Cartwright, Madison

Article

Internationalising state power through the internet: Google, Huawei and geopolitical struggle

Internet Policy Review

Provided in Cooperation with:
Alexander von Humboldt Institute for Internet and Society (HIIG), Berlin

Suggested Citation: Cartwright, Madison (2020) : Internationalising state power through the internet: Google, Huawei and geopolitical struggle, Internet Policy Review, ISSN 2197-6775, Alexander von Humboldt Institute for Internet and Society, Berlin, Vol. 9, Iss. 3, pp. 1-18, https://doi.org/10.14763/2020.3.1494

This Version is available at:
https://hdl.handle.net/10419/224937

INTERNET POLICY REVIEW
Journal on internet regulation

Volume 9 | Issue 3

Internationalising state power through the internet: Google, Huawei and geopolitical struggle

Madison Cartwright
Department of Government and International Relations, University of Sydney, Australia, madison.cartwright@sydney.edu.au

Published on 16 Sep 2020 | DOI: 10.14763/2020.3.1494

Abstract: This article argues that the United States (US) has been able to exploit the international market dominance of US-based internet companies in order to internationalise state power through surveillance programmes conducted by national security and law enforcement agencies. The article also examines the emerging threat to the US from China, which is attempting to establish 'geo-economic space' for its own internet and technology companies. As Chinese companies become more competitive, they threaten both the commercial dominance of US companies as well as the geopolitical power of the US state. Furthermore, the US has concerns that the entrance of Chinese companies into its own market, specifically Huawei, could make it susceptible to the 'internationalised' power of China – such as Chinese state surveillance. In response, the US has sought to shrink the 'geo-economic space' available to Huawei by using its firms, such as Google, to disrupt Huawei's supply chains.

Keywords: Surveillance, Huawei, Geopolitics, State power

Article information

Received: 26 Sep 2019 **Reviewed:** 21 Dec 2019 **Published:** 16 Sep 2020

Competing interests: The author has declared that no competing interests exist that have influenced the text.

URL:
http://policyreview.info/articles/analysis/internationalising-state-power-through-internet-google-huawei-and-geopolitical

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

This paper is part of Geopolitics, jurisdiction and surveillance, a special issue of Internet Policy Review *guest-edited by Monique Mann and Angela Daly.*

INTRODUCTION

This article examines the importance of the market dominance of private companies in geopolitical struggles between states. In particular, it assesses how the United States (US) has used the market dominance of its internet companies to attempt to restrict the growth of 'geo-economic space' for Chinese competitors. This is more broadly in response to the challenge that China now poses to US hegemony over global communication systems. Overall, the article argues that dominant private firms can have geopolitical significance, acting as conduits through which states can exercise power.

It is true that modern corporations have enormous economic power, which they can leverage for private political authority in the international economy (Büthe and Mattli, 2011; Elbra, 2014; Haufler, 2006; Quack and Dobusch, 2013; Tusikov, 2019b). However, international firms can also be used as conduits for internationalising state power through the extra-territorial application of state authority (Crasnic, Kalyanpur, and Newman, 2017; Farrell and Newman, 2019; Tusikov, 2016, 2019a). Whilst multinational corporations are integral to global internet governance, it is more true to say that *American* multinational corporations are (Tusikov, 2016). The US government can use this to its advantage. Other economic powers, such as the European Union (EU), have sought to exercise their own authority over US firms through reforms such as the General Data Protection Regulation (GDPR).

The US has internationalised its authority through private companies to pursue its security interests, including by harvesting data collected through the international operations of US internet firms (Farrell and Newman, 2019; Mann and Warren, 2018). Through programmes such as PRISM, the National Security Agency (NSA) and other law enforcement agencies have accessed data directly from major US internet firms, without having to make a request to the firms or having to obtain individual court orders (Greenwald and MacAskill, 2013). These firm-focused programmes were combined with so-called 'upstream' methods which harvested information from fibre optical cables and other infrastructure as data was in transit. Security agencies are able to achieve this because, as the NSA explained, "[m]uch of the world's communications flow through the U.S." (National Security Agency & Special Source Operations, 2013, p. 2, PDF).

