Routledge
Taylor & Francis Group

Review of International Political Economy

ISSN: 0969-2290 (Print) 1466-4526 (Online) Journal homepage: www.tandfonline.com/journals/rrip20

Weaponised interdependence in a bipolar world: how economic forces and security interests shape the global reach of US and Chinese cloud data centres

Vili Lehdonvirta, Boxi Wú & Zoe Hawkins

To cite this article: Vili Lehdonvirta, Boxi Wú & Zoe Hawkins (2025) Weaponised interdependence in a bipolar world: how economic forces and security interests shape the global reach of US and Chinese cloud data centres, Review of International Political Economy, 32:5, 1442-1467, DOI: 10.1080/09692290.2025.2489077

To link to this article: https://doi.org/10.1080/09692290.2025.2489077

REVIEW OF INTERNATIONAL POLITICAL ECONOMY
2025, VOL. 32, NO. 5, 1442–1467
https://doi.org/10.1080/09692290.2025.2489077

Weaponised interdependence in a bipolar world: how economic forces and security interests shape the global reach of US and Chinese cloud data centres

Vili Lehdonvirta[a,b], Boxi Wú[b] and Zoe Hawkins[b]

[a]Oxford Internet Institute, University of Oxford, Oxford, United Kingdom; [b]Department of Computer Science, Aalto University, Espoo, Finland

ABSTRACT

United States (US) and Chinese technology companies dominate digital networks. What explains the extent to which third countries attach to US versus Chinese network hubs? The answer matters, because both governments have demonstrated the ability to 'weaponise' their hubs to advance their security interests. We synthesise three hypothetical explanations for third countries' network hub attachment from previous qualitative literature: (1) Network hub attachment is a product of economic forces; (2) network hub attachment is determined by rivaling great powers coaxing and coercing third countries to attach to their hubs over their rival's; and (3) network hub attachment results from third-country governments' strategic policy choices. In the first quantitative study on the topic, we assess these explanations with original data on the global geography of US and Chinese -owned hyperscale cloud infrastructures. Based on the findings, we argue that third countries or 'spoke states' enjoy agency in bipolar networks which they did not have in unipolar networks, and that their strategic interests in combination with economic forces shape the topology of geographically distributed bipolar networks more so than great-power rivalry. Our model contributes to the weaponised interdependence framework which predicted the rise of alternative hubs but lacked a model of bipolar network topology.

ARTICLE HISTORY Received 20 December 2023; Accepted 26 February 2025

KEYWORDS Technological dependence; weaponised interdependence; cloud computing; big tech; digital infrastructure; tech war; digital sovereignty; bipolar networks; geoeconomics

Introduction

The United States (US) and China have emerged as the world's two digital superpowers, in the sense that they are the two countries least dependent on foreign

CONTACT Vili Lehdonvirta vili.lehdonvirta@oii.ox.ac.uk Oxford Internet Institute, University of Oxford, Oxford, United Kingdom; Department of Computer Science, Aalto University, Espoo, Finland.

Supplemental data for this article can be accessed online at https://doi.org/10.1080/09692290.2025.2489077.

digital infrastructures—such as search engines, social media platforms, and cloud computing services—while other countries are to varying extents dependent on their infrastructures (Mayer & Lu, 2023; Evans & Gawer, 2016). Which countries rely on which of the two powers' infrastructures? The answer matters, because the two governments increasingly position one another as geopolitical rivals in a binary competition for global supremacy, in which digital infrastructures play an instrumental role (Farrell & Newman, 2019a; Gray, 2021).

To understand digital infrastuctures as sources of power and dependence between states, many scholars of international political economy (IPE) have in recent years turned to the so-called weaponised interdependence framework (Farrell & Newman, 2019a; 2023). In the language of weaponised interdependence, the US and China possess many 'hubs' in global digital networks, while other countries attach to their hubs as 'spokes'. Both governments have demonstrated the ability to 'weaponise' their hubs' central positions in network topologies for espionage, surveillance, censorship, and/or blockades against people, organisations, and governments abroad (Cartwright, 2020; Farrell & Newman, 2016; Kello, 2022).

A key question in this literature has been how such network topologies conducive to weaponisation by certain states against certain others emerge in the first place. In the original weaponised interdependence framework, the topology of global networks was seen mainly as a product of blind economic forces (Farrell & Newman, 2019a, 2023). Positive network effects (Katz & Shapiro, 1994), preferential attachment (Barabási & Albert, 1999), and learning-by-doing (Gulati, 1999) ensured that networks coalesced around a small number of large hubs. That these hubs predominantly emerged in the US and Western Europe was seen to result from these regions' first-mover advantages in new technology industries more than from any conscious political project to obtain commanding positions in global networks (Gjesvik, 2023).

However, once policy makers realised that US network hubs could be weaponised, network topology turned into a political matter. Other governments began to promote alternative hubs, with the most successful challengers arising from China (Rodrigues Vieira, 2023). TikTok challenged the dominance of Meta's social media platforms (Gray, 2021). Huawei's 5G networks challenged those of Ericsson and Nokia (Cartwright, 2020; Farrell & Newman, 2019b; Gonzalo et al., 2023). AliExpress and Temu challenged Amazon as the world's pre-eminent e-commerce hub (Shen & He, 2022). Proponents of the weaponised interdependence framework predicted the rise of such alternative hubs. But so far, the framework has not offered any explicit model of how the topology of such *bipolar* networks is shaped—what determines the extent to which a third country attaches to US versus Chinese hubs? As a result of its US-centricity, the original weaponised interdependence framework is increasingly considered insufficient for analysing contemporary networks (Rodrigues Vieira, 2023).

In this study, we use the case of cloud computing to extend the weaponised interdependence framework to bipolar networks. Cloud computing entails moving computation and data storage from end-user devices and organisations' own on-premises servers into very large data centres owned by cloud computing providers (Hu, 2016; Mosco, 2014). This demand aggregation and centralisation produces significant scale economies in operational costs, capital requirements, and energy efficiency (Masanet et al., 2020; Talukder et al., 2010). It turns computer server hardware from a capital asset duplicated by each organisation into a common infrastructure owned by a

provider serving many organisations. The global demand for cloud infrastructure is high, and many governments promote the uptake of cloud as a central part of their digital transformation and productivity agendas. For example, the European Union (EU) recently legislated that 'at least 75% of European enterprises should have taken up cloud computing services' by 2030 (European Union, 2022). New generative AI services in particular rely heavily on cloud computing (Lehdonvirta et al., 2024). Although businesses and public sector organisations can and do use cloud data centres situated in other countries, the most important data and workloads are often hosted in centres situated in their own territories, due to corporate policies or, increasingly, government data localisation rules (Ferracane, 2022).

However, the ownership of cloud computing infrastructures is heavily polarised. US-based Amazon Web Services (AWS), Microsoft Azure, and Google Cloud control roughly 70% of the market for on-demand cloud computing infrastructure services globally, while Chinese tech giants Alibaba, Huawei, and Tencent control much of the remaining 30%. These leading cloud providers are called 'hyperscalers', in part because their infrastructures allow other organisations to rapidly 'scale up' their computation and data storage use on demand (Narayan, 2022). The term also reflects the enormous scale of these providers' operations, as each provider operates a globe-spanning network of giant data centres meshed together with private fiber-optic undersea cables. Another term used to describe these providers' services is 'public cloud'. The term originally refers to the fact that the services are available to the general public over the Internet, but today it also reflects the public service -like role that hyperscale cloud computing has come to play in digitalised societies. Like search engines and social media platforms, cloud thus fits a classic definition of infrastructure as (private) 'capital that provides a public service' (Hirschman, 1958).

Cloud computing infrastructures and the hyperscalers that operate them can in principle be weaponised as other network hubs have been in the past. The US Cloud Act of 2018 and Foreign Intelligence Surveillance Act Section 702 can empower authorities to access data held by US companies regardless of where in the world the data centre is physically located (Abraha, 2019, 2021). China's National Intelligence Law is thought to have comparable effects (Ruan, 2018). Both governments could moreover deny access to cloud services to sanctioned entities. At 10:30 ET on 7 December 2021 numerous digitally enabled services suddenly froze in the eastern United States (Greene, 2020). Roomba robots stopped moving, mobile banking apps didn't respond, fulfilment warehouses came to a standstill, and Ring security camera feeds cut out. The reason was a brief accidental outage at one AWS data centre in Virginia, but the incident hints at the crippling effects that denial of service could have on financial activity, security systems, and critical infrastructure in a country reliant on cloud. Complete, sustained loss of access to cloud infrastructure would be an 'extreme cyber risk scenario'—very unlikely but potentially very disruptive (Eling et al., 2023).

In such a high-stakes network, why is a given third country more attached to hubs associated with one of the powers than another? We use previous qualitative studies to synthesise three hypothetical explanations. The first is that network hub attachment is a product of economic forces: Countries are more likely to be attached to hubs from those countries that they trade with. The second hypothetical explanation is that network hub attachment is determined by great power rivalry: US and Chinese governments coax and coerce third countries to associate

with their own hubs and to reject their rival's. The third explanation is that network hub attachment results from strategic policy choices made by the third-country governments: Governments steer their economies to attach to those hubs that better align with their national and economic security interests.

To assess these three explanations empirically in the context of cloud computing, we conduct a unique census of the six hyperscalers' physical infrastructures situated around the world as of October 2023. We use logistic regression models to examine how international trade flows, security cooperation ties, and interstate conflicts may be able to explain to what extent data centres situated in a given country belong to US versus Chinese providers. Consistent with the economic forces explanation, we find that countries that import more from the US/China also host more cloud infrastructure belonging to US/Chinese providers. But we also find robust evidence that cloud infrastructure is associated with security politics: Countries are much less likely to host US or Chinese providers' cloud infrastructure if they have a history of interstate conflict with that superpower. This association goes beyond the usual dampening effect that conflict has on trade. We interpret the findings as being more consistent with the idea that network hub attachment is shaped by proactive strategic choices made by third-country governments, and less consistent with the idea that hub attachment is driven top down by the great powers in an expansive quest for empire. We combine these interpretations with other recent scholarship to propose a model of bipolar network hub attachment, and discuss its implications.

