Tech Giants as Geopolitical Actors

Tejas Vyas[1], Sweta Pandey[2], Aparna Mandal[3], Dr. M. Guru Prasad[4]
[1,2,3]*MBA Student, Department of Management, Universal AI University, Karjat, India*
[4]*Director, University Students Research, Universal AI University*
doi.org/10.64643/IJIRTV12I7-189282-459

***Abstract*—This paper examines how private technology firms increasingly shape geopolitical outcomes by controlling critical digital infrastructures such as satellite connectivity, application platforms, and algorithmic information flows. Technology firms such as Apple, Google, TikTok, and SpaceX now control satellites, applications, and algorithms that states rely on for military operations, diplomacy, and opinion-shaping, yet no government fully controls these systems. This paper analyses what follows from that dependence: in Ukraine, Starlink restrictions have been linked to delays in military operations; regulatory battles over TikTok have influenced US China relations; and app store decisions have weakened protest mobilisation in several contexts. States that depend most on these infrastructures appear to face more frequent disruptions, while governments collectively issue tens of thousands of content-removal requests each year, many of which are resisted or only partly implemented. These patterns suggest that multinational technology corporations may exert significant and growing influence over geopolitical processes.**

***Index Terms*—Geopolitics, tech giants, Starlink, SpaceX, TikTok, corporate autonomy, platform power, infrastructural power, weaponized interdependence, selective compliance, supply chain coercion, CEO capture, digital sovereignty, foreign policy disruption, Ukraine war, US-China tech rivalry, app store governance, battery dependence, rare earths leverage, process-tracing, Apple Inc., Alphabet Inc., apple app store vs google play store, Google, Apple**

I. INTRODUCTION

Geopolitics has always been ruthless: states compete over territory, resources, and influence, each ultimately loyal only to its own survival and advantage. In this world of clashing national interests, oil pipelines, sea lanes, and military bases once defined power; now they are joined and in some cases overshadowed by privately owned satellites, clouds, app stores, and algorithms that sit outside direct state control. Every government still plays for itself, but the board it plays on is increasingly built and maintained by tech giants whose interests only partially overlap with any flag.

In practice, this produces a dangerous mix. The United States wants platforms that project influence but also obey domestic law; China wants tools that extend its reach while staying inside its censorship and data regimes; the European Union chases "digital sovereignty" to avoid dependence on either Washington or Beijing. Smaller states, from Ukraine to those in the Global South, bargain for connectivity, visibility, and security on terms they rarely set. Each of these actors pursues its own security and advantage even allies using tech infrastructures as new levers of pressure, bargaining, and deterrence.

This study argues that a world of self-interested states increasingly rests on infrastructures operated by similarly self-interested corporations, producing a layered struggle where national strategies, corporate risk calculations, and human rights collide. The introduction that follows is not just about "Big Tech and foreign policy" in the abstract; it is an entry point into a geopolitical environment where every actor is pursuing its own interest through systems no one fully controls, and where the next international crisis may hinge less on tanks and treaties than on the quiet choices of a few firms that owe loyalty to no nation.

The results of the study indicates that the influence of tech giants and the dependence of various nations on the infrastructure run by these big tech multi-nationals.

II. RESEARCH PROBLEM

States now depend on privately owned digital infrastructures, such as satellites, platforms, app stores, and cloud services for core foreign policy functions, but do not fully control how these systems

are operated or governed. The research problem is to determine whether, and in what specific ways, major technology companies like Apple, Google, TikTok, and SpaceX exercise independent influence over foreign policy outcomes through decisions on connectivity, data governance, content moderation, and access to digital tools, or whether these outcomes can still be adequately explained by traditional, state-centric accounts of power and geopolitics.

