidential Election.

Government Partnerships

Government partnerships are crucial when analyzing how tech companies operate as geopolitical actors because these firms wield significant influence over global infrastructure, information flows, and national security. As technology giants expand their reach, they shape digital

economies, control vast amounts of user data, and even influence political discourse, often operating across multiple jurisdictions with varying regulations. Governments, recognizing this power, engage in partnerships with these companies to ensure national security, protect critical infrastructure, and maintain regulatory oversight. Such collaborations help address issues like cybersecurity threats, data privacy, and the potential misuse of technology for political manipulation. Moreover, partnerships between governments and tech firms can serve as a counterbalance to state-backed technological advancements in rival nations, particularly in areas such as artificial intelligence, telecommunications, and semiconductor production. As such, by working together, or often in competition, governments and tech companies can navigate the intersection of economic power and strategic interests in an increasingly digitized and contested global landscape.

Ownership of Emerging Technologies

Big Tech's ownership of emerging technologies like Artificial Intelligence and cloud computing is redefining the balance of power between the public and private sectors. The rapid popularization of generative AI since August 2022 has driven unprecedented adoption, with the number of U.S. users rising from 7.8 million in 2022 to over 100 million in 2024, a rate surpassing even that of smartphone adoption.[54] This explosive growth reflects widespread interest from individuals, governments, and industries in integrating AI-driven solutions into everyday operations. For instance, Singapore's Integrated Health Information System is developing SecureGPT on Microsoft's Azure cloud, and Japan has partnered with Microsoft to design an in-house GenAI model for government use.[55,56] No longer just technology providers, these firms have positioned themselves as strategic partners in national digital infrastructure, embedding themselves deeply in governance structures. They act as policy entrepreneurs, promoting digital platforms as essential policy tools. For example, during the COVID-19 pandemic, the UK government enlisted Big Tech representatives to help design policy solutions, leading to the development of contact tracing tools, "Disease Prevention Maps," medical capacity tracking systems, and AI-driven vaccine development.[57]

Tools of Power Key Takeaways

The possession of these tools is the greatest quality that enables tech companies to exert influence over geopolitical affairs. These tools are not meant to be understood as existing in isolation, and in fact, it is likely always the case that these tools are used in conjunction by a tech company to achieve a geopolitical aim. A key point is that these tools are not only ways to wield power in the geopolitical arena but may amplify that power through their use.

4. Regulatory Environments

Regulations in China that prevent tech companies from exerting agency

- "Golden Shares": A golden share is a type of share that gives its shareholder veto power over changes to the company's charter. It holds special voting rights, giving its holder the ability to block another shareholder from taking more than a ratio of ordinary shares.[58] The Chinese government has acquired Golden Shares in Alibaba, Tencent, and ByteDance.[59]
- The National Intelligence Law: This law requires "any organization or citizen to support, assist, and cooperate with state intelligence work" and to maintain the confidentiality of intelligence operations. The law also allows the CCP to compel firms to install backdoors in their equipment or software, and it creates a system of incentives and penalties for compliance.[60]
- The 2017 Cybersecurity Law: This law requires critical infrastructure companies to store data within the PRC and make this data accessible to intelligence services.[61]
- The 2021 Data Security Law: This law expands CCCP access to companies and data within China, including the ability to control out-bound data flows.[62]

Regulations in the U.S. that encourage tech companies to exert agency

- First Amendment to the Constitution: The First Amendment protects individuals right to free speech and was utilized by Apple computer as an argument in the case Apple v FBI, in which the FBI used the All Writs Act to claim that Apple needed to provide the FBI with a "backdoor" by which to access data stored on their devices. Although this case was rendered moot by the FBI's hacking of the device and subsequently dropping the case, it provides important precedent that Apple was not forced to provide backdoor.[63]
- Microsoft v. United States: In this case, it was alleged that Microsoft was obligated under the Stored Communications Act to comply with a warrant obtained by the U.S. government and release data stored on servers controlled by Microsoft located in Ireland. Though initially the Southern District of New York ruled in favor of the U.S., the Second Circuit Court of Appeals ultimately decided in favor of the tech company. While this did lead to the passage of the CLOUD Act, which gave the government broader access to corporate data, it remains an important precedent.[64]