As societies and economies become increasingly dependent on transnational digital infrastructures and networks, we argue that understanding how the political topology of such networks is shaped is a critical task for IPE. The weaponised interdependence framework provided a compelling explanation for how the US came to occupy a central position in global networks and how it has been able to leverage this position for global influence. But we demonstrate that its economic determinism is no longer sufficient to explain network topology in a bipolar world. We contribute a theoretically and empirically grounded model that extends the framework in a way that addresses this and certain other overlooked factors, while retaining much of the parsimoniousness that made the original framework successful (Gjesvik, 2023).

Background

Originally introduced by Farrell and Newman (2016, 2019a) as part of the new interdependence approach, weaponised interdependence seeks to explain under what conditions networks of economic interdependence result in some states gaining influence over other states—that is, how 'network topography generates enduring power imbalances among states' (2019a, p. 45). The framework borrows concepts from network science, while the empirical subject matter that it deals with is often transnational infrastructures. The key argument is that economic forces tend to produce centralised network structures in which certain territories become hubs that link other territories. States on whose territories the hubs reside—which we call 'hub states'—may be able to 'weaponise' the hubs for espionage and embargoes against other states. Farrell and Newman gave examples such as the US National Security Agency using fiberoptic cable landing points to spy on digital

communications (2016) and the Trump administration using interbank payment messaging network SWIFT to unilaterally reintroduce a global financial blockade on Iran (2019a).

Gjesvik (2023) used the case of transatlantic undersea cable networks to highlight that there were two distinct 'modes of centralization': Geographic and ownership-based. During the first fiberoptic undersea cable construction boom, cables were built by consortia of national telecommunications companies. Their ownership was relatively diversified, but in terms of physical geography, they almost all converged on a small number of landing points in the US and United Kingdom (UK). These specific locations—including Miami, US, and Porthcurno, UK—became physical hubs or 'chokepoints' in global data networks. US and UK governments were able weaponise the hubs by virtue of having territorial jurisdiction over them.

However, since 2010, a different type of network structure has started to emerge. New cables are increasingly built not by large consortia of national telecom firms, but by individual hyperscalers with very deep pockets. The physical footprint of the network is diversifying and becoming less geographically concentrated on the international level, as new cables weave together hyperscalers' data centres situated in different places around the world. At the same time, cable ownership is highly concentrated. In this situation, the most important 'network hubs' in the sense of weaponised interdependence theory are no longer physical locations, but the hyperscale firms who own and operate the infrastructure. Hub states are the hyperscalers' home states, and their legal capacity to weaponise the hubs is based on legislation that requires their firms to comply with extraterritorial data warrants and other requests (Gjesvik, 2023).

Whether a network is centralised in terms of geography or ownership, a key question is how its topology emerges. According to Farrell and Newman's original account, geographic centralisation and ownership concentration of digital and financial networks were mostly the product of blind economic forces (2019a; 2023). Private centralised institutions arose out of decentralised networks as an efficient market solution to information asymmetries and transaction costs (Farrell & Newman, 2019a; Lehdonvirta, 2022). Positive network effects (Katz & Shapiro, 1994), preferential attachment (Barabási & Albert, 1999), and learning-by-doing (Gulati, 1999) ensured that networks coalesced around a small number of large hubs. That these hubs predominantly emerged in the US and Western Europe was seen to be more a result of accident than design, resulting from these regions' first-mover advantages in new technology industries, rather than any conscious political project to obtain commanding positions in contemporary network topologies (Farrell & Newman, 2019a, 2023).

However, once security agencies and policy makers realised that network hubs could be weaponised, the topology of the networks turned into a political matter (Farrell & Newman, 2016, 2023). US policy makers began to consciously promote and defend the dominant position of American hubs. Other governments began to discuss, explore, and in some cases support the development of alternative hubs. European policy makers discussed whether the EU should develop its own international payment channels that would be less vulnerable to US pressure (Farrell & Newman, 2019a; 2019b). The EU also promulgated regulations that sought to attenuate US tech companies' power by promoting interoperability and competition. Russian authorities began to work towards creating a domestic 'sovereign Internet'

that would not depend on US-based root infrastructures, though after a decade of work, the goal still appears to elude them (Soldatov & Borogan, 2022).

The most successful challengers to US network hubs emerged from China. China's Cross-Border Interbank Payment System (CIPS) has made little progress towards challenging SWIFT in global payments. But Chinese tech companies have emerged as serious competitors to US and European firms in global markets. Huawei's 5 G network infrastructures challenge Europe's Ericsson and Nokia. TikTok challenges the dominance of Meta's social media platforms in many countries. E-commerce firms Aliexpress and Temu challenge Amazon Marketplace as the largest hub connecting consumers and e-commerce vendors. Much of this global expansion has been supported by the Chinese government through initiatives such as the Belt and Road (BRI) and the Digital Silk Road (DSR) (Bradford, 2023; Erie & Streinz, 2021). The global expansion of China's digital hubs has taken place at the same time as Chinese firms have constructed and purchased conventional infrastructure hubs, such as ports and airports, around the world. Chinese-led networks have also provided a crucial outlet to war-waging Russia, helping to explain the relatively modest effects of Western sanctions (Rodrigues Vieira, 2023).

For weaponised interdependence theory, the question of how network topologies are shaped is therefore no longer simply a matter of explaining why networks centralise, but *whose* hubs they centralise around. In a network with competing hubs associated with rivaling governments, why does a third country become more attached to one side rather than the other? The proponents of the framework predicted the rise of alternative hubs from the start, but their theorising treated weaponisable networks largely as 'passive sites that hegemonic powers can use and misuse' rather than as 'sites of agentic politics of their own' (de Goede & Westermeier, 2022, p. 4).

A growing number of studies address the question of hub attachment with qualitative evidence and case studies of particular technology companies' international expansion efforts, their home governments' efforts to support such expansion, and other governments' policy responses. Such studies do not necessarily use the language of networks and hubs or engage with the interdependence framework, but rather are found across literatures on international relations, political science, geography, law, sociology, and media studies. In the sections below we bring together a number of these diverse studies to sketch three stylised answers to this question, that is, hypothetical explanations that could explain hub attachment in a bipolar weaponisable network. We also consider how they could be indirectly observed *via* their associations with directly observable aspects of the bilateral relationships between the hub states and third countries, namely trade and security relationships.

Network hub attachment as a product of economic forces

Since the liberalisation of the global telecommunications market from early 1980s onwards, the baseline assumption has in many ways been that the global diffusion of different technologies and providers is a competitive, market-driven process (Cowhey, 1990; Meltzer, 2015). According to this view, the global adoption of US technology companies' products and infrastructure hubs reflects their innovativeness and early-mover advantages. If competition in digital markets has somewhat diminished over time and markets become captured by US hyperscalers, this

reflects the natural dynamics of network competition and scale economies, rather than any US government efforts to foreclose competition by political means (Katz & Shapiro, 1994). The efficient scale of such business is thought to be very large—certainly transnational, perhaps global—implying that concentration is inevitable (Herr, 2020). EU efforts to intervene in the cloud market with competition-enhancing regulation are seen by some authors as protectionism that threatens the valuable scale economies enabled by an open transatlantic market (Herr, 2020). The Chinese government likewise engages in protectionism, but Chinese technology hubs' ability to compete with US hubs also reflects the country's massive domestic market size, which allows its technology companies to achieve sufficient scale in their home market to be globally competitive (Plantin & De Seta, 2019).

As for why a particular third country is more attached to US or Chinese hubs, this is primarily seen as a matter of supply and demand. As publicly listed for-profit companies, the major cloud providers expand their infrastructures in response to growth and profit opportunities. When cloud infrastructures are extended physically closer to customers, these customers enjoy improved service quality, in the form of higher availability and lower latency (Stocker et al., 2021). But cloud infrastructure is expensive to build and operate, so investments are only commercially justifiable if demand for new or improved services in the third country is sufficiently high. Amazon said that it opened its first European data centres because 'developers in Europe… wanted the same high-quality, low-cost service, but with lower latency and local data storage' (Amazon, 2007). Demand for expansion into a third country can also come from other firms in the provider's home country that export to the third country. Alibaba Cloud is used as 'basic infrastructure' by other Chinese firms for their ventures abroad; in 2017, it was used by more than 100 Chinese software companies that engaged in exports (Shen & He, 2022).

Besides sufficient demand, the business case for cloud expansion also depends on costs, so cloud providers are incentivised to invest into third countries that present lower non-tariff barriers and other trade frictions with their home country. In other words, according to this economic forces hypothesis of network hub attachment, cloud infrastructure providers' international expansion is shaped essentially by the same factors that shape all international trade and investment, from physical distance and cultural affinities to trade agreements (Keshk et al., 2004; Meltzer, 2015). Whether the balance of data centre investment in a third country is more US or Chinese heavy should therefore correlate with trade volumes between the countries. In particular, it should correlate with imports from the hub states to the third countries, since imports are reflective of both market demand and bilateral trade openness.