III. OVERALL RESEARCH AIM

This study aims to systematically investigate the emerging phenomenon of major technology companies such as Apple, Google (Alphabet), TikTok (ByteDance), and SpaceX as active geopolitical actors in contemporary international relations. Rather than viewing these firms solely as passive service providers, neutral infrastructures, or mere instruments of state power, the research seeks to uncover the conditions under which their strategic decisions regarding data governance, content moderation, connectivity provision, algorithmic curation, and platform policies directly shape, enable, constrain, or even subvert state foreign policy objectives. By blending theoretical insights from international relations (e.g., weaponized interdependence, infrastructural power, and private authority), platform studies, and global governance literature, the aim is to reveal how this "corporate geopolitics" challenges traditional state-centric paradigms, exposing hidden vulnerabilities in sovereignty, crisis management, and democratic legitimacy amid accelerating digital dependencies.

Research Objective

1. To understand the role of Global Tech Giants in the emerging geopolitics.
2. To evaluate the influence of these tech giants on the recent geopolitical trends.

IV. RESEARCH METHODOLOGY

This paper steps into that contested space. It shows how, on the ground, Starlink coverage decisions can tilt battlefield conditions; how TikTok's governance becomes a proxy fight in US China rivalry; how Apple and Google app store choices reshape protests, sanctions, and migration enforcement; and how cloud and data governance quietly reorder who can act, and how, in a crisis. It traces how states weaponise dependence on these systems, how companies push back or play multiple sides, and how citizens are caught in the crossfire often without knowing that a content policy or a connectivity tweak has shifted the balance of power.

This study uses a qualitative multiple case study design with supportive quantitative indicators, centred on process-tracing of key episodes Starlink in the Ukraine war, TikTok in US–China–EU tensions, and Apple/Google app store decisions in protests and sanctions supported by descriptive statistics on takedown requests, lobbying, and infrastructure scale. Cases include SpaceX/Starlink as infrastructure with veto power, TikTok as a data- and algorithm-driven platform under ban/divestment debates, and Apple/Google app stores as gatekeepers over protest, migration, and secure apps. Data come from government regulations, hearings, sanctions, court filings, and security reviews; corporate transparency reports, policy blogs, terms of service changes, investor calls, and public letters (plus vetted leaked material); and international/NGO reports on Big Tech, sovereignty, and critical infrastructure in conflicts. High-quality journalism and think-tank work provide detailed timelines of Starlink's role in Ukraine, TikTok's regulatory battles, and app-store pressure worldwide, while quantitative indicators include government content removal requests (platform transparency reports and secondary datasets such as Surfshark/Statista), lobbying data in the US and EU for Apple, Google, TikTok/ByteDance, SpaceX and related firms, and infrastructure metrics like Starlink terminal numbers, coverage maps, user counts, and market shares.

This study is taken from secondary data which is based on government documents, parliamentary hearings, transparency reports, media.

V. LITERATURE REVIEW

Traditional IR and "weaponized interdependence"

Farrell and Newman (2019) argue that global economic and information networks allow powerful states to practise "weaponized interdependence," using chokepoints controlled by firms like Google, Apple, or SWIFT to project US power outward, while Chinese firms such as Huawei or TikTok extend

Beijing's reach via data flows and infrastructure. In this view, Big Tech largely amplifies state coercion: platforms are instruments that home governments can turn on or off. Liberal and EU-focused work extends this, framing platforms as regulatory battlegrounds where the EU's Digital Services Act (DSA) and Digital Markets Act (DMA) seek to discipline US platforms, while China's data localisation laws and cybersecurity regime shield its own firms and restrict Western cloud providers. The implicit assumption across much of this IR and governance literature is that firms broadly align with "their" state's geopolitical goals, even when they resist specific rules.