Regulatory Environments Key Takeaways

- Companies owned by state entities, whether through the issuance of Golden Shares or a nationalization effort, appear to be more subject to State authority than those that are not.
- Western-style judicial and legislative infrastructure may provide corporations a venue in which to air grievances and win significant arguments against a hostile or overly burdensome State authority.
- Legal and judicial limits are being placed on Western tech companies through legislative decrees such as the CLOUD Act or Sarbanes-Oxley.
- The Western legal principle of shareholder protection is seemingly more encouraging of tech companies acting autonomously than legal frameworks that lack the principle.

Bibliography

[1] Harwell, Drew. “Trump vilified tech giants. Now they’re giving him millions.” *Washington Post*, 21 January 2025, https://www.washingtonpost.com/technology/2025/01/11/trump-big-tech-inauguration-zuckerberg-bezos-google//.

[2] Swenson, Ali. “These Tech Billionaires Flanked Trump at Inauguration.” *AP News*, 20 January 2025, apnews.com/article/trump-inauguration-tech-billionaires-zuckerberg-musk-wealth-0896bfc3f50d941d62cebc3074267ecd.

[3] Althauser, Joshua. “If Apple, Microsoft and Amazon Were Countries – Rank Top 10 Richest Nations.” *Headline Bulletin*, 31 March 2022, https://hbuk.co.uk/apple-microsoft-and-amazon-were-countries-would-rank-in-the-top-10-richest-nations.

[4] Bradford, Anu. Digital Empires: The Global Battle to Regulate Technology. *Oxford University Press*, 2023.

[5] Bradford, Anu. Digital Empires: The Global Battle to Regulate Technology. *Oxford University Press*, 2023.

[6] “Agency Definition & Meaning.” Merriam-Webster. Accessed May 15, 2025. https://www.merriam-webster.com/dictionary/agency.

[7] Birch, Kean and Kelly Bronson, “Big Tech,” *Science as Culture* Vol. 31, No. 1, 1-14, 2022, https://doi.org/10.1080/09505431.2022.2036118.

[8] Saaty, Thomas L. and Mohamad W. Khouja, “A Measure of World Influence,” *Journal of Peace Science* 2, no. 1, 1 February 1976, 31–48, https://doi.org/10.1177/073889427600200103.

[9] Marton, Péter. “A Theory of Non-state Actors,” *Palgrave Macmillan, Cham*, 29 April 2024, https://link.springer.com/referenceworkentry/10.1007/978-3-031-05750-2_89-1.

[10] Dahl, Robert A. “The Concept of Power,” Behavioral Science, vol. 2, no. 3, 1957.

[11] Munro, André. “State Monopoly on Violence,” *Britannica*, https://www.britannica.com/topic/state-monopoly-on-violence.

[12] Levingston, Ivan, et al. “US Investors in ByteDance Explore TikTok Deal to Appease Donald Trump.” *Financial Times*, 21 March 2025, www.ft.com/content/8611dc56-4333-405c-b8bb-592eb940ba70.

[13] Hannah Murphy and Demetri Sevastopulo. “Donald Trump to Extend Deadline for TikTok Deal in the US.” *Financial Times*, 4 April 2025, www.ft.com/content/7f5d15eb-39f8-4ded-8f5c-46ef8ab4d19d.

[14] Ebrahim, Nadeen. "Middle Eastern Regimes Have a History of Shutting Down the Internet. But it's Costing Them." *CNN*, 3 July 2023, www.cnn.com/2023/07/03/middleeast/middle-east-internet-shutdowns-mime-intl/index.html.

[15] Johnston, Emerson. "From App to Allegory: The TikTok Ban as a Symbol of Deeper Geopolitical." *Stanford*, 2024, fsi.stanford.edu/sipr/tik-tok-geopolitical-tensions.