Network hub attachment as an outcome of great power rivalry

Viewing the expansion of digital infrastructures as a purely apolitical market-driven process is obviously somewhat naive, however. The liberalisation of the global telecommunications market itself was arguably a 'regime change' driven by the US and her allies in accordance with their national interests (Cowhey, 1990). The original multilateral telecommunications governance institutions that managed interactions between countries' distinct, sovereign telecommunications markets gave way to a more internationalised governance approach featuring global standard setting,

interoperability, and multistakeholderism, in which large US technology companies were able to wield significant global influence (Radu, 2019; Raymond & DeNardis, 2015). The old regime was arguably economically inefficient, but it was predicated on protecting national telecommunications monopolies in each country and upholding the principle 'that it was unacceptable for national security to rely on other countries for network equipment' (Cowhey, 1990, p. 179). Regardless of what economic benefits the new regime had, it paved the way for the global expansion of US technology companies, and the internationalisation of US state power *via* a growing 'underground empire' of global infrastructures whose hubs fell under US jurisdiction (Farrell & Newman, 2023). History echoed, as new fiberoptic Internet cables often followed the routes of old telegraph cables originally laid to serve the needs of the British and American empires (de Goede, 2021).

From 2000s onwards, the Chinese government has attempted to follow the US example and establish a 'geo-economic space' for its own technology companies (Cartwright, 2020; Munn, 2023). It has encouraged its private sector in general and technology companies in particular to 'go out' and expand globally, with the explicit aim of expanding Chinese state influence abroad (Keane & Yu, 2019). China's Digital Silk Road initiative uses both economic and political incentives to 'push' Chinese digital infrastructures, including cloud data centres, to third countries (Bradford, 2023; Erie & Streinz, 2021). These incentives have included things such as cheap export credit to the companies and political favours to third-country governments. As a result, Chinese cloud providers, such as Alibaba Cloud, have begun to challenge the dominance of US hubs especially in Southeast Asia (Naughton, 2020; Shen & He, 2022). Chinese technology companies have thus arguably become part of another 'digital empire in the making' (Keane & Yu, 2019).

An ostensible objective of such 'digital imperialism' (Kwet, 2019) is to gain influence over other countries by having the option of weaponising hubs that other countries have come to rely on, whether through espionage or by withholding access. Withholding access to global networks can be considered a digital-era equivalent of a blockade, which originated as a coercive wartime tool (Mulder, 2022). For instance, as Chinese navy and coast guard vessels clashed with Filipino ships over disputed maritime territories, the Chinese government 'pushed' digital infrastructures into the country, sponsoring the construction of an Alibaba Cloud data center in Manila (Hussain et al., 2024). If cheap, low-latency cloud services offered through this hub entice businesses to migrate their data and workloads, the Chinese government gains additional leverage. According to this view, network hub attachment should thus be correlated to some extent with militarised conflict, as expansionary powers use all means at their disposal—from military to techno-economic—to expand their influence over third countries.

Following this logic, rivaling great powers should use their influence over third countries to turn those countries away from their rival's hubs. The US government persuaded many of its allies to exclude Huawei hardware from future 5G mobile network investments, even when such bans risked running against World Trade Organisation (WTO) trade rules and other international norms (Hoffmann et al., 2021). In 2020, the US State Department also announced a 'Clean Network' initiative, which included a 'Clean Cloud' component that labeled Alibaba's and Tencent's cloud services as unsafe (Cartwright, 2020; Shen & He, 2022). The Trump administration claimed to have signed up more than thirty countries and territories to

the initiative. The Biden administration continued similar policies. In 2021, following US government pressure, video platform TikTok annnounced that it was switching from Alibaba Cloud to Amazon's AWS for its business outside China (Shen & He, 2022). According to this view, a third country's network hub attachment should thus also be correlated with any membership it has in either great power's security blocs.

In some countries' cases, these two proposed statistical correlates of hub attachment—conflict and bloc membership—point in opposing directions. For instance, Philippines faces military pressure from China, but is also a US Major Non-Nato Ally, implying that both powers would be trying to promote their own hubs in the country and/or containing their rival's.

Network hub attachment as a result of third-country strategic choices

The great power rivalry explanation sketched above misses the fact that third-country governments would be unlikely to remain passive in the face of expanding 'digital empires'. The acceleration of global connectivity in a context of heightening geopolitical tensions has led many governments to be increasingly careful about foreign investment in their infrastructures. The huge scale and reach of infrastructures like cloud computing mean that there is a greater public interest in actively managing the associated security risks than there has been with most other technologies supplied by foreign firms (Herr, 2020). The stakes are further heightened by path dependencies associated with infrastructural technologies: Adopting US or Chinese infrastructures now will favour more technology adoption from the same source in the future (Hoffmann et al., 2021). As a result, many governments are deploying 'a mix of innovative as well as time-tested interventions in the economy directed at safeguarding their 'strategic assets', 'critical infrastructures' or 'emerging technologies' from control or influence by foreign state and/or market forces' (Choer Moraes & Wigell, 2022, p. 30). Data centres in particular are increasingly framed as critical infrastructure in need of safeguarding (Eling et al., 2023). From this point of view, third-country governments can thus be seen not as passive victims, but as actors with agency and strategic choices available to them in how they engage with network topologies vulnerable to weaponisation (Narlikar, 2021).

According to this third-country-centric view, the governments of third countries can adopt a variety of stances and approaches to manage their country's attachment to different network hubs (Walter, 2021). In Europe, government responses have included attempts at creating local alternatives to avoid the binary choice between US and Chinese hubs (Germann, 2023; Lambach & Oppermann, 2023; Lavery, 2024). For instance, France launched its first 'sovereign cloud' project already in 2009. However, it never gained traction and was shut down as a failure in 2020. A key problem seems to be that national cloud initiatives lack the scale necessary to compete with multinational hyperscale cloud providers in operational efficiency, energy efficiency, cybersecurity, and research and development spending (Bremmer, 2021; Srnicek, 2022). Newer attempts such as Gaia-X involve collaboration between multiple European countries, but common efforts tend to be hampered by EU member states' varied economic and security interests (Poutala et al., 2022), and at least for the time being European countries remain highly dependent on foreign digital infrastructures (Mayer & Lu, 2023).

Even if Europe's 'digital sovereignty' remains elusive (Mayer & Lu, 2023), governments nevertheless have tools to influence on whose infrastructures their societies rely. Imposing parameters on public sector technology use is commonplace and comparatively simple. German, Australian, and Taiwanese government agencies banned staff from connecting to Zoom when its global infrastructure was found to route some data through servers in mainland China (Chen, 2022). Russia's 2022 attack prompted the Ukrainian government to move all its critical government registries and services to US cloud platforms (Moss, 2022). UK, German, and French governments have created cloud certification schemes that in practice restrict certain cloud providers' ability to provide services to certain types of public sector organisations and uses (Herr, 2020). It is less straightforward for governments in liberal democracies to influence private sector organisations' network hub choices. However, many democracies are implementing reforms that enhance their ability to intervene in foreign investment on national security grounds. For example, Australia amended legislation in 2020 to give the government greater power to review and, in extreme cases, deny significant private foreign investment into infrastructures deemed as critical. Governments also positively shape incoming investment by for instance offering subsidies and incentives to data centre builders (Mayer, 2023).

To whose network hubs do third-country governments seek to attach their countries with these policy tools? According to Hoffman and colleagues (2021), many countries are facing 'competing strategic choices… as they struggle with the wider implications of buying and using technologies that may be at odds with their traditional security and intelligence interests and partnerships' (p. 242). Many European governments strongly resent US governments' weaponisation of network hubs for surveillance and espionage against their citizens and leaders (Farrell & Newman, 2016). Local citizens have in some cases mobilised against large US data centres in part due to their associations with surveillance (Hogan, 2015; Rone, 2024). But when faced with a choice between US and Chinese hubs, Europeans have still largely preferred to depend on the US (Dover, 2014). For instance, most European organisations outsource their email services to Microsoft or Google, and almost none to China-based Tencent (Liu et al., 2021). In general, technological dependence on the US over China has been preferred in countries whose values and global security interests are more aligned with the former (Dover, 2014). For US treaty allies, attachment to US hubs may be thought of a safer bet also because the security relationship is in principle moderated by treaty and the US government shares some of the intelligence. In the UK, even national security services have reportedly chosen to store classified materials on AWS (Warrell & Fildes, 2021), and Australia recently appears to be doing the same (Australian Government, 2024).

For third-country governments in the Global South, such as Brazil, India, and Indonesia, the factors that influence the decision may be somewhat different. Infrastructures such as 5G and cloud computing are seen as critical to national development (Gonzalo et al., 2023). Vendor choices are influenced by economic considerations, and Chinese infrastructures tend to be more affordable (Hussain et al., 2024; Rabe & Kostka, 2023). National security considerations also matter, but the US is not always the preferred security partner. US cloud providers and cloud-related legislation have not always been sensitive to the needs of Global South countries even on basic issues such as law enforcement access to digital evidence (Abraha, 2021). Some Global South governments are moreover attracted to the Chinese model of

digital development that promises to leave the state firmly in control of national cyberspace, and therefore steer their country toward Chinese-made infrastructures (Erie & Streinz, 2021). That said, several countries in East and Southeast Asia have contentious security relationships with China, including ongoing territorial disputes, which could make their governments wary of Chinese network hubs from a national security point of view. Organisations in Southeast Asia as well as in South America still outsource their email services largely to US Microsoft and Google rather than to, for instance, Chinese Tencent (Liu et al., 2021).

According to this explanation, network hub attachment is thus a strategic national and economic security choice for third-country governments. The governments possess levers to influence inbound infrastructure investment, including import restrictions, incentives, regulation, and public procurement. As a result of such interventions, a country's network hub attachment should be positively correlated with its security cooperation ties but negatively correlated with its interstate conflicts with the hub states.