However, in order for states to use private companies to internationalise their power, they must be able to exercise authority over these companies. That is, states must be able to compel a firm to, for example, grant security agencies access to its data. One way a state can achieve this is through controlling a company's access to its market – that is utilising the state's 'market power' (Tusikov, 2019a). However, other conditions, both exogenous and endogenous, are crucial in enabling states to effectively leverage market power (Crasnic et al., 2017; Farrell and Newman, 2010; Kaczmarek and Newman, 2011; Newman and Posner, 2011). This article focuses specifically on two such conditions: sunk cost, or the level of investment in a market, and jurisdictional substitutability, that is the availability of alternative markets (Crasnic et al., 2017). These conditions will determine if a state can exercise authority over private firms.

However, this is only useful in internationalising state power if these firms are *internationally dominant* in their respective markets. For example, the Society for Worldwide Interbank Financial Telecommunication (SWIFT) is a Belgian-based firm which handles approximately 80 percent of all global wire transfer traffic. Despite being a Belgian company, SWIFT has a data processing centre based in the US, where copies of transactions are temporarily stored. Following the September 11 attacks, the US Treasury subpoenaed SWIFT data as part of its

Terrorist Finance Tracking Program (de Goede, 2012). The authority of the US to subpoena SWIFT's data, the location of its data centre in the US, and the international reach of the firm (80 percent of the market) made SWIFT a useful tool for global surveillance.

The spatial location of a firm's operations will thus determine how useful it is to a state in internationalising state power. The firm must be sufficiently embedded within a state's territory in order for that state to exercise authority over it, meanwhile it must also have sufficient presence in foreign markets for the state to be able to internationalise that authority through the firm's operations. The so-called 'transnational' corporation is not placeless, and *where* it operates matters. If states have authority over firms that are particularly central to international economic activity, they can 'weaponise' them for geopolitical and security ends by coercing unfriendly states (Crasnic et al., 2017; Farrell and Newman, 2019).

This article analyses how control over internet companies has empowered the US in responding to the geopolitical threat posed by China. Whilst the internet has emerged over the past few decades, dominance over international information and communication infrastructure has been a source of conflict between great power states for over a century (Hills 2002; Powers and Jablonski, 2015). Control over international information flows is important to the geopolitical power of great power states and is often dominated by the world's hegemonic state (Hills, 2002). Geopolitical power refers to how the spatial allocation of resources between states shapes international politics.

The 'transnationality' of the internet does not diminish the role of geopolitics because, as will be discussed, internet businesses and infrastructure remain geographically concentrated within specific territories. Furthermore, the prominent role of private interests in the geopolitics of communications is not novel to the internet. Past technological innovations, such as submarine telegraph cables, broadcast radio and the telephone, all involved heavy involvement with private firms which would work with states to "alter established international power relations" (Hills, 2002, p. 7). Thus, emerging market competitors from other countries threaten not just the commercial interests of US firms but the geopolitical influence of the US state. In this way, the growing international competitiveness of Chinese internet and technology companies, such as Huawei, potentially threatens US national security by enabling the same sort of surveillance programmes that the US is known to engage in.

The article begins by discussing the literature on international market regulation to establish what conditions are required to exercise extraterritorial authority over multinational corporations. This section will also examine how extraterritorial authority can be used to internationalise state power. Second, the article illustrates that the US has considerable leverage over its internet firms, and that these firms have extensive international reach. The article then argues that taken together, the extraterritorial authority of the US and international operations of internet firms makes them useful conduits for internationalising US power. Last, the article analyses how the US has used this power to respond to an emerging threat to its hegemonic position from China, through the growing international dominance of Chinese companies, in particular Huawei. The article examines how the US has sought to leverage its incumbent position in the market to disrupt Huawei's supply chains in an effort to slow its growth in international markets.

EXTRATERRITORIAL AUTHORITY AND STATE POWER

To illustrate how the US has internationalised its power through internet firms the article draws on the international market regulation literature. This literature analyses how domestic laws can establish rules in internationally-exposed markets (Farrell and Newman, 2010). Globalisation creates opportunities for states with large markets, such as the US, Europe and China, to extend and apply their regulations extraterritorially and effect enforcement in other jurisdictions (Farrell and Newman, 2015, 2016; Kaczmarek and Newman, 2011). However, market size is a necessary but not a sufficient variable in enabling states to do this. Domestic institutional capacity, such as the expertise and capabilities of regulators, are also important in allowing states to effectively leverage their market (Bach and Newman, 2010; Farrell and Newman, 2010).