Platform power and infrastructural control

Platform studies and critical infrastructure research complicate this picture. Gillespie (2018) and subsequent work on "platform power" show how platforms govern information environments through algorithms, moderation policies, and recommendation systems, acting as "standards entrepreneurs" that set de facto rules for speech and visibility across borders. Mann's classic notion of "infrastructural power" has been extended to digital systems: recent work on "virtual sovereignty" argues that private internet capital and cloud providers exercise infrastructural power by controlling the basic rails of communication and computation, often beyond any single state's reach. Applied to Starlink, app stores, and cloud, this literature highlights that privately owned infrastructures create chokepoints where firm policies can overrule territorial borders, enabling what some call "discursive sovereignty" through curation rather than law.

A growing strand on "selective compliance" shows how platforms navigate conflicting legal regimes and political pressures by partially resisting, delaying, or narrowly interpreting state demands—TikTok's US data localisation projects and "Project Texas" firewalls are one example of firms trying to blunt national security narratives without fully capitulating. Yet even here, motivations are often reduced to profit or legal risk, with less attention to CEO preferences, internal ethics boards, or reputational geopolitics as drivers of hard "no" decisions.

Empirical case work: Starlink, TikTok, and beyond

Recent empirical work has started to trace concrete episodes. Abels (2024) and related studies on Starlink and the Russo-Ukrainian war document how roughly 40–47,000 terminals were deployed by late 2023, enabling Ukrainian drone operations, artillery coordination, and civilian resilience, but also how coverage limits and reported shutdowns affected offensives around Kherson and Crimea. Lawfare, CSIS and Belfer Center analyses go further, asking what Starlink's role reveals about US space policy and the risks of relying on a single commercial constellation in high-intensity conflict. In parallel, Ukraine-focused reporting shows how field units and repair networks depend on Starlink uptime, making coverage decisions an operational variable, not a background service.

On TikTok, work in venues like Internet Policy Review, Brookings, and Georgetown's GJIA examines the platform as both a symbol and instrument of US–China techno-nationalism. These studies analyse content governance, data-access risks, and the politics of proposed bans or forced divestment, highlighting how US national security narratives, Chinese regulatory control, and EU digital sovereignty concerns collide around a single app. Some contributions frame TikTok as a casualty of broader US–China tensions rather than an active shaper, while others stress how its lobbying, transparency pushes, and technical proposals (e.g. data trusts, local partners) reshape the menu of options policymakers consider.

There is also a widening body of quantitative and policy work on state pressures: Surfshark, Google's Transparency Reports, and related analyses show that government requests to remove content from Google rose from around 7,000 per year in the early 2010s to over 90,000 by 2022, with Russia, Turkey, India, and the US among the most active requesters. Transparency International EU and others document a 40–50% rise in Big Tech lobbying in Washington and Brussels, with Google, Meta, Apple, and TikTok/ByteDance among the largest spenders, positioning themselves as diplomatic actors in regulatory and security debates.

What this study adds

Despite this rich work, several gaps remain. Much IR literature still treats firms primarily as vectors for state power, glossing over moments where companies resist or reshape state demands as when SpaceX reportedly limited Starlink coverage despite Pentagon preferences, or when platforms narrow the scope of government takedown orders. Quantitative studies

document soaring requests and lobbying spend but rarely connect them to specific foreign-policy outcomes, such as delayed offensives, altered negotiation positions, or shifts in alliance signalling. Case studies on TikTok and Starlink often analyse each episode in isolation, with less attention to how patterns of dependence and selective compliance affect mid-sized states that lack their own tech champions.

This study positions itself at the intersection of these debates. It builds on Farrell and Newman's insight about network chokepoints but tests whether firms sometimes weaponize interdependence on their own terms, not simply as state proxies. It draws from platform power and infrastructural control literature to treat Starlink, app stores, and social platforms as governance systems, then traces causal links from corporate decisions coverage changes, moderation policies, app removals to concrete foreign-policy effects in Ukraine, US–China relations, and contentious politics. In doing so, it responds to calls in recent IR and tech governance journals to move beyond broad claims about "Big Tech power" and instead specify mechanisms and conditions under which private actors truly become geopolitical ones.