Summary: three hypothetical explanations for network hub attachment, observable indirectly via trade and security variables

To summarise, it is possible to synthesise three hypothetical explanations from the previous literature to the question of why a given country is more attached to one power's hubs than the other's: According to the great power rivalry explanation, hub attachment is shaped by would-be empires' attempts at extending their infrastructures into third countries and containing each others' expansion. According to the third-country choice explanation, network hub attachment is shaped by third-country governments making strategic choices over which hubs to favour in accordance with their own security interests. Both of these views suggest that a third country's network hub attachment should be correlated positively with its security cooperation ties with the two great powers. But the two views differ with regards to how network hub attachment should be associated with interstate conflict. The great power rivalry explanation allows for conflict to be positively associated with hub attachment, as would-be empires may complement military coercion with network expansion as a means to influence third countries. The third-country strategic choice view implies that conflict should be negatively associated with nework hub attachment, as governments steer away from hubs governed by hostile powers.

In the great power rivalry explanation the agency to shape network topology thus lies primarily with the hub states, whereas in the third-country strategic choice explanation the agency lies with third-country governments. But both are essentially realist explanations of hub attachment, since the underlying idea in both is that hub attachment is driven by state actors who are attempting to maximise their own security and power. Such realist explanations can be contrasted with a more liberal explanation, which we termed the economic forces explanation. According to this explanation, a third country's network hub attachment is mainly shaped by the commercial interests of the large multinational technology companies, or hyperscalers, who build and operate the cloud infrastructures. According to this explanation, hub attachment should be correlated with international trade and especially the balance of a third country's imports from the US versus China. The three explanations thus differ especially with regards to where agency to shape network topologies lies: With great powers, third countries, or technology firms.

In the following section we describe an empirical study to assess these explanations in the context of the world's hyperscale cloud computing infrastructure.

Data and methods

Our methodological approach is based on modeling a third country's attachment to US and Chinese cloud computing infrastructure hubs as a function of its trade and security relationships with these two powers. The ideal methodology would incorporate time as a dimension of analysis, examining how hub attachments evolve and interact with changes in trade and security ties. However, as the first quantitative study on the topic, we use original snapshot data on global cloud infrastructure that lacks such a temporal dimension. Our approach is thus cross-sectional in nature and can be thought of as a first attempt to discover whether associations are detectable even without resorting to more complex models and data.

The variables used in our analysis are summarised in Table 1 and detailed in the following subsections. For trade and security variables we draw on commonly used databases. Trade and security relationships are known to be mutually correlated, in such a way that trade tends to 'follow the flag' over time (Keshk et al., 2004). By including both as explanatory variables, we essentially ask what additional effects security relationships have on cloud infrastructure investment on top of the effects that security usually has on international trade.

Statistical power limits our ability to add further control variables, but insofar as network hub attachment is thought to be shaped by the same factors that shape international trade in general (e.g. distance, language, trade agreements), the effects of these factors are already incorporated in our trade variables. Other controls such as market size, climate, and energy availability would be necessary for modeling whether a country has cloud computing infrastructure on its soil in the first place, but our design instead takes the presence of infrastructure as a given and asks what explains *whose* infrastructure it is.

Trade variables

Our theoretical propositions on trade are concerned with the relative strength of the trade ties that each third country has with each of the two hub states. To this end, we use relative rather than absolute measures, defining a country's import variable *impo* as the log ratio of its imports from the US versus its imports from

Table 1. Variables and descriptive statistics.

	N	Mean	SD	Min	Max
Dependent variable					
Number of US AZs	37	5.92	4.77	0	17
Number of Chinese AZs	37	2.62	2.80	0	11
Hub attachment *p*	37	0.64	0.38	0	1
Independent variables					
Relative imports *impo*	37	−0.28	0.93	−2.20	2.12
Relative exports *expo*	37	−0.12	1.16	−2.18	3.25
Cooperation *coop*	37	0.57	0.60	−1	1
Conflict *conf*	37	−0.08	0.49	−1	1

Notes: unstandardised; level: third country.

China. A positive value indicates that the country is importing more from the US than from China, while a negative value indicates more imports from China. Similarly, we define a country's export variable *expo* as the log ratio of its exports to the US versus its exports to China. The advantage of these combined measures is that they reduce model degrees of freedom, but a shortcoming is that they are unreliable for countries that trade little with either hub state, which could lead us to underestimate trade effects.

As a data source, we used the International Monetary Fund (IMF) Direction of Trade Statistics database (July 28, 2023 update; see International Monetary Fund, 2023), which is commonly used in studies of interstate relations and trade (Keshk et al., 2004). Exports are measured using Free On Board (FOB) partner export data and imports using Cost, Insurance, and Wreight (CIF) partner import data. The unstandardised means of our export and especially import variables are negative, indicating that the countries in our data set on average have stronger trade links with China than with the US (Table 1).

Security variables

We measure the security relationship between each third country and great power on two dimensions: Cooperation and conflict. We coded a country as cooperating with the US if it is a member of NATO or designated by the US government as a Major Non-NATO Ally. We coded a country as cooperating with China if it is a member or an observer in the Shanghai Cooperation Organization (SCO). We also coded Hong Kong as 'cooperating' with China. As an alternative operationalisation we considered coding countries that participate in China's BRI, but as of December 2023 they number as many as 150. Moreover, 90% of the SCO countries are also in BRI, so we considered it a stronger indicator of cooperation with China.

As an alternative operationalisation, we also counted the number of ties between each third-country–great power dyad in the Alliance Treaty Obligations and Provisions (ATOP) database 5.1, which covers alliances through December 2018 (Leeds et al., 2002). The resulting measure was similar but not entirely satisfactory from a face validity perspective; for example, Hong Kong as a non-state entity was not included, Israel was not aligned with the US as of 2018, new NATO member Finland was missing, and China's only cooperation was with North Korea. In the analyses we thus use the codings based NATO and SCO memberships. We do not claim them to be a definitive measure of international security cooperation, but for the purposes of this study they are unambiguous, up to date, and based on well-defined legal instruments.

The resulting groups are mutually exclusive, so we combined them into a single continuous variable labelled *coop*, defined as 1 = cooperating with the US; −1 = cooperating with China; 0 = neither. This reduction in degrees of freedom is helpful given the inherently small N of a cross-sectional country study, and theoretically justifiable insofar as our propositions juxtapose US and China as opposing poles. The unstandardised mean of this variable is positive (see Table 1), indicating that more countries in our data set cooperate with the US than with China.

To measure conflict, we used the Militarized Interstate Disputes database 5.0 (MID5), which covers disputes through December 2014 (Maoz et al., 2019). We coded a country as having a conflict with the US/China if it appeared on a different side in any dispute in the database since 1990. Varying this cutoff year a decade

in either direction did not materially change the results. The resulting groups are mutually exclusive, so we combined them into a single continuous variable *conf*: 1 = conflict with the US, −1 = conflict with China; 0 = neither. The unstandardised mean of this variable is slightly negative (Table 1), indicating that slightly more countries in our data set have had conflict with China than with the US.

Network hub attachment variables

We operationalise a country's network hub attachment as the Availability Zones (AZ) that different hyperscale cloud providers have located in that country. An AZ corresponds roughly to 1–3 large, interconnected data centres along with their power, cooling, and networking equipment. Global hyperscale cloud platforms also include a variety of smaller facilities, such as different kinds of edge computing facilities, but we focus on AZs because they carry out the majority of all data storage and processing and provide a rough level of comparability across different providers. Using public sources such as cloud providers' websites and customer user interfaces, we conducted a 'census' of all the AZs belonging to the top three US and Chinese providers globally as of October 2023. These providers were AWS, Microsoft Azure, Google Cloud, Alibaba Cloud, Huawei, and Tencent. Although we did not include smaller providers in the data set, these six leading providers controlled the vast majority of the public cloud market globally as well as in each individual country market, so the data arguably captures the main contours of the phenomenon.

Our census identified a total of 526 AZs globally. We identified the physical location of each AZ as follows: The cloud providers group their AZs into 'cloud regions' or clusters of infrastructure situated in a given area, and name the regions after nearby cities, such as 'Warsaw' or 'Doha'. We recorded these names as part of collecting the census and used the World Cities Database (World Cities Database, 2024) to map the names to physical locations. The approximate locations are depicted in Figure 1. We found that 73 AZs were located in the US, 137 AZs in mainland China, and 316 AZs in 37 third countries. Hong Kong is included in our

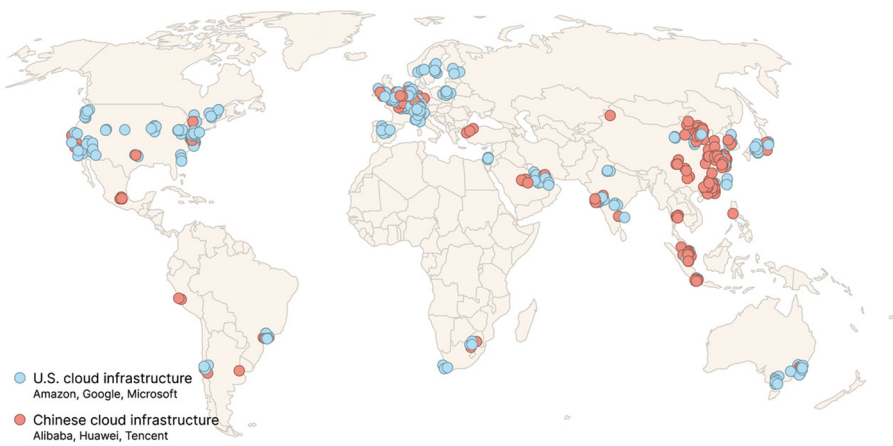

Figure 1. US (blue) and Chinese (red) cloud availability zones.