As Crasnic et al. have illustrated, another important factor in the ability of states to apply extraterritorial authority is their access to multinational businesses and their capacity to "reach through the affiliate or subsidiary structure into the business practices of the corporate group" (2017, p. 911). This capacity is determined by two variables. The first is sunk cost: the investment of the firms in the state's market and thus the costs of exiting the market in an effort to avoid regulatory oversight. The second is jurisdictional substitutability: the availability of other markets with less stringent oversight that still provide comparable business opportunity. Therefore, states benefit from having a number of multinational firms with high sunk costs located within their national jurisdiction, with few suitable options for relocation.

The above two variables determine if a state has high or low levels of extraterritorial authority over a given firm, provided that the state has the institutional capacity to exercise this authority. However, the ability of states to internationalise state power through the firm depends on another variable: the dominance of that firm in international markets. Market dominance here refers to high levels of market share, as well as dominance over small but crucial elements of supply chains, in at least two different markets.

Table 1 illustrates how these two variables, extraterritorial authority and international market dominance, interact. As it shows, if a state has high levels of extraterritorial authority over a firm with high levels of international market dominance then the state has the ability to use the firm to internationalise its power, as the US was able to do with SWIFT as discussed above. However, if the state has low extraterritorial authority over a firm with high international market dominance then it may be subject to the internationalised power of other states. Firms with low levels of international market dominance primarily operate in a single domestic market and cannot be used to internationalise state power.

Table 1: Internationalising state power through firms

		Extraterritorial authority	
		High	**Low**

International market dominance	**High**	The firm can be used to internationalise state power.	The state may be subject to the internationalised power of other states using the firm.
	Low	The firm primarily operates domestically and cannot be used to internationalise state power.	The firm primarily operates in a foreign domestic market and cannot be used to internationalise state power.

It is important to make two further observations at this point. First, most international industries do not function as competitive markets but are dominated by a select few oligopolistic corporations (Mikler, 2011, 2018). This means that the ability to exercise extraterritorial authority over a few market leading firms can result in wide reaching effects on the entire international market. Second, these dominant firms are territorially embedded, in terms of sales, assets, employment and ownership, within a select few host states, the most prominent of which is the US (Mikler, 2011, 2018; Starrs, 2013). In other words, the most dominant firms have high sunk costs in powerful states. The internationalisation of corporations thus provides a powerful asset through which states can internationalise their power.

EXTRATERRITORIAL AUTHORITY AND STATE POWER ON THE INTERNET

The ability of the US state to realise its power through its internet firms is crucial to its mass online surveillance programmes. As the Snowden leaks revealed in 2013, US internet companies, including Microsoft, Google, Yahoo, Facebook and Apple, have all been used in US surveillance (Greenwald and MacAskill, 2013; National Security Agency and Special Source Operations, 2013, PDF). For example, Microsoft helped the NSA and the Federal Bureau of Investigation (FBI) gain access to encrypted information on its email, cloud storage and online voice chat services (Greenwald, MacAskill, Poitras, Ackerman, and Rushe, 2013).

Meanwhile, the NSA piggybacked on Google's cookies to identify targets for offensive hacking operations (Soltani, Peterson, and Gellman, 2013). The NSA also received or intercepted computer network devices such as routers being exported from the US and implanted them with backdoor surveillance tools (Greenwald, 2014). It was later revealed that after the Snowden leaks, in 2015, Yahoo built custom software to enable the NSA and the FBI to search incoming Yahoo email for specific information (Menn, 2016).

The above demonstrates that the US clearly can exercise authority over its internet firms in order to assist in online surveillance. Yet despite this, these firms have not sought to exit the US market in order to dodge this authority. Nor has the reputational damage from the Snowden and other leaks been sufficient to trigger market exit.

This should not be surprising because many of these companies are heavily invested in the US and thus have high sunk costs. For example, Alphabet (i.e. Google) holds 77 percent of its assets and employs 77 percent of its workers in the US and Microsoft holds 56 percent of its assets and employs 60 percent of its workers in the US. Amazon has less sunk costs in the US, holding 29 percent of its assets and employing 29 percent of its workers there, however this remains a considerable investment in the US (UNCTAD, 2019, XLS). Furthermore, the domestic market provides an outsized share of revenues for American firms: 46 percent of Alphabet's revenue came from within the US; 51 percent of Microsoft's revenue came from within the US; 61 percent of Amazon's revenue came from within the US; and 43 percent of Facebook's revenue came from within the US (Facebook Inc, 2019; UNCTAD, 2019, XLS). The high dependence on the US market means that jurisdictional substitutability is low.