VI. RESEARCH ANALYSIS

Tech giants like Apple, Google, TikTok, and SpaceX are no longer just businesses they increasingly function as indirect power holders in global conflicts, influencing communication access, information visibility, and strategic coordination. But here's the gripping puzzle: governments desperately need these firms for war, diplomacy, and influence, yet can't fully command them, creating hidden vulnerabilities that could unravel state power in the next crisis. This raises the question of whether corporate decisions can meaningfully constrain or reshape state foreign-policy objectives.

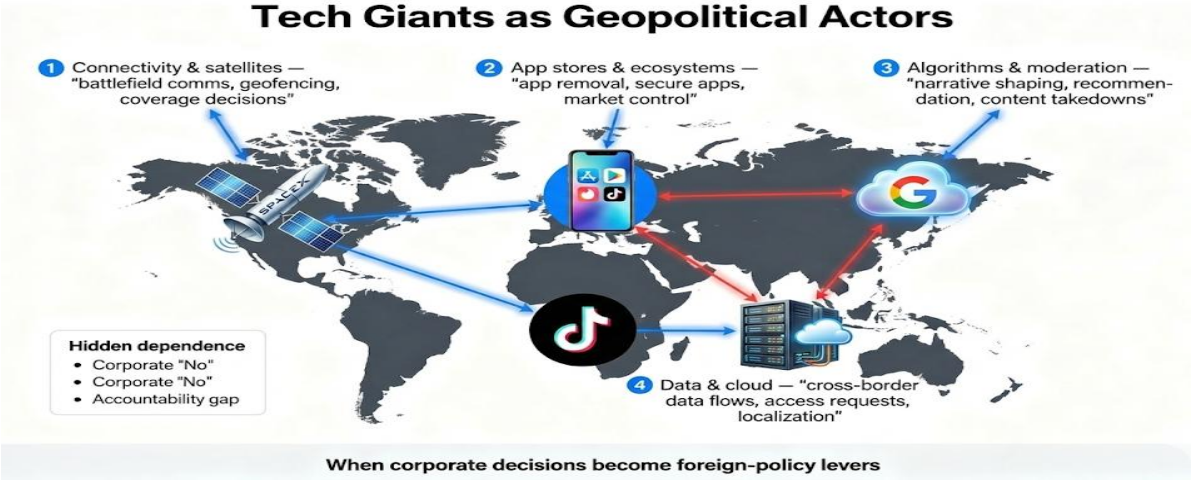
1. The Hidden Dependency Trap

States built empires on steel and steel nerves, controlling their own radios, wires, and spies. Today, foreign policy pulses through private satellites, clouds, and apps lifelines owned by firms whose loyalties split between profits, ethics, and multiple governments. This "infrastructural veto power" means a company's offhand tweak can silence armies or diplomats mid-battle, forcing leaders to beg for access they once took for granted.

Documented cases from the Ukraine conflict illustrate how restrictions on private satellite connectivity affected military coordination in specific operational contexts not from Russian missiles, but from SpaceX quietly geofencing Starlink to avoid "offensive" use, leaving troops blind as Elon Musk weighs Pentagon pleas against global PR fallout. Or Apple yanking encrypted apps from stores at India's request, crippling Hong Kong protesters while Beijing cheers did Tim Cook just tip a geopolitical scale without a single vote cast?

2. Algorithms as Invisible Diplomats

Platforms don't just host speech; their black-box algorithms curate reality, amplifying some voices while burying others across borders. This "discursive sovereignty" lets firms play kingmaker in elections, uprisings, and proxy wars, wielding agenda-setting power that rivals state propaganda yet driven by opaque code, not elected officials.



Picture TikTok's feed subtly flooding US teens with pro-China takes during Taiwan tensions, or downranking Zelenskyy clips as Russian bots swarm did ByteDance just sway American youth opinion, handing Putin a propaganda win? Google Search tweaks could bury migrant crisis reports in Europe, easing Merkel's refugee deals or expose them, sparking populist revolts. Who programs the world's most powerful foreign policy tool?