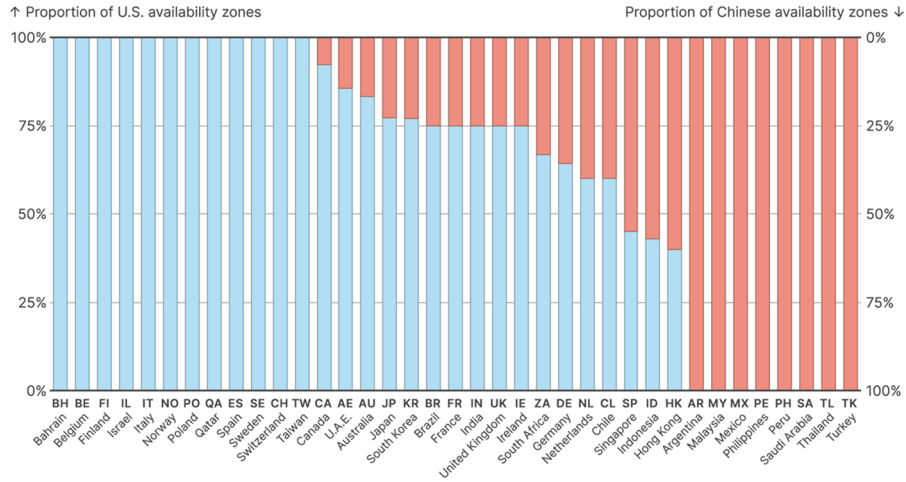

Figure 2. Proportions of US (blue) and Chinese (red) availability zones by country.

list of third countries/regions because it is measured as a distinct entity in international trade data as well as in cloud providers' region data.

Of the 316 AZs located in third countries, 219 belonged to US cloud providers and 97 to Chinese cloud providers. We measure third country *j*'s hub attachment as the proportion p_j of US AZs located in it, depicted in Figure 2. The proportion of Chinese AZs is the inverse, 1-p_j. The mean hub attachment is 0.64, indicating that the average third country has somewhat more US than Chinese cloud computing infrastructure (Table 1).

Statistical model

To assess whether and how our independent variables are associated with hub attachment, we estimate binomial logistic regression models of the following specification:

$$\ln\left(\frac{p_j}{1-p_j}\right) = \beta_0 + \beta_1 impo_j + \beta_2 expo_j + \beta_3 coop_j + \beta_4 conf_j + u_j.$$

The left-hand side of the equation is the log-odds of country *j*'s network hub attachment p_j. The higher the odds, the more American the country's cloud infrastructure is; the lower the odds, the more Chinese it is. The right-hand side of the equation comprises the fixed intercept term β_0, a country-specific random intercept term u_j, and the four country-level independent variables together with their coefficients, whose estimates we are interested in.

The left-hand side can also be written as:

$$\ln\left(\frac{Pr\left(az_{ij} = U.S.\right)}{Pr\left(az_{ij} = Chinese\right)}\right) = \beta_0 + \beta_1 impo_j + \beta_2 expo_j + \beta_3 coop_j + \beta_4 conf_j + u_j,$$

that is, the log-odds of availability zone i in country j belonging to a US provider instead of a Chinese provider. This is in effect a multi-level model in which the unit of analysis is an individual AZ, but all the independent variables are at the country level. Although we do not have any AZ-level independent variables, we prefer this specification because including information on the number of trials per cluster can produce better parameter estimates. Thus, in practice we input the US and Chinese AZ counts to R's *glmer* package as a two-dimensional response variable (instead of combining them into p) to estimate the models.

We estimate and compare multiple versions of the specification: A null model with the intercept only, fixed effects models that add the independent variables, and finally the full mixed effects model that also adds the country-specific random intercept. Our data set is somewhat small for the mixed effects model (37 clusters with 8.54 mean trials per cluster) and fails to satisfy the assumption that the random intercepts are normally distributed, but we nevertheless include the model in our findings for completeness and to facilitate model assessment in terms of fit versus complexity.

The shape of the probability distribution as seen in Figure 2 is such that zero/one inflated models could yield better fits than plain logistic regression, but such models would require a larger data set to estimate.

To facilitate coefficient interpretation, all independent variables are standardised (mean = 0, SD = 1) prior to model estimation.

Findings

Which variables can explain the extent to which a country is more attached to US or Chinese cloud computing hubs? Our model estimation results are presented in Table 2. When only trade variables are included as explanatory variables (Model 1), imports are positively associated with hub attachment, while exports have no discernible effect. When only security variables are included (Model 2), cooperation is positively associated with hub attachment, while conflict is negatively associated, but the statistical significance of the latter association is weak. The security model

Table 2. Network hub attachment model coefficients (SE in parenthesis).

	Null model	Model 1	Model 2	Model 3	Model 4
Fixed int.	.81 (.12)***	.88 (.13)***	.86 (.13)***	.86 (.13)***	1.05 (.25)**
Impo		.44 (.15)**		.38 (.16)*	.53 (.40)
Expo		−0.16 (.15)		.15 (.19)	−0.01 (.39)
Coop			.40 (.11)***	.30 (.12)**	.51 (.32)
Conf			−0.26 (.13)*	−0.40 (.14)**	−0.54 (.36)
Rand int.					(1.52)
Trials	316	316	316	316	316
Clusters	37	37	37	37	37
Df	36	34	34	32	31
Resid. dev.	134.37	124.71	117.85	110.08	25.35
AIC	182.82	177.16	170.3	166.53	149.00
Nagelk. R^2	.00	.23	.36	.49	.70

***$p<.001$.
**$p<.01$.
*$p<.05$.

is able to explain a greater share of the variation in the response variable than the trade model, as measured by Nagelkerke's pseudo-R^2.

When both trade and security variables are modeled together (Model 3), the directions of the effects remain the same, but conflict becomes more statistically significant while cooperation and imports become less so. This combined model is able to explain a much larger share of variation in hub attachment than either the trade or security model could individually. It also performs better in terms of the Aikake information criterion (AIC), which is used to assess model fit versus complexity. This indicates that security variables have an association with cloud network hub attachment above and beyond the effects that security relationships have on trade in general.

If the country-specific random intercept term is added to the model (Model 4), the share of variance explained increases further and AIC performance likewise improves. This is because the country-specific intercept captures any idiosyncratic country-specific variation in hub attachment that is not captured by the general trade and security variables. However, the trade and security variables' standard errors increase, and statistical significance falls off in this model, reflecting the limited statistical power of the design. The directions of the fixed effects remain the same and the effect sizes remain similar, suggesting that trade and security factors provide a reasonable and parsimonious explanation for the phenomenon at hand even without attempting to model country-specific idiosyncrasies. Given also the fact that Model 4's assumptions are not met, our preferred model for interpreting the results is thus Model 3.

The effect sizes in Model 3 are of a practically significant magnitude. As a country's balance of imports shifts towards the US by one standard deviation, the odds of a given cloud availability zone in that country belonging to a US provider increase by a factor of $\exp(.38) \approx 1.46$. A one standard deviation shift in cooperation is associated with the odds increasing by a factor of $\exp(.30) \approx 1.35$. A corresponding shift in conflict decreases the odds by a factor of $\exp(-0.40) \approx .67$.

Discussion and conclusions

Today's Internet is not the rhizomatic, decentralised network of self-organising servers that it was once thought to be (Starosielski, 2015). It has a hierarchical topology in which hyperscale cloud computing infrastructures function as central hubs that store data, process workloads, and serve content to users. States with jurisdiction over the firms that own the infrastructures may be able to 'weaponise' them for espionage and blockades. What explains the extent to which third countries attach to one state's hubs rather than another's? A basic conclusion that can be drawn from our study is that the economic determinism that characterised the unipolar, US-centric weaponised interdependence framework is insufficient to explain network topology in a bipolar world. In a network where Chinese technology firms challenge US hubs' dominance, not only trade but also security variables explain a significant part of the topology. In the following discussion, we interpret these statistical associations against the three hypothetical explanations we synthesised from qualitative literature, according to which third countries' hub attachment is shaped by (1) economic forces; (2) great-power rivalry;

or (3) third-country strategic choice. We then propose a model of bipolar network topology that combines all three explanations and discuss its implications and limitations.

We found that third countries' cloud hub attachment is systematically associated with trade ties, and specifically with imports: Countries that import more from China than from the US tend to attach to Chinese cloud hubs, and vice versa. For example, Malaysia and Thailand import far more from China, and their hyperscale cloud infrastructures are all from Chinese providers. Formally neutral country Switzerland imports more from the US and its cloud infrastructure is fully American (smaller countries are somewhat overrepresented in these illustrative examples because they have fewer data centres and thus tend towards extremes on the attachment variable, but our statistical model accounts for this bias). This finding is consistent with the economic forces explanation of network hub attachment, in which attachment is a competitive, market-driven process: Providers expand their infrastructures to third countries in response to demand from those countries and from home-country businesses that are exporting to those countries (Shen & He, 2022).

An alternative interpretation of this association would be that causality flows in the other direction: That cloud infrastructure from a given provider fosters additional (digital) trade with the provider's home country (Meltzer, 2015). However, we found no association between hub attachment and exports from third countries to the hub states. It is possible that common cloud infrastructure for some reason fosters significant amounts of inbound trade but not outbound trade. But it seems more likely that these results reflect cloud providers responding to demand rather than the other way round (e.g. Amazon, 2007). Future research could attempt to identify influence in the other direction by focusing specifically on digital trade and by examining the relationship between hub attachment and trade over time, which we did not attempt.

At the same time, our findings challenge a purely economically deterministic view by showing that a country's cloud hub attachment is also associated with its security relationships. It is well understood that national security and trade are correlated, as government policies and market sentiments favour trade with friendly nations over trade with enemies (Keshk et al., 2004). But we found that the associations between cloud and security persisted even when trade and security variables were modeled together. This indicates that security variables have an additional effect on cloud on top of the general effects that they have on trade. In other words, cloud appears more securitised than trade ties in general.