However, substitutability is about more than sales and revenue. Internet firms have emerged within the US market and have developed their business models to match its regulatory environment, namely as it relates to liability for online intermediaries. This is particularly true for the US copyright regime. The *Digital Millennium Copyright Act of 1998* plays an important role in this, along with other legislation and public law which are unique to the US market, such as fair use (Samuelson, 2015). Of course, the US regulations could be changed, and if they were the high sunk costs and large dependence on the US market would discourage market exit. However, the US regulatory framework is, broadly speaking, favourable for internet firms when compared to alternative markets.

US internet companies have even complained to the US Trade Representative that copyright liability on internet intermediaries in Europe constitutes a trade barrier. The opposition to copyright law in Europe drove many internet companies to lobby against the Anti-Counterfeiting Trade Agreement, which included the EU in the negotiations. Meanwhile, US internet companies have attempted to export US-style copyright laws internationally, through US trade agreements (Cartwright, 2019).

In addition to high sunk costs and low jurisdictional substitutability, internet firms have also benefited from a sort of *jurisdictional protection* which has further increased the leverage of the US. 'Jurisdictional protection' has involved internet firms trying to avoid the extraterritorial application of laws from other countries by claiming that the US has primary authority over them. For example, in June 2017 the Canadian Supreme Court ruled that Google is required to globally delist content when removing it from its Canadian subsidiary, in a case involving counterfeit goods sold online (Supreme Court of Canada, 2017). However, Google prevented the enforcement of this ruling over its global network after a US District Court found in its favour in November 2017. The court found that Google meets the requirements for immunity from liability under the Section 230 of the *Communications Decency Act* – a US law. In the ruling the judge opined that "the Canadian order undermines the policy goals of Section 230 and threatens free speech on the global internet" (United States District Court, 2017, p. 6, PDF).

Google has similarly resisted efforts by European authorities to have their regulations apply across Google's global network. For example, in 2015 French authorities ordered Google to ensure that content removed under Europe's so-called 'right to be forgotten' laws was effective throughout Google's global network. However, Google refused to do this, only removing links from traffic coming from France. In 2019 the Court of Justice of the EU (CJEU) found that EU laws should not apply outside of the EU, and therefore Google would only be compelled to remove content across EU member states and not globally (Court of Justice of the European Union, 2019). Meanwhile, other European regulations, such as the General Data Protection Regulation (GDPR) and the recent Directive on Copyright in the Digital Single Market, have suffered from lack of enforcement in the face of intransigent US internet companies (Vinocur, 2019; Willsher, 2019). By contrast, US internet companies have willingly applied US domestic law across their global networks, including the *Digital Millennium Copyright Act*'s so-call 'take down' requirement which, like the examples above, requires companies to remove content from their networks. Both Google and Facebook apply these take-downs globally.

However, as table 1 illustrates, the ability to exercise authority over firms is only useful in internationalising state power if these firms are internationally dominant. This is certainly the case for US internet companies. Table 2 below shows the companies which both appear on the 2019 Fortune 500 list of largest corporations in the world by revenue, and which own a website that is among the top 50 most visited in the world (in July 2019). As the table illustrates, all of

these firms are based in either the US or China, and together they account for half of the top 50 most visited websites. Table 2 also shows the share of traffic each domain receives from its home market. As the table shows, top domains from US-based firms receive more traffic from outside the US market than from within it (with the exceptions of Amazon.com and eBay.com). This illustrates that the dominance of US-based firms is a result of their international competitiveness, not just the size of the US market.

Table 2: Top internet firms by traffic

Firm	Country HQ	Domain	Alexa rank	% of traffic from home market
Alphabet Inc.	US	Google.com	1	20.00%
		Youtube.com	2	14.40%
		Blogspot.com	22	9.70%
		Google.co.hk	30	5.40%
		Google.co.in	42	0.70%
Amazon.com	US	Amazon.com	12	67.30%
		Twitch.tv	37	31.30%
		Amazon.co.jp	46	8.10%
		Imdb.com	49	32.60%
Microsoft	US	Live.com	18	14.40%
		Bing.com	25	44.90%
		Office.com	32	33.60%
		Microsoft.com	33	26.30%
		Msn.com	47	20.50%
Facebook	US	Facebook.com	5	29.90%
		Instagram.com	24	29.30%
Alibaba Group Holding	China	Tmall.com	3	88.60%
		Taobao.com	8	88.50%
		Login.tmall.com	9	88.60%
		Pages.tmall.com	19	88.30%
		Alipay.com	23	90%
		Aliexpress.com	44	*
JD.com	China	Jd.com	14	88.20%

Firm	Country HQ	Domain	Alexa rank	% of traffic from home market
Tencent Holdings	China	Qq.com	6	87%
		Soso.com	41	98.70%
Source: (Alexa, 2019; Fortune Magazine, 2019). * No data as home market was ranked too low.				