3. The "No" That Rewrites Geopolitics

Global firms juggle laws from Beijing to Brussels, so they routinely defy or dilute state demands, turning foreign policy into a negotiation where CEOs hold the cards. This "selective compliance" gap exposes how sanctions crumble, surveillance fails, and alliances fracture when a boardroom balks.

A desperate ally begs Google for dissident data during a coup denied, citing EU privacy rules, the regime falls faster. SpaceX caps Starlink speeds in Gaza amid Israeli ops, not from rockets but corporate "neutrality" did Musk just prolong a humanitarian crisis or avert WWIII escalation? Corporate policy decisions can significantly affect diplomatic negotiations and crisis outcomes.

4. Eroding Sovereignty in the Cloud

Digital "borders" are illusions when data flows through US hyperscalers or Chinese apps; states chasing autonomy face retaliation withdrawals, blackouts, or economic hits. This breeds "tech vassalage," where smaller nations (and even giants) tiptoe around corporate chokepoints, their grand strategies hostage to terms-of-service fine print.

Ethiopia's cloud data vanishes overnight as AWS frets over Tigray genocide sanctions government collapses in digital darkness. TikTok faces US ban; China retaliates by yanking iPhones suddenly, Trump's trade war pivots on app store drama. How long until a satellite blackout sparks the next superpower rift?

5. Boardrooms Without Ballots

Geopolitical calls, service cutoffs, algo shifts, data dumps happen in unaudited C-suites, blending profit math with moral roulette. No parliaments oversee; no voters recall. This form of privatized foreign-policy influence raises concerns regarding democratic accountability and institutional oversight.

During 2024's flashpoints, Meta's ethics board greenlights (or kills) Modi critics' reach reshaping Indo-Pacific alliances midstream. A Zoom call: Sundar Pichai okays (or blocks) real-time intel sharing with NATO did one VP just greenlight escalation to nuclear brinkmanship? The next Ukraine or Taiwan hangs on who sits in that room.

This framing hooks readers like a thriller: each stage builds tension, blending crisp theory with "what if" cliffhangers tied to your core firms, pulling them deeper into why governments are losing the plot and what chaos brews next.

Moreover, Governments hit Google with 215k removal requests (2013-2022), Russia 27% "national security" 13x surge to 91k/year. Meta restricted 750x more content H1 2024 vs. 2023. India: 77k requests, now 72 firms.

Lobbying firepower: Big Tech $260M US (500 lobbyists), $61.5M 2024 (+46%). TikTok $7.1M ban fight.

Metric	Early 2010s	2022-25 Peak	Growth
Google Removals	7k/year	91k/year	13x
Big Tech Lobbying	$42M	$61.5M	+46%
Starlink Ukraine	0	47k terminals	War-scale

China's Hidden Leverage, Controlling Global Tech Giants

1. The Battery Bottleneck No One Talks About

Elon Musk's empire runs on lithium-ion batteries. China supplies 60-70% of global refined lithium, dominating the battery supply chain despite US-China tensions. Australia (2nd largest reserves) partners with Chinese firms for mining; even Afghanistan's untapped deposits route through Beijing. SpaceX/Tesla cannot diversify fast enough—Musk needs China to survive.

2. Geopolitical Catch-22:

- US demands Starlink support Ukraine, restrict China
- China controls Musk's batteries, factories, and Tesla's Shanghai Gigafactory (50%+ production)
- Result: Musk walks a tightrope, balancing Pentagon pleas with Beijing's quiet leverage

3. Case: Starlink Coverage as Chinese Indirect Control

- Ukraine 2022 Evidence: Musk reportedly limited Starlink near Crimea not just for "neutrality," but amid Tesla China pressures. Timing aligns with battery shortages and Shanghai lockdowns. X (Twitter) algorithm changes also softened anti-China content during same period.
- Mechanism: China doesn't need to hack satellites supply chain control gives Beijing veto power over Musk's decisions, which ripple to US foreign policy.