[16] Mai, Jun, "Chinese holiday island to unlock Facebook, Twitter and YouTube for foreign visitors," *South China Morning Post*, June 22, 2018, https://www.scmp.com/news/china/policies-politics/article/2152102/chinese-holiday-island-unlock-facebook-twitter-and.

[17] McBride, James, Noah Berman and Andrew Chatzky. "China's Massive Belt and Road Initiative." *Council on Foreign Relations,* 2 February 2023, https://www.cfr.org/backgrounder/chinas-massive-belt-and-road-initiative.

[18] Wu, Jieh-min. "Silicon Shield 2.0: A Taiwan Perspective." *The Diplomat,* 14 September 2024, https://thediplomat.com/2024/09/silicon-shield-2-0-a-taiwan-perspective/.

[19] "Undermining Ukraine: How Russia Widened Its Global Information War in 2023." *Atlantic Council*, 29 February 2024, www.atlanticcouncil.org/in-depth-research-reports/report/undermining-ukraine-how-russia-widened-its-global-information-war-in-20.

[20] Roula Khalaf, Henry Foy and Andy Bounds. "EU could tax Big Tech if Trump trade talks fail, says von der Leyen." *Financial Times,* 10 April 2025, https://www.ft.com/content/fba18bd9-46f9-4736-89f3-976afe3abf7a.

[21] Perez, Christian and Anjana Nair. "Information Warfare in Russia's War in Ukraine." *Foreign Policy*, Foreign Policy, 7 March 2023, https://foreignpolicy.com/2022/08/22/information-warfare-in-russias-war-in-ukraine/.

[22] "Oil Embargo, 1973–1974." *State.gov*, Office of the Historian, 2023, history.state.gov/milestones/1969-1976/oil-embargo.

[23] "Arab Oil Embargo." *Encyclopædia Britannica*, 20 March 2025, www.britannica.com/event/Arab-oil-embargo.

[24] Mueller, Robert S.. *Report On The Investigation Into Russian Interference In The 2016 Presidential Election*, U.S. Department of Justice, March 2019.

[25] Rasha, Abdulla. "Egypt's Media in the Midst of Revolution*." Carnegie Endowment for International Peace*, 16 July 2014, carnegieendowment.org/2014/07/16/egypt-s-media-in-midst-of-revolution-pub-56164.

[26] "Civil Movements: The Impact of Facebook and Twitter." *Arab Social Media Report*, *Dubai School of Government*, journalistsresource.org/wp-content/uploads/2011/08/DSG_Arab_Social_Media_Report_No_2.pdf.

[27] Ebrahim, Nadeen. "Middle Eastern Regimes Have a History of Shutting Down the Internet. But it's Costing Them." *CNN*, Cable News Network, 3 July 2023, www.cnn.com/2023/07/03/middleeast/middle-east-internet-shutdowns-mime-intl/index.html.

[28] Mueller, Robert S.. *Report On The Investigation Into Russian Interference In The 2016 Presidential Election*, U.S. Department of Justice, March 2019.

[29] Cronin, Audrey. "How Private Tech Companies Are Reshaping Great Power Competition." *Johns Hopkins SAIS*, 21 February 2024, https://sais.jhu.edu/kissinger/programs-and-projects/kissinger-center-papers/how-private-tech-companies-are-reshaping-great-power-competition.

[30] Sauer, Pjotr. "Russia Bans Facebook and Instagram under 'Extremism' Law." *The Guardian*, 21 March 2022, www.theguardian.com/world/2022/mar/21/russia-bans-facebook-and-instagram-under-extremism-law.

[31] Perez, Christian and Anjana Nair. "Information Warfare in Russia's War in Ukraine." *Foreign Policy*, 2022, foreignpolicy.com/2022/08/22/information-warfare-in-russias-war-in-ukraine/.

[32] Wheeler, Tom. "Techlash: Who Makes the Rules in the Digital Gilded Age?" *Rowman & Littlefield*, 2023.