US internet companies dominate other online markets as well. In 2019, Google's Chrome and Apple's Safari had a combined 79 percent share of the global internet browser market (StatCounter, 2020) [1]. Meanwhile, 16 of the 20 most installed apps through Google Play – the app marketplace for the Android operating system – are developed by either Google itself or Facebook. Of the 52 apps in the Google Play store which have over a billion installs, 34 are developed by either Facebook, Google or Microsoft (Androidrank, 2020). With US internet companies both being under the authority of the US state and being internationally dominant, they can thus be placed in the upper left quadrant of table 1 above. This makes them useful for the US in internationalising its power through surveillance programmes that have harvested information from these companies and their international networks.

INTERNATIONALISED POWER AND GEOPOLITICAL STRUGGLES

With high extraterritorial authority and international market dominance, internet companies can be powerful tools for the US state. However, this is increasingly under threat from China, which has developed a home grown internet sector of its own through targeted industrial policy, aided by information sovereignty and online censorship policies which have restricted the market access of foreign internet companies (i.e. the 'Great Firewall') (Hong, 2017, pp. 123-146; Powers and Jablonski, 2015). As Powers and Jablonski argue, "China is well on its way to having a popular and robust de facto intranet system" (Powers and Jablonski, 2015, p. 169), with 96 percent of all pageviews in China being of sites hosted within China. This is reflected in table 2 above, which shows that whilst Chinese firms have a strong presence on the internet, they nevertheless have low levels of *international* market dominance, mostly relying on their home market. However, China is increasingly moving from the techno-nationalist emphasis on developing home grown industries and technologies, to becoming more outwardly focused and more willing to pursue its own internet governance preferences – though with varying levels of success (Higgins 2017; Hong, 2017, pp. 141-145; Suttmeier, Yoa and Tan, 2009).

China's growing demands for "more power in allocation and control decisions about critical information resource" indicates "mounting geopolitical tensions centered on communications" (Hong, 2017, p. 11). First, in challenging the US hegemonic position, China is seeking to create a new 'geo-economic space' to maintain export markets for its emerging technology giants (Hong, 2017, p. 138). This is evident through international institution building, such as free trade agreements, as well as through China's ambitious Belt and Road Initiative (BRI). The BRI includes a so-called 'digital silk road' alongside its transportation infrastructure, which is being developed and built by Chinese firms (Shen, 2017). This 'digital road' has also "expanded the geographical range, organized specific policy funds, and coordinated an extensive network of resources for corporate China to go global" (Shen, 2017, p. 2688). Alibaba, for example, is

rapidly expanding its cloud computing business overseas, with a strong emphasis on BRI countries (Shen, 2017, p. 2689).

Second, as these geo-economic spaces are established Chinese firms are becoming more internationally competitive. For example, popular Chinese video-sharing app Douyin, owned by the Chinese parent company ByteDance, was launched internationally as 'Tiktok' in 2017. TikTok later merged with the US-owned video sharing app, music.ly, after it was bought by ByteDance. In November 2019, TikTok had been downloaded over a combined 1.5 billion times across the Apple App Store and Google Play store, up from the 500 million just 16 months earlier (Chapple, 2019). Another Chinese technology company enjoying increased growth is Huawei. In December 2015, Huawei's share of the international mobile vendor market was just two percent, however by December 2019 it had risen to ten percent. In Europe, Huawei's market share grew from four percent to 18 percent during the same period (StatCounter, 2020). As companies such as Huawei and ByteDance continue to emerge and gain market dominance, they have the potential to increase the geopolitical power of China by moving from the lower left to the upper left quadrant in table 1.

The US fears that this potential will be realised. In October 2019, Senators Tom Cotton and Charles ('Chuck') Schumer wrote to the Director of National Intelligence requesting an assessment of the national security risks posed by TikTok's collection of user data. The letter noted that while "the company has stated that TikTok does not operate in China and stores U.S. user data in the U.S., ByteDance is still required to adhere to the laws of China" (Schumer and Cotton, 2019, PDF). In other words, they were concerned not only by the company's growing international presence and collection of data, but also by the potential for China to exercise authority over ByteDance and thus internationalise state power. Two months later the Department of Treasury's Committee on Foreign Investment in the US opened an investigation into both TikTok's use of its users' data and its acquisition of music.ly (Espinosa de los Monteros Pereda, 2019).