Specifically, we found evidence that countries that are engaged in security cooperation with one hub state tend to attach to that state's network hubs rather than the other's. For example, Finland, Norway, and Sweden are NATO members and host exclusively US cloud infrastructure. There were no such clear examples for China, however, and since operationalising security cooperation with China is more conceptually challenging, as a robustness check, we also estimated Model 3 with an alternative version of the *coop* variable that included only US cooperation and not Chinese cooperation. The results were materially the same (imports, cooperation, and conflict statistically significant with the same coefficient signs). This suggests that the present results are driven by US cooperation ties, but does not exclude the possibility of Chinese cooperation having the same effect.

In any event, this association between network hub attachment and security cooperation is consistent with the hypothetical great-power rivalry explanation of hub attachment, which entails each great power coaxing and coercing bloc members to reject their rival's hubs in favour of their own. But it is equally consistent with the third-country strategic choice explanation of hub attachment, which entails third-country governments using their policy levers to willingly choose hubs owned by an ally over those of a non-ally.

Helping to distinguish between the two proposed explanations, we found evidence of a negative association between cloud hub attachment and conflict: Countries that have been involved in militarised interstate disputes with the US or China are much less likely to be attached to that hub state's network hubs. This finding is somewhat inconsistent with the notion of network hub attachment as driven by rivaling great powers' efforts to expand their influence over third countries. If the powers have attempted to induce deeper network hub attachment as a complement to military coercion, then those attempts appear to have generally failed, since the statistical association between the two is negative. The finding is instead more consistent with the view of network hub attachment as being driven by third-country strategic choices: Third-country governments are wary of letting their countries become attached to weaponizable network hubs under the control of states with whom they are in conflict, so they use the policy levers available to them to steer towards alternative hubs. For example, Taiwan imports much more from China than from the US, and is not a formal US ally, yet hosts only American cloud infrastructure.

In sum, out of the three hypothetical explanations synthesised from qualitative literature, we conclude that economic forces and third-country strategic choice appear more likely explanations for the observed topology of the world's hyperscale cloud infrastructure than great-power rivalry does.

A model of bipolar network topology formation

Yet how can we make sense of the conclusion that the US and China have not been very forceful in shaping hub attachment, if weaponizable networks are such potent sources of influence as the weaponised interdependence literature suggests (Farrell & Newman, 2023)? To address this puzzle, further theoretical elaboration appears necessary.

One explanation could be that neither the US nor the Chinese hyperscalers that build the infrastructures are simply 'tools in the hands of governments' (Bremmer, 2021, p. 113; Nanni, 2022). Gjesvik (2023) argues that compared to firms in geographically concentrated networks, firms in ownership-concentrated networks have more agency to choose the physical locations of their infrastructures in accordance with their commercial interests, paying less heed to state security interests. Among other reasons, this is because they are not so dependent on any particular physical location and thus cannot as easily be coerced with, for instance, conditional operating licenses. Being pushed into commercially unattractive markets or being confined into blocs runs against these companies' economic interests (Farrell & Newman, 2016; Liu, 2021).

Our findings bear out this argument insofar as they support the idea that hub attachments are shaped by economic forces and not shaped by hub states' efforts

to bring third countries under their hubs' influence, at least as a complement to military coercion. But in contrast to Gjesvik (2023), we find that another category of states does continue to have agency in shaping an ownership-concentrated, geographically dispersed network: Namely, third-country states. We argue that this is because they exercise strong jurisdiction on their own territory and have means to, for instance, block foreign investment when it is not in their interest. It is not economically feasible for states to remain disconnected from global networks entirely, so in the age of unipolar networks this blocking ability was of little use. But in the age of bipolar networks third-country states now have a choice over which hub's 'spokes' to become. As a result, they obtain a degree of agency within the confines of the network's bipolar structure.

Based on the foregoing, we posit the following model of network topology that reconciles the previous literature with the findings from our empirical study: In a bipolar weaponizable network, third-country or 'spoke state' network hub attachment is shaped by

1. economic forces; and
2. in a geographically concentrated network, predominantly by hub states' great-power rivalry; or
3. in an ownership-concentrated network, predominantly by the spoke states' own strategic interests.

This model addresses the need to extend weaponised interdependence theory from unipolar networks to bipolar networks, but it does so without reducing international technology politics to a mere arms race between great powers (Bryson & Malikova, 2021; Qiu et al., 2022; Rodrigues Vieira, 2023). It recognises third countries as actors, a previously under-addressed category in weaponised interdependence scholarship (Narlikar, 2021), but it does not claim that third countries have unfettered agency. It identifies the circumstances under which network hub attachment may be driven by third countries' (spoke states') interests as opposed to great power (hub state) rivarly; that is, when third countries can be network shapers as opposed to merely network takers. The model also retains much of the parsimonious character that arguably made the original framework so effective (Gjesvik, 2023), thus offering weaponised interdependence scholarship a viable baseline for understanding the topology of bipolar networks.

For instance, the model offers a concise explanation for why ownership-concentrated unipolar networks quickly became bipolar, and specifically why Chinese hubs rather than European hubs emerged as challengers to US dominance. In a context where US hyperscalers extracted monopoly rents and US state agencies weaponised their infrastructures, there were predictions that networks would fragment, as countries or regions would choose to disconnect from hubs (Farrell & Newman, 2016; Hill, 2012). But centralised networks proved surprisingly sticky, which according to our explanation is because of economic forces (1), such as scale economies that could be obtained from attaching to global networks *via* hubs. Rather than disconnecting entirely, third countries therefore sought alternative hubs of sufficient scale (Farrell & Newman, 2019). Nascent European hubs were too small to be competitive, whereas China's massive domestic market size made it possible for hyperscalers to emerge in the country (Plantin & De Seta,

2019). As a result, third-country interest in attaching to alternative hubs (3) mainly benefited Chinese hubs, resulting in the bipolar US-China network topology that we observe today.

Limitations and future research

Our empirical study of network hub attachment was conducted in the context of the world's hyperscale cloud computing infrastructure, an ownership-concentrated network. We used previous theoretical literature to posit how the model would differ for geographically concentrated networks. Future research should evaluate this model empirically also in geographically concentrated networks, such as the advanced semiconductor supply chain (Malkin & He, 2024; Miller, 2022; Zhang, 2024). For instance, Beaumier and Cartwright (2023) showed that the semiconductor supply chain was geographically concentrated on multiple levels. The focus of their analysis was on describing the network's structure and understanding its vulnerability to weaponisation. But they also discussed factors that shaped the structure over time, suggesting that the concentrated topography initially resulted from economic forces and was then shaped by US government rivalry with China, while an attempt by Japan to shape the network essentially failed.

A notable feature of our study is that we understood security relationships in rather traditional terms as alliances and kinetic, hard-power conflict. We did not attempt to address the linkages between network topology and broader forms geoeconomic statecraft, which can be seen as substitutes to states' use of hard power today (Mulder, 2022; Roberts et al., 2019). The advantage of this approach is that traditional security categories like NATO membership and militarised interstate conflict are conceptually, and in terms of operationalisation, less ambiguous than the tools of contemporary geoeconomic statecraft, so the findings provide a clearer baseline understanding of the relationship between network topology and state interests/agency.

However, the significant disadvantage of this approach is that any possible linkages between network topology and broader geoeconomics are obscured. In practice, the effects that we attributed to economic forces are likely to also comprise some effects of geoeconomic tools, such as preferential trade agreements, which in some cases may have been designed by hub states with the specific intent of promoting third countries' attachment to their network hubs, besides boosting trade in general. For instance, in 2021, the Biden administration announced plans for an Indo-Pacific Economic Framework, which among other things aimed to promote digital trade rules modeled on US rather than Chinese or European standards (Natalegawa & Poling, 2022). To obtain an increasingly refined understanding of how bipolar network topologies are shaped, future research should thus consider how to reasonably model the relationship between network topology and broader geoeconomics.

Our study also comes with many empirical limitations. Although US and Chinese hyperscale cloud providers dominate the public cloud market, and public cloud use has grown rapidly, it is by no means the case that all data and workloads have moved into public cloud; many governments and enterprises are also holding on to smaller data centres and on-premises solutions, sometimes specifically for the

purpose of avoiding dependence on foreign firms and/or states (Choer Moraes & Wigell, 2022). Measuring and conceptualising the geography and topology of such smaller-scale computation presents a challenge for future research.

Our snapshot data obscures any potential changes that may have taken place in associations between the variables over time. For instance, it is plausible that great-power rivalry as a driving mechanism of hub attachment could have become more prominent over the past few years. Time series data with a modeling approach such as punctuated equilibrium could potentially capture such effects. That being said, cloud infrastructures as large, transnational infrastructures are slow-moving capital investments, with the consequence that any notable changes in the overall picture would likely take several years to unfold. Thus, we do not think that our results are very sensitive to the particular year in which the snapshot was taken. Nevertheless, adding time as a dimension of analysis, which was not possible with our current data set, would allow this question to be interrogated. Even if year-to-year changes are small, it might be possible to identify over cloud's 20-year history a few distinct 'eras' of cloud geopolitics. Given that our approach demonstrated utility, future studies should invest into developing larger data sets suited to analysing evolving political topologies of digital networks over time and in greater granularity.

Acknowledgements

Anu Bradford, Robert Trager, Dariusz Wójcik, Fabian Stephany, Johannes Gölz, Jack Qiu, Ralph Schroeder, and participants of the Oxford-Aalto Digital Economic Security seminar and the TUM Campus Heilbronn Global Technology Forum 2023 provided useful feedback on earlier versions of this study. The authors also gratefully acknowledge the feedback from three anonymous peer reviewers.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

This study was supported by a grant from the Dieter Schwarz Stiftung.

Notes on contributors

Vili Lehdonvirta is Professor of Economic Sociology at the Oxford Internet Institute, University of Oxford, and Professor of Technology Policy at Aalto University, Finland, where he leads the Digital Economic Security Lab DIESL. He is the recipient of three European Research Council grants, most recently on 'Geopolitics of Cloud Computing'. His books *Cloud Empires* and *Virtual Economies* are published by MIT Press.