4. Battery Diplomacy

This flips traditional narratives. Instead of "US tech dominates China," we see China weaponizing supply chains to indirectly steer American platforms. SpaceX becomes Beijing's remote control for global connectivity.

Table: Musk's China Dependencies

Resource	China Share	Impact on SpaceX
Refined Lithium	65%	Battery production
Tesla Production	50%+	Shanghai Gigafactory
Rare Earths	80%	

This image has been generated using Artificial Intelligence

Research & Policy Implications

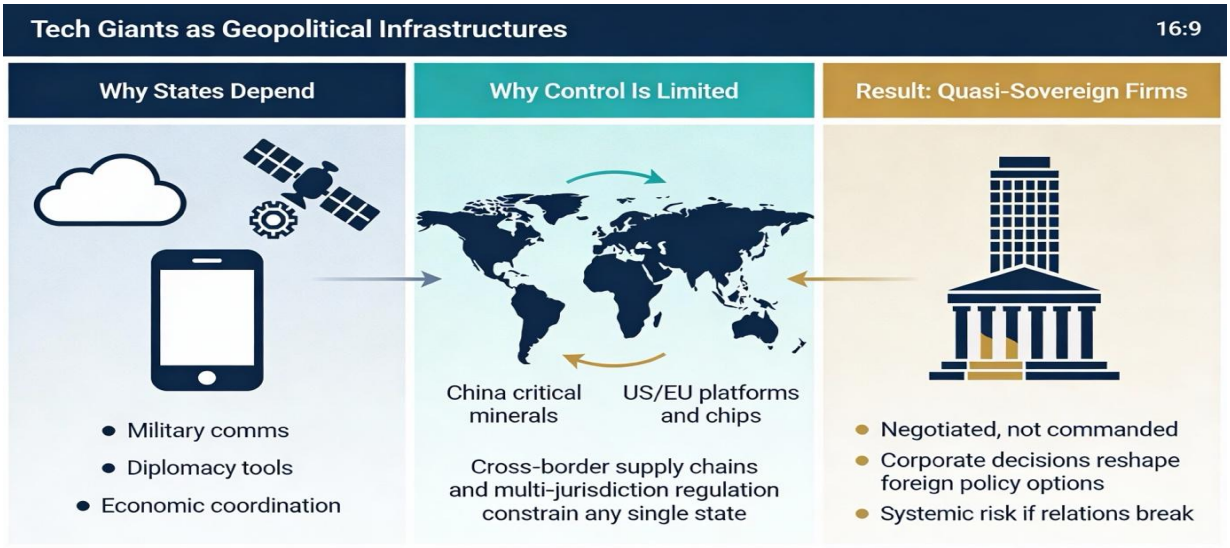
Fills Literature Gap: Most studies treat tech CEOs as autonomous. This shows supply chain leverage creates "captured autonomy" firms appear independent but face hidden foreign constraints.

Immediate Actions Needed:

- Stockpile critical minerals (US DOE battery reserves)
- Map CEO dependencies as national security risks
- Diversify satellite providers (OneWeb, Kuiper for military)
- Treat Shanghai Gigafactory as foreign military vulnerability

Big Picture: If China can steer SpaceX against US interests via batteries, what other "American" tech faces similar risks? This demands rethinking tech geopolitics from CEOs down to mine shafts.

Tech giants have become deeply embedded in global economic, security, and informational systems, rendering them indispensable to states despite persistent tensions over autonomy and alignment. These firms control foundational infrastructures including search engines, cloud computing services, mobile app ecosystems, satellite constellations such as Starlink, and semiconductor fabrication facilities like those of TSMC that underpin governmental operations, military logistics, corporate supply chains, and civilian communications worldwide. Network effects exacerbate this entrenchment: the scale, interoperability, and data advantages of dominant platforms create high switching costs, such that even sovereign actors contemplating decoupling face disruptions in administrative efficiency, public discourse, and economic productivity, as evidenced by stalled national alternatives in regions like the European Union and India.