On 6 August 2020, the Trump Administration responded to the security concerns over TikTok. In an executive order, President Trump declared that TikTok's "data collection threatens to allow the Chinese Communist Party access to Americans' personal and proprietary information" (Trump, 2020a). In response, the executive order issued a ban on 'transactions' with ByteDance, to be specified by the Secretary of Commerce within 45 days of the order. On the same day, similar restrictions were placed on other Chinese internet companies, including WeChat (Trump, 2020b). Reports prior to the executive order indicated that TikTok could be sold to an American company, Microsoft (a known PRISM participant), in order to avoid the ban (Isaac, Swanson and Rappeport, 2020). This would cut off ByteDance's *international* dominance, thus curtailing its ability to internationalise Chinese state power for surveillance purposes and thus the national security threat posed to the US.

The US has also long held concerns about the growing international reach of Huawei, and its perceived links to the Chinese government. In 2012, the House Intelligence Committee published an investigation into Huawei and ZTE's (another Chinese telecommunications company) involvement in the US telecommunications market. The report argued that the two companies posed a major threat for the US, as "to the extent these companies are influenced by the state, or provide Chinese intelligence services access to telecommunication networks, the opportunity exists for further economic and foreign espionage by a foreign nation-state already known to be a major perpetrator of cyber espionage" (Rogers and Ruppersberger, 2012, p. iv). That is, the report raised the concern that allowing Huawei or ZTE to gain a significant position

in the US market would allow China to internationalise its power through the companies and undermine the US national interest. US intelligence officials would later claim, in February 2020, that Huawei has indeed had 'backdoor' access to mobile phone networks through its telecommunications products since 2009 - which the company denies (Pancevski, 2020).

The House Intelligence Committee report advised US companies against trading with Huawei and ZTE, and recommended executive and legislative action to stall their growth in the US market (Rogers and Ruppersberger, 2012, pp. iv-vii). The following year, Huawei's Chief Executive Officer responded by beginning to exit the US market voluntarily, saying that "[i]f Huawei gets in the middle of U.S-China relations", and causes problems, "it's not worth it" (in Harris and Fish, 2013). In addition to preventing the 'espionage' detailed in the report, given the size and importance of the US market, this has also presumably hampered Huawei's international growth.

However, as the report also noted in 2012, the growing *global* presence of Chinese companies is also a concern. Whilst the US can restrict access to its own market, limiting the growth of these firms in third markets is more complicated. In particular, Huawei's deepening involvement in 5G infrastructure has become a major issue for the US, among others. An executive order from President Trump on 15 May 2019, though not specifically mentioning Huawei, articulated the US concerns:

> [F]oreign adversaries are increasingly creating and exploiting vulnerabilities in information and communications technology and services, which store and communicate vast amounts of sensitive information, facilitate the digital economy, and support critical infrastructure and vital emergency services, in order to commit malicious cyber-enabled actions, including economic and industrial espionage against the United States and its people. (Trump, 2019, PDF)

The response by the US has been to attempt to shrink the 'geo-economic space' available to Huawei by pressuring other states to ban the company from their national 5G rollouts. This has included traditional tools of statecraft. For example, the US has leveraged its market power by warning the United Kingdom that a post-Brexit trade deal with the US would not be possible if Huawei were to provide equipment for the 5G network there (Isaac, 2019). The US has also threatened to withhold intelligence from Germany should it allow Huawei involvement in its network (Pancevski and Germano, 2019). The United Kingdom would eventually ban Huawei from its 5G rollout in July 2020, however Germany and other european states remain open to the company playing some role in their networks (Baker and Chalmers, 2020). This illustrates the growing international market dominance of Huawei, and perhaps the waning influence of the US.

However, in addition to this bilateral pressure, the US has also been able to use its authority over US-based software and hardware firms to unilaterally disrupt Huawei's business. In this way, private US-based internet firms have become tools of statecraft, acting as conduits through which the US state can exercise power. The day after the Trump Administration made the above executive order, the US Department of Commerce placed Huawei and 68 of its affiliates [2] on the 'Entity List' believing there is "reasonable cause to believe that Huawei has been involved in activities contrary to the national security or foreign policy interests of the United States" (Bureau of Industry and Security, 2019). Being on the Entity List means that US firms must receive a license in order to trade with Huawei.