Boxi Wú is a doctoral researcher at the Oxford Internet Institute, University of Oxford, and member of the Digital Economic Security Lab DIESL. Their research focuses on the political and environmental impacts of AI infrastructure and has been published in *Big Data & Society*, *Philosophy & Technology*, *ACM Fairness, Accountability & Transparency* and *AAAI/ACM AI, Ethics & Society*.

Zoe Jay Hawkins is Co-Founder & Deputy Executive Director of the Tech Policy Design Institute (TPDi), an independent non-partisan think tank dedicated to technology policy based in Australia. As a Research Associate at the University of Oxford, Zoe collaborates with Professor Vili Lehdonvirta and Boxi Wu to research the political geography of AI and digital infrastructure, including for the Digital Economic Security Lab DIESL and OECD.

References

Abraha, H. H. (2019). How compatible is the US 'CLOUD Act' with cloud computing? A brief analysis. *International Data Privacy Law*, *9*(3), 207–215. https://doi.org/10.1093/idpl/ipz009

Abraha, H. H. (2021). Law enforcement access to electronic evidence across borders: Mapping policy approaches and emerging reform initiatives. *International Journal of Law and Information Technology*, *29*(2), 118–153. https://doi.org/10.1093/ijlit/eaab001

Amazon. (2007, November 6). *Amazon Web Services offers European storage for Amazon S3*. Amazon Press Centre. https://press.aboutamazon.com/2007/11/amazon-web-services-offers-european-storage-for-amazon-s3

Australian Government. (2024, July 4). *Australian Government partners with Amazon Web Services to bolster national defence and security*. Australian Government Defence Media releases. https://www.minister.defence.gov.au/media-releases/2024-07-04/australian-government-partners-amazon-web-services-bolster-national-defence-and-security

Barabási, A.-L., & Albert, R. (1999). Emergence of scaling in random networks. *Science*, *286*(5439), 509–512. https://www.jstor.org/stable/2899318 https://doi.org/10.1126/science.286.5439.509

Beaumier, G., & Cartwright, M. (2023). Cross-network weaponization in the semiconductor supply chain. *International Studies Quarterly*, *68*(1), sqae003. https://doi.org/10.1093/isq/sqae003

Bradford, A. (2023). *Digital empires: The global battle to regulate technology*. Oxford University Press.

Bremmer, I. (2021). The technopolar moment: How big tech will reshape the global order. *Foreign Affairs*, *100*(6), 112–128.

Bryson, J. J., & Malikova, H. (2021). Is there an AI cold war? *Global Perspectives*, *2*(1), 24803. https://doi.org/10.1525/gp.2021.24803

Cartwright, M. (2020). Internationalising state power through the internet: Google, Huawei and geopolitical struggle. *Internet Policy Review*, *9*(3). https://doi.org/10.14763/2020.3.1494

Chen, W. (2022). Zoom in and zoom out the glocalized network: When transnationalism meets geopolitics and technopolitics. *Information, Communication & Society*, *25*(16), 2381–2396. https://doi.org/10.1080/1369118X.2022.2118545

Choer Moraes, H., & Wigell, M. (2022) Balancing dependence: The quest for autonomy and the rise of corporate geoeconomics. In M. Babić, A. D. Dixon, & I. T. Liu (Eds.), *The political economy of geoeconomics: Europe in a changing world* (pp. 29–55). Palgrave Macmillan.

Cowhey, P. F. (1990). The international telecommunications regime: The political roots of regimes for high technology. *International Organization*, *44*(2), 169–199. https://doi.org/10.1017/S0020818300035244

De Goede, M. (2021). Finance/security infrastructures. *Review of International Political Economy*, *28*(2), 351–368. https://doi.org/10.1080/09692290.2020.1830832

De Goede, M., & Westermeier, C. (2022). Infrastructural geopolitics. *International Studies Quarterly*, *66*(3), sqac033. https://doi.org/10.1093/isq/sqac033

Dover, R. (2014). The world's second oldest profession: The Transatlantic spying scandal and its aftermath. *The International Spectator*, *49*(2), 117–133. https://doi.org/10.1080/03932729.2014.904989

Eling, M., Elvedi, M., & Falco, G. (2023). The economic impact of extreme cyber risk scenarios. *North American Actuarial Journal*, *27*(3), 429–443. https://doi.org/10.1080/10920277.2022.2034507

Erie, M. S., & Streinz, T. (2021). The Beijing Effect: China's digital Silk Road as transnational data governance. *New York University Journal of International Law and Politics*, *54*(1), 1–92. https://www.nyujilp.org/wp-content/uploads/2022/02/NYUJILP_Vol54.1_Erie_Streinz_1-91.pdf

European Union. (2022). Decision (EU) 2022/2481 of the European Parliament and of the Council of 14 December 2022 establishing the Digital Decade Policy Programme 2030. *Official Journal of the European Union, L*, *323*, 4–26. https://eur-lex.europa.eu/eli/dec/2022/2481/oj

Evans, P. C., & Gawer, A. (2016, January 2016). *The rise of the platform enterprise: A global survey*. The Centre for Global Enterprise. https://www.thecge.net/app/uploads/2016/01/PDF-WEB-Platform-Survey_01_12.pdf

Farrell, H., & Newman, A. (2016). The transatlantic data war: Europe fights back against the NSA. *Foreign Affairs*, *95*(1), 124–133. https://www.jstor.org/stable/43946632

Farrell, H., & Newman, A. (2019a). Weaponized interdependence: How global economic networks shape state coercion. *International Security*, *44*(1), 42–79. https://doi.org/10.1162/isec_a_00351

Farrell, H., & Newman, A. (2019b). Weaponized globalization: Huawei and the emerging battle over 5G networks. *Global Asia*, *14*(3), 8–12. https://www.globalasia.org/v14no3/cover/weaponized-globalization-huawei-and-the-emerging-battle-over-5g-networks_henry-farrellabraham-newman

Farrell, H., & Newman, A. (2023). *Underground empire: How America weaponized the world economy*. Henry Holt and Co.

Ferracane, M. (2022). *The Digital Trade Integration database: Description of pillars and indicators* (Working paper no. RSC 2022/70). Robert Schuman Centre for Advanced Studies Research. https://cadmus.eui.eu/bitstream/handle/1814/75011/RSC_WP_2022_70.pdf

Germann, J. (2023). Global rivalries, corporate interests and Germany's 'National Industrial Strategy 2030'. *Review of International Political Economy*, *30*(5), 1749–1775. https://doi.org/10.1080/09692290.2022.2130958

Gjesvik, L. (2023). Private infrastructure in weaponized interdependence. *Review of International Political Economy*, *30*(2), 722–746. https://doi.org/10.1080/09692290.2022.2069145

Gonzalo, M., Sly, M. H., Lavarello, P., & Harfuch, M. P. (2023). 5G kick-off in India and Brazil: InterState competition, national systems of innovation, and catch-up implications for the Global South. *Seoul Journal of Economics*, *36*(1), 53–78. https://doi.org/10.22904/sje.2023.36.1.002

Gray, J. E. (2021). The geopolitics of 'Platforms': The TikTok challenge. *Internet Policy Review*, *10*(2). https://doi.org/10.14763/2021.2.1557

Greene, J. (2020, November 25). *Amazon Web Services outage hobbles businesses*. Washington Post. https://www.washingtonpost.com/business/economy/amazon-web-services-outage-stymies-businesses/2020/11/25/b54a6106-2f4f-11eb-860d-f7999599cbc2_story.html

Gulati, R. (1999). Network location and learning: The influence of network resources and firm capabilities on alliance formation. *Strategic Management Journal*, *20*(5), 397–420. http://www.jstor.org/stable/3094162 https://doi.org/10.1002/(SICI)1097-0266(199905)20:5<397::AID-SMJ35>3.3.CO;2-B

Herr, T. (2020). *Four myths about the cloud: The geopolitics of cloud computing* (Report). Atlantic Council: Scowcroft Center for Strategy and Security and Cyber Statecraft Initiative. https://www.atlanticcouncil.org/in-depth-research-reports/report/four-myths-about-the-cloud-the-geopolitics-of-cloud-computing/

Hill, J. F. (2012). A Balkanized internet? The uncertain future of global internet standards. *Georgetown Journal of International Affairs*, 49–58. https://www.jstor.org/stable/43134338

Hirschman, A. (1958). *The strategy of economic development*. Yale University Press.

Hoffmann, S., Bradshaw, S., & Taylor, E. (2021). Great power rivalries in 5G technology markets. In C. A. Crocker, F. O. Hampson, & P. Aall (Eds.), *Diplomacy and the future of world order* (pp. 241). Georgetown University Press.

Hogan, M. (2015). Data flows and water woes: The Utah data center. *Big Data & Society*, *2*(2). https://doi.org/10.1177/2053951715592429

Hu, T.-H. (2016). *A prehistory of the cloud*. MIT Press.

Hussain, F., Hussain, Z., Khan, M. I., & Imran, A. (2024). The digital rise and its economic implications for China through the Digital Silk Road under the Belt and Road Initiative. *Asian Journal of Comparative Politics*, *9*(2), 238–253. https://doi.org/10.1177/20578911231174 73

International Monetary Fund. (2023). *Direction of trade statistics database* [data set]. IMF Data Portal. https://data.imf.org/?sk=9d6028d4-f14a-464c-a2f2-59b2cd424b85

Katz, M. L., & Shapiro, C. (1994). Systems competition and network effects. *Journal of Economic Perspectives*, *8*(2), 93–115. https://doi.org/10.1257/jep.8.2.93

Keane, M., & Yu, H. (2019). A digital empire in the making: China's outbound digital platforms. *International Journal of Communication*, *13*, 4624–4641. https://ijoc.org/index.php/ijoc/article/view/10995?fbclid=IwAR0FZPRRc_vsXI_2OlKZpx79M20SH-VTYqd7sH1KY95Bm6IIJzRf1Ok-I9M

Kello, L. (2022). *Striking back: The end of peace in cyberspace and how to restore it*. Yale University Press.