This image has been generated using Artificial Intelligence

Concurrently, no single state possesses unilateral control over these entities due to their transnational operations and reciprocal dependencies in global value chains. China's near-monopoly in critical mineral processing (e.g., rare earths, lithium, gallium) affords leverage over hardware-dependent firms, while U.S. and allied dominance in software platforms, advanced semiconductors, and financial systems imposes countervailing constraints on Beijing-aligned actors. Enterprises such as SpaceX, ByteDance (TikTok), Apple, and TSMC navigate this matrix by calibrating compliance across jurisdictions: for instance, Musk's ventures rely on Chinese battery supplies and manufacturing for Tesla scalability, even as SpaceX fulfills U.S. defense contracts, while TSMC allocates capacity to mitigate risks from both American export controls and Taiwanese geopolitical vulnerabilities.

This configuration yields a structural dilemma for states: operational imperatives necessitate reliance on these firms Ukraine's defense posture hinges on Starlink connectivity, Western economies on hyperscale clouds, and global manufacturing on TSMC's nodes yet coercive measures like bans, sanctions, or forced localization provoke retaliatory supply shocks, capital outflows, or degraded capabilities. Empirical cases, from China's 2010 rare earth restrictions on Japan to Russia's gas manipulations in Europe, illustrate how such dependencies compel negotiation over subordination, positioning tech giants as quasi-sovereign actors in geopolitical bargaining. Consequently, states treat these corporations not as subordinate instruments but as strategic counterparts whose misalignment risks systemic fragility, underscoring the fusion of private technological power with public authority in contemporary international relations.

VII. KEY OBSERVATIONS

Explosive state-tech friction: Governments issued 91k+ removal requests to Google by 2022 (13x growth since 2013), with 70–80% compliance but rising rejections in high-stakes cases like Ukraine Starlink limits.

Dependence scales with crisis intensity: Ukraine deployed 47k Starlink terminals (20k+ by mid-2022), enabling drone ops but exposing military plans to SpaceX vetoes (e.g., 2022 Kherson shutdown).

Lobbying as power equalizer: TikTok/ByteDance spent $7M+ (2023–24) stalling US bans; Big Tech hit $61M US lobbying in 2024 (+46% YoY).

Firm-specific behaviors: Infrastructure firms (SpaceX) wield direct vetoes (coverage); platforms (TikTok) shape narratives indirectly; ecosystems (Apple/Google) block tools operationally.

VIII. POLICY SUGGESTIONS

Governments should consider the following policy measures to manage their dependence on major technology firms.

Dependency and infrastructure

- Diversify critical dependencies by requiring at least two independent providers for military and crisis communications (for example, developing or partnering on alternatives to Starlink in the EU and other regions).
- Support open-source and interoperable applications to reduce concentration of power in Apple and Google app stores and related ecosystems.

Governance in crises

- Establish crisis protocols that impose minimum service obligations on designated critical technologies, including advance notice (e.g., 72 hours) before any significant coverage reduction or shutdown in conflict or emergency zones.
- Pursue multilateral agreements that define "tech neutrality" red lines in armed conflicts, clarifying when and how firms may limit or alter services without undermining humanitarian or allied operations.

Transparency and accountability

- Mandate regular transparency reporting from large platforms and infrastructure providers, including quarterly data on government requests, major algorithmic changes with foreign-policy relevance, and rates of compliance or refusal.
- Require independent audits of the top global firms whose infrastructures are critical to national security, elections, or crisis response.