The ban on Huawei will have limited impact on its revenue or sales due to the loss of access to the US market, where it has no presence. However, Huawei is vulnerable to the US market for other reasons. Huawei relies heavily on US-based firms such as Intel, Qualcomm, and Xilinx for semiconductors and other components used in its products (King, Bergen, and Brody, 2019). Huawei phones also use the Android operating system. Therefore, the dominance of US-based firms in Huawei's supply chains means that the ban acts as a chokepoint on the firm, cutting it off from the vital hardware and software it needs to operate. The US has sought to protect this advantage, blocking takeovers of US semiconductor manufacturers on national security grounds – including proposed takeovers from Chinese companies (Woodhouse, 2018).

In response to Huawei being placed on the Entity List, Google suspended some of its business with Huawei on 19 May 2019, immediately ending Huawei's access to Android operating system updates. New Huawei products, meanwhile, would only have access to the Android Open Source Project version of the Android operating system, meaning that proprietary Google mobile applications such as the Google Play store, Gmail and YouTube would not be available (Moon, 2019). Losing access to Google apps is less a problem for Huawei in its main market, China, where Google itself is effectively banned. However, it is a major problem for Huawei's presence in foreign markets, particularly Europe where Huawei has a growing market share, considering Android's share of the mobile phone market is 72 percent both globally and in Europe (StatCounter, 2020).

However, a day after Google's suspension the US Department of Commerce issued a temporary general license, giving Huawei a 90 day reprieve so that businesses could prepare. The temporary general licence allows "certain activities necessary to the continued operations of existing networks and to support existing mobile services" (US Department of Commerce, 2019b). This has allowed Google to continue updating existing Huawei devices, however semiconductor manufacturers remain unable to supply Huawei with components to manufacture new devices.

The temporary general licence has since been extended four times, however the Department of Commerce believes the latest renewal, made on 15 May 2020, to be the last. It then urged companies to prepare to apply for individual licences in order to trade with Huawei once the general licence expired again on 3 August (US Department of Commerce, 2020). On 15 May 2020 the Department also further restricted Huawei's access to semiconductors by placing export restrictions on *foreign* manufactured components, mainly from Taiwan and South Korea, which use US software and/or US chip-making technology (Davis and Ferek, 2020).

However, despite the temporary general licences offered to Google, Huawei is nevertheless moving to a permanent Google-free position in order to maintain future reliability in its supply chains. Its newest flagship model, which has no access to the Google Play store, was launched in select international markets in late-2019 (Smith, 2020). As part of its commitment to moving away from Google, Huawei has joined three other companies to develop an alternative, and ultimately a competitor, to the Google Play store for the international market (Kirton, 2020). The success or failure of this initiative will ultimately determine how effective the Trump Administration's ban will be in limiting the growth of Huawei in international markets over the long-term. In the short-term, there is some evidence that the ban has hurt Huawei. Despite a surge in sales in its home market of China, Huawei's mobile sales have slumped elsewhere (Pham, 2019).

In the meantime, the US continues to restrict the 'geoeconomic space' available to Chinese-owned internet companies. In addition to the TikTok and WeChat bans discussed above, the US

has also expanded its so-called 'Clean Network' programme in an attempt to further sideline Chinese companies from telecommunications networks, mobile application stores, smartphones, cloud-based systems, and submarine internet cables. The Clean Network programme encourages other countries and private actors to shun 'untrusted' Chinese vendors with the explicit goal of securing national data against the "CCP's [Chinese Communist Party's] surveillance state" (Pompeo, 2020). The programme is thus directly aimed at hampering the ability of Chinese companies to gain international market dominance and by extension the ability of the Chinese state to internationalise its power and conduct surveillance abroad.

As Chinese companies become internationally competitive their market dominance increases. The US is concerned that this will enable Chinese technology and internet companies to access information on behalf of the Chinese state, in a similar way to how we know the US uses its own internet companies to conduct surveillance. In response to this threat the US has leveraged its incumbent position, using the dominance of its firms in supply chains to shrink the 'geo-economic space' available to Chinese companies. The ability of the US to impose export restrictions on even *foreign* manufactured goods, because they use US technology and software, illustrates the potential of exercising authority over firms with high market dominance to internationalising state power.