Keshk, O. M. G., Pollins, B. M., & Reuveny, R. (2004). Trade still follows the flag: The primacy of politics in a simultaneous model of interdependence and armed conflict. *The Journal of Politics*, *66*(4), 1155–1179. https://doi.org/10.1111/j.0022-3816.2004.00294.x

Kwet, M. (2019). Digital colonialism: US empire and the new imperialism in the Global South. *Race & Class*, *60*(4), 3–26. https://doi.org/10.1177/0306396818823172

Lambach, D., & Oppermann, K. (2023). Narratives of digital sovereignty in German political discourse. *Governance*, *36*(3), 693–709. https://doi.org/10.1111/gove.12690

Lavery, S. (2024). Rebuilding the fortress? Europe in a changing world economy. *Review of International Political Economy*, *31*(1), 330–353. https://doi.org/10.1080/09692290.2023.2211281

Leeds, B., Ritter, J., Mitchell, S., & Long, A. (2002). Alliance treaty obligations and provisions, 1815-1944. *International Interactions*, *28*(3), 237–260. https://doi.org/10.1080/03050620213653

Lehdonvirta, V. (2022). *Cloud empires: How digital platforms are overtaking the state and how we can regain control*. MIT Press.

Lehdonvirta, V., Wú, B., & Hawkins, Z. (2024). Compute north vs. compute south: The uneven possibilities of compute-based AI governance around the globe. *Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society*, *7*(1), 828–838. https://doi.org/10.1609/aies.v7i1.31683

Liu, L. (2021). The rise of data politics: Digital China and the world. *Studies in Comparative International Development*, *56*(1), 45–67. https://doi.org/10.1007/s12116-021-09319-8

Liu, E., Akiwate, G., Jonker, M., Mirian, A., Savage, S., & Voelker, G. M. (2021). Who's got your mail? Characterizing mail service provider usage. *Proceedings of the 21st ACM Internet Measurement Conference* (pp. 122–136). https://doi.org/10.1145/3487552.3487820

Malkin, A., & He, T. (2024). The geoeconomics of global semiconductor value chains: Extraterritoriality and the US-China technology rivalry. *Review of International Political Economy*, *31*(2), 674–699. https://doi.org/10.1080/09692290.2023.2245404

Maoz, Z., Johnson, P. L., Kaplan, J., Ogunkoya, F., & Shreve, A. P. (2019). The Dyadic Militarized Interstate Disputes (MIDs) dataset version 3.0: Logic, characteristics, and comparisons to alternative datasets. *Journal of Conflict Resolution*, *63*(3), 811–835. https://doi.org/10.1177/0022002718784158

Masanet, E., Shehabi, A., Lei, N., Smith, S., & Koomey, J. (2020). Recalibrating global data center energy-use estimates. *Science (New York, N.Y.)*, *367*(6481), 984–986. https://doi.org/10.1126/science.aba3758

Mayer, V. (2023). When do we go from here? Data center infrastructure labor, jobs, and work in economic development time and temporalities. *New Media & Society*, *25*(2), 307–323. https://doi.org/10.1177/14614448221149947

Mayer, M., & Lu, Y.-C. (2023). Digital autonomy? Measuring the global digital dependence structure. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4404826

Meltzer, J. P. (2015). The internet, cross-border data flows and international trade. *Asia & the Pacific Policy Studies*, *2*(1), 90–102. https://doi.org/10.1002/app5.60

Miller, C. (2022). *Chip war: The fight for the world's most critical technology*. Simon & Schuster UK.

Mosco, V. (2014). *To the cloud: Big data in a turbulent world*. Routledge.

Moss, S. (2022, July 7). *Ukraine awards Microsoft and AWS peace prize for cloud services & digital support*. Data Center Dynamics. https://www.datacenterdynamics.com/en/news/ukraine-awards-microsoft-andaws-peace-prize-for-cloud-services-digital-support/

Mulder, N. (2022). *The economic weapon: The rise of sanctions as a tool of modern war*. Yale University Press.

Munn, L. (2023). Red territory: Forging infrastructural power. *Territory, Politics, Governance*, *11*(1), 80–99. https://doi.org/10.1080/21622671.2020.1805353

Nanni, R. (2022). Digital sovereignty and internet standards: Normative implications of public-private relations among Chinese stakeholders in the Internet Engineering Task Force. *Information, Communication & Society*, *25*(16), 2342–2362. https://doi.org/10.1080/1369118X.2022.2129270

Narayan, D. (2022). Platform capitalism and cloud infrastructure: Theorizing a hyper-scalable computing regime. *Environment and Planning A: Economy and Space*, *54*(5), 911–929. https://doi.org/10.1177/0308518X221094028

Narlikar, A. (2021). Must the weak suffer what they must? The global south in a world of weaponized interdependence. In D. W. Drezner, H. Farrell, & A. L. Newman (Eds.), *The uses and abuses of weaponized interdependence*(pp. 289–304). Brookings Institution Press.

Natalegawa, A., & Poling, G. B. (2022, May 5). *The Indo-Pacific economic framework & digital trade in Southeast Asia*. Center for Strategic & International Studies (CSIS). https://www.csis.org/analysis/indo-pacific-economic-framework-and-digital-trade-southeast-asia

Naughton, B. (2020). Chinese industrial policy and the Digital Silk Road: The case of Alibaba in Malaysia. *Asia Policy*, *15*(1), 23–39. https://doi.org/10.1353/asp.2020.0006

Plantin, J.-C., & De Seta, G. (2019). WeChat as infrastructure: The techno-nationalist shaping of Chinese digital platforms. *Chinese Journal of Communication*, *12*(3), 257–273. https://doi.org/10.1080/17544750.2019.1572633

Poutala, T., Sinkkonen, E., & Mattlin, M. (2022). EU strategic autonomy and the perceived challenge of China: Can critical hubs be de-weaponized? *European Foreign Affairs Review*, *27*(Special Issue), 79–98. https://doi.org/10.54648/EERR2022015

Qiu, J. L., Yu, P. K., & Oreglia, E. (2022). A new approach to the geopolitics of Chinese internets. *Information, Communication & Society*, *25*(16), 2335–2341. https://doi.org/10.1080/1369118X.2022.2136856

Rabe, W., & Kostka, G. (2023). China's growing digital reach: Explaining citizens' high approval rates of fintech investments in Southeast Asia. *Review of International Political Economy*, *30*(3), 1098–1124. https://doi.org/10.1080/09692290.2022.2044884

Radu, R. (2019). *Negotiating internet governance* (1st ed.). Oxford University Press.

Raymond, M., & DeNardis, L. (2015). Multistakeholderism: Anatomy of an inchoate global institution. *International Theory*, *7*(3), 572–616. https://doi.org/10.1017/S1752971915000081

Roberts, A., Choer Moraes, H., & Ferguson, V. (2019). Towards a geoeconomic order in international trade and investment. *Journal of International Economic Law*, *22*(4), 655–676. https://doi.org/10.1093/jiel/jgz036

Rodrigues Vieira, V. G. (2023). The limits of weaponised interdependence after the Russian war against Ukraine. *Contemporary Security Policy*, *44*(4), 642–660. https://doi.org/10.1080/13523260.2023.2256065

Rone, J. (2024). The shape of the cloud: Contesting date centre construction in North Holland. *New Media & Society*, *26*(10), 5999–6018. https://doi.org/10.1177/14614448221145928

Ruan, L. (2018, June 22). *Big data in China and the battle for privacy* (Issues paper report no.5/2018). Australian Strategic Policy Institute. https://www.aspi.org.au/report/big-data-china-and-battle-privacy

Shen, H., & He, Y. (2022). The geopolitics of infrastructuralized platforms: The case of Alibaba. *Information, Communication & Society*, *25*(16), 2363–2380. https://doi.org/1369118X.2022.2128599

Soldatov, A., & Borogan, I. (2022, June 7). *The new iron curtain*. Center for European Policy Analysis (CEPA). https://cepa.org/comprehensive-reports/the-new-iron-curtain-2/

Srnicek, N. (2022). Data, compute, labor. In M. Graham, & F. Ferrari (Eds.), *Digital work in the planetary market* (pp. 241–261). MIT Press.

Starosielski, N. (2015). *The undersea network*. Duke University Press.

Stocker, V., Knieps, G., & Dietzel, C. (2021). The rise and evolution of clouds and private networks – internet interconnection, ecosystem fragmentation. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3910108

Talukder, A. K., Zimmerman, L., & Prahalad, H. A. (2010). Cloud economics: Principles, costs, and benefits. In N. Antonopoulos, & L. Gillam (Eds.), *Cloud computing* (pp. 343–360). Springer London.

Walter, S. (2021). The backlash against globalization. *Annual Review of Political Science*, *24*(1), 421–442. https://doi.org/10.1146/annurev-polisci-041719-102405

Warrell, H., & Fildes, N. (2021, October 25). *Amazon strikes deal with UK spy agencies to host top-secret materials*. Financial Times. https://www.ft.com/content/74782def-1046-4ea5-b796-0802cfb90260

World Cities Database. (2024). *Simplemaps: Interactive maps & data* [data set]. https://simplemaps.com/data/world-cities

Zhang, K. H. (2024). Geoeconomics of US-China tech rivalry and industrial policy. *Asia and the Global Economy*, *4*(2), 100098. https://doi.org/10.1016/j.aglobe.2024.100098