[33] Gordon, John Steele. "How Pierpont Morgan Saved the Gold Standard." *ABA Banking Journal*, 13 March 2020, https://bankingjournal.aba.com/2020/03/how-pierpont-morgan-saved-the-gold-standard/.

[34] Gordon, John Steele. "The Morgan Lineage in U.S. Financial History." *ABA Banking Journal*, 12 March 2021, bankingjournal.aba.com/2021/03/the-morgan-lineage-in-u-s-financial-history/.

[35] Moscrop, David. "Tech Titans Are the Robber Barons of Our Gilded Age." *Jacobin.com*, 13 March 2024, jacobin.com/2024/03/big-tech-apple-epic-regulations.

[36] Cronin, Audrey. "How Private Tech Companies Are Reshaping Great Power Competition." *Johns Hopkins SAIS*, 21 February 2024, https://sais.jhu.edu/kissinger/programs-and-projects/kissinger-center-papers/how-private-tech-companies-are-reshaping-great-power-competition.

[37] Posaner, Joshua. "EU to Help Ukraine Replace Musk's Starlink." *POLITICO*, 2 March 2025, https://www.politico.eu/article/eu-to-help-ukraine-replace-musks-starlink/.

[38] Satariano, Adam. "Elon Musk Doesn't Want His Satellites to Run Ukraine's Drones." *The New York Times*, 9 February 2023, https://www.nytimes.com/2023/02/09/world/europe/elon-musk-spacex-starlink-satellite-ukraine.html.

[39] Pollet, Mathieu. "Ukraine Is Stuck with Musk's Starlink for Now." *POLITICO*, 7 April 2025, www.politico.eu/article/ukraine-stuck-with-elon-musk-starlink-satellite-internet/.

[40] Satariano, Adam, Scott Reinhard, Cade Metz, Sheera Frenkel, and Malika Khurana. "Elon Musk's Unmatched Power in the Stars." *The New York Times*, 28 July 2023, https://www.nytimes.com/interactive/2023/07/28/business/starlink.html.

[41] Snyder, Miriam and Alison Kramer. "How Elon Musk Became a Powerful Player in Geopolitics." *Axios*, 25 October 2022, www.axios.com/2022/10/25/elon-diplomacy-starlink-ukraine.

[42] Snyder, Miriam and Alison Kramer. "How Elon Musk Became a Powerful Player in Geopolitics." *Axios*, 25 October 2022, www.axios.com/2022/10/25/elon-diplomacy-starlink-ukraine.

[43] Vick, Karl. "Inside the Clandestine Efforts to Smuggle Starlink Into Iran." *TIME*, 25 January 25 2023, https://time.com/6249365/iran-elon-musk-starlink-protests/.

[44] Vick, Karl. "Inside the Clandestine Efforts to Smuggle Starlink Into Iran." *TIME*, 25 January 25 2023, https://time.com/6249365/iran-elon-musk-starlink-protests/.

[45] Satariano, Adam, Scott Reinhard, Cade Metz, Sheera Frenkel, and Malika Khurana. "Elon Musk's Unmatched Power in the Stars." *The New York Times*, 28 July 2023, https://www.nytimes.com/interactive/2023/07/28/business/starlink.html.

[46]Jones, Julia Vargas, Stefano Pozzebon and Chris Lau. "Brazil Begins to Block X as Elon Musk's Feud with Judge Deepens." *CNN*, 30 August 2024. https://www.cnn.com/2024/08/30/business/brazil-suspends-x-elon-musk-moraes-intl-hnk/index.html.

[47] Tapper, James. "Elon Musk Backs Down in His Fight with Brazilian Judges to Restore X." *The Guardian*, 21 September 2024, https://www.theguardian.com/technology/2024/sep/21/elon-musk-backs-down-in-his-fight-with-brazilian-judges-to-restore-x.