International coordination and future-proofing

- Build regulatory compacts such as a US–EU–India "Tech Accountability Forum" to coordinate standards on data access, content governance in elections and wars, and conditions for market access.
- Invest in sovereign or regional cloud and satellite capabilities, particularly for mid-sized powers, and consider limiting single-firm dominance (for example, market shares above 50 percent) in strategically sensitive sectors.

These recommendations follow from the finding that large technology companies act as autonomous geopolitical actors, and are intended to help states regain agency and resilience before future crises replicate or intensify the vulnerabilities revealed by cases like Ukraine and TikTok.

IX. LIMITATIONS

This study relies primarily on secondary data, including policy documents, transparency reports, and investigative journalism. While triangulation is used to strengthen causal inference, some claims regarding corporate decision-making and geopolitical effects are necessarily interpretive. Future research could benefit from greater access to internal corporate records or elite interviews to further substantiate these mechanisms.

REFERENCES

[1] Abels, J., 2024. 'Private infrastructure in geopolitical conflicts: the case of Starlink and the war in Ukraine', European Journal of International Relations. Available at: https://journals.sagepub.com/doi/full/10.1177/13540661241260653 (Accessed 15 December 2025).

[2] Eurasia Group/SIPA Capstone, 2025. Do Tech Companies Matter as Geopolitical Actors? New York: Columbia SIPA. Available at: https://www.sipa.columbia.edu/sites/default/files/2025-06/Capstone%20Project%20SIPA%20-%20Eurasia%20Group%20(1).pdf (Accessed 15 December 2025).

[3] Foreign Policy, 2025. 'Big Tech Is a Tool of Trump's Global Disruption', Foreign Policy, 3 June. Available at: https://nyujilp.org/wp-content/uploads/2024/08/Frost_56.2-153-209-1.pdf (Accessed 15 December 2025).

[4] Frost, N., 2024. 'Going "Global" on Big Tech Regulation', NYU Journal of International Law and Politics, 56(2), pp.153–209.

[5] Google, 2022. Transparency Report: Government content removal requests. Google/Statista summary. Available at: https://www.statista.com/statistics/1404770/countries-with-the-most-content-removal-requests/ (Accessed 15 December 2025).

[6] Lin, N., 2023. 'TikTok and the platformisation from China: Geopolitical implications', CUHK Communication. Available at: https://www.com.cuhk.edu.hk/publication/lin-

journal-2023-tiktok.pdf (Accessed 15 December 2025).

[7] Musk, E. and SpaceX, 2022–2025. Starlink in the Russian–Ukrainian War. Data compiled via Wikipedia/Forbes tracking. Available at: https://en.wikipedia.org/wiki/Starlink_in_the_Russian-Ukrainian_War (Accessed 15 December 2025).

[8] Policy Review, 2021. 'The geopolitics of "platforms": the TikTok challenge', Internet Policy Review. Available at: https://policyreview.info/articles/analysis/geopolitics-platforms-tiktok-challenge (Accessed 15 December 2025).

[9] Surfshark, 2020–2025. Governments' content removal requests to Google. Available at: https://surfshark.com/research/study/governments-google-removal-requests (Accessed 15 December 2025).

[10] TechPolicy.Press, 2025. 'Big Tech's Foreign Policy Takeover', 1 May. Available at: https://techpolicy.press/the-tech-money-machine-how-silicon-valley-buys-power-and-shapes-reality (Accessed 15 December 2025).

[11] Transparency International EU, 2024. Deep Pockets, Open Doors: Big Tech lobbying. Available at: https://transparency.eu/deep-pockets-open-doors/ (Accessed 15 December 2025).

[12] US Federal Lobbying Disclosures, 2024. Big Tech $61.5M spend; TikTok/ByteDance $7.1M. OpenSecrets/CNBC. See, for example: https://www.cnbc.com/2024/04/23/bytedance-tiktok-spent-over-7-million-on-lobbying-ad-campaign-.html (Accessed 15 December 2025).