[48] Srivastavsa, Swati. "Corporate Sovereign Awakening and the Making of Modern State Sovereignty: New Archival Evidence from the English East India Company." *Cambridge University Press,* 4 March 2022, https://www.cambridge.org/core/journals/international-organization/article/corporate-sovereign-awakening-and-the-making-of-modern-state-sovereignty-new-archival-evidence-from-the-english-east-india-company/FF618229BF140A5F1C0ED188F294784A.

[49] "East India Company | Definition, History, & Facts." *Encyclopedia Britannica*, 2019, www.britannica.com/topic/East-India-Company.

[50] Zhang, Helen. "Donald Trump Tariffs: Artificial Intelligence and Chips Are the New Battlegrounds for Global Power." *Australian Financial Review*, 21 April 2025, .www.afr.com/policy/foreign-affairs/the-next-global-crisis-won-t-be-about-oil-or-banks-but-tech-20250421-p5lt.

[51] Mariana Mazzucato and David Eaves, *Digital Public Infrastructure and Public Value* (2024).

[52] Shira Ovide, "How Apps Are Turning You into an Unpaid Lobbyist," *Washington Post*, March 26 2024, https://www.washingtonpost.com/technology/2024/03/26/tiktok-ban-lobbying-congress/.

[53] "Meta Fact-Checking Live Updates," *New York Times*, January 7 2025, https://www.nytimes.com/live/2025/01/07/business/meta-fact-checking.

[54] Lebow, Sara. "Generative AI Hits 100 Million User Milestone in US." *eMarketer.* July 30 2024. https://www.emarketer.com/content/generative-ai-hits-100-million-users-milestone-us.

[55] Zhaki Abdullah, "MOH Agency IHiS, Microsoft to Develop AI Tool to Help Healthcare Workers in Singapore," The Straits Times, July 8 2023, https://www.straitstimes.com/singapore/health/moh-agency-microsoft-to-develop-ai-tool-for-healthcare-workers-in-s-pore.

[56] Sam Nussey, "Microsoft to Supply AI Tech to Japan Government, Nikkei Reports," Reuters, July 26 2023, https://www.reuters.com/technology/microsoft-supply-ai-tech-japan-government-nikkei-2023-07-26/.

[57] Tamar Sharon, "Blind-Sided by Privacy? Digital Contact Tracing, the Apple/Google API and Big Tech's Newfound Role as Global Health Policy Makers," Ethics and Information Technology 23 (2021): 45–57, https://doi.org/10.1007/s10676-020-09547-x.

[58] Sweney, Mark. "China to Take 'Golden Shares' in Tech Firms Alibaba and Tencent." *The Guardian*, 13 January 2023, www.theguardian.com/world/2023/jan/13/china-to-take-golden-shares-in-tech-firms-alibaba-and-tencent.

[59] "The Chinese Communist Party (CCP): A Quest for Data Control." *CIS*, 2024, www.cisecurity.org/insights/blog/the-chinese-communist-party-ccp-a-quest-for-data-control.

[60] Bosley, Shana. "New Court Decision: The FBI, Apple & the Company That Broke iPhone Encryption." *Abrams Fensterman, LLP*, 28 October 2017, www.abramslaw.com/media/thought-leadership/new-court-decision-the-fbi-apple-the-company-that-broke-iphone-encryption/.

[61] Derico, Ben. "Brazil Lifts Ban on Elon Musk's X after It Pays $5m Fine." *BBC.com*, BBC News, 8 October 2024, www.bbc.com/news/articles/c5y06vzk3yjo.

[62] Derico, Ben. "Brazil Lifts Ban on Elon Musk's X after It Pays $5m Fine." *BBC.com*, BBC News, 8 October 2024, www.bbc.com/news/articles/c5y06vzk3yjo.

[63]"Microsoft Corp. V. United States." *Harvard Law Review*, 9 December 2016, https://harvardlawreview.org/print/vol-130/microsoft-corp-v-united-states/.

[64]"Microsoft Corp. V. United States." *Harvard Law Review*, 9 December 2016, https://harvardlawreview.org/print/vol-130/microsoft-corp-v-united-states/.