CONCLUSION

This article analysed the role of internet companies in the geopolitical struggle between the US and China. It illustrated how the US has been able to use internet firms to internationalise state power to conduct surveillance. The article began by arguing that internationalising state power through multinational firms depends on two variables. First, states must be able to exercise high levels of extraterritorial authority over firms. If a firm has high levels of sunk costs in a national market and/or if the firm has few alternative markets to exploit, then exiting that market to avoid regulatory oversight is costly. This increases the leverage of the state over the firm, creating high levels of extraterritorial authority – although this must be coupled with the institutional capacity to exercise this authority. Second, the firm subject to a state's extraterritorial authority must also be internationally dominant, either through having a high overall market share or by having a high share in a small but crucial part of a market's supply chain.

The article then examined the growing threat of China to the US hegemony over the internet, focusing specifically on China's efforts to internationalise its technology companies such as Huawei. This has included work by China to create 'geo-economic space' in which its companies can build international market dominance. The US not only sees these efforts as an economic risk to the competitiveness of its industries, but as a security and political threat. In response, the US has sought to shrink this geo-economic space, both by denying its own market and encouraging others to do the same. Finally, the US has also used the international market dominance of its companies to directly disrupt Huawei's operations and the appeal of its products in third markets.

REFERENCES

Alexa. (2019). *The top 500 sites on the web*. https://www.alexa.com/topsites

Androidrank. (2020). *List of Android Most Popular Google Play Apps*. Androidrank. https://www.androidrank.org/android-most-popular-google-play-apps?start=1&sort=4&price=all&category=all

Bach, D., & Newman, A. L. (2010). Governing lipitor and lipstick: Capacity, sequencing, and power in international pharmaceutical and cosmetics regulation. *Review of International Political Economy*, *17*(4), 665–695. https://doi.org/10.1080/09692291003723706

Baker, L., & Chalmers, J. (2020). As Britain bans Huawei, U.S. pressure mounts on Europe to follow suit. *Reuters*. https://www.reuters.com/article/us-britain-huawei-europe/as-britain-bans-huawei-u-s-pressure-mounts-on-europe-to-follow-suit-idUSKCN24F1XG

Bureau of Industry and Security, Commerce. (2019). *Addition of Entities to the Entity List, A Rule by the Industry and Security Bureau on 05/21/2019*. Federal Register. https://www.federalregister.gov/documents/2019/05/21/2019-10616/addition-of-entities-to-the-entity-list.

Büthe, T., & Mattli, W. (2011). *The New Global Rulers: The Privatization of Regulation in the World Economy*. Princeton University Press. https://doi.org/10.23943/princeton/9780691144795.001.0001

Cartwright, M. (2019). Business conflict and international law: The political economy of copyright in the United States. *Regulation & Governance*. https://doi.org/10.1111/rego.12272

Chapple, C. (2019, November 14). TikTok Clocks 1.5 Billion Downloads on The App Store and Google Play [Blog post]. *Sensort Tower Blog*. https://sensortower.com/blog/tiktok-downloads-1-5-billion

Crasnic, L., Kalyanpur, N., & Newman, A. (2017). Networked liabilities: Transnational authority in a world of transnational business. *European Journal of International Relations*, *23*(4), 906–929. https://doi.org/10.1177/1354066116679245

Davis, B., & Ferek, K. /S. (2020, May 15). U.S. Moves to Cut Off Chip Supplies to Huawei. *The Wall Street Journal*. https://www.wsj.com/articles/u-s-moves-to-cut-off-chip-supplies-to-huawei-11589545335

De Goede, M. (2012). The SWIFT affair and the global politics of European security. *Journal of Common Market Studies*, *50*(2), 214–230. https://doi.org/10.1111/j.1468-5965.2011.02219.x

Donnan, S., Leonard, J., & King, I. (2019, July 23). Trump meets with tech CEOs and takes a step toward easing Huawei ban. *The Los Angeles Times*. https://www.latimes.com/business/technology/story/2019-07-23/trump-moves-toward-easing-huawei-ban

Elbra, A. D. (2014). Interests need not be pursued if they can be created: Private governance in African gold mining. *Business and Politics*, *16*(2), 247–266. https://doi.org/10.1515/bap-2013-0021

Facebook Inc. (2019). *Form 10-K: Annual Report Pursuant to Section 13 or 15 (D) of the*

Securities Exchange Act of 1934 for the fiscal year ended December 31, 2018. Facebook Inc.

Farrell, H., & Newman, A. (2015). The new politics of interdependence: Cross-national layering in trans-Atlantic regulatory disputes. *Comparative Political Studies*, *48*(4), 497–526. https://doi.org/10.1177/0010414014542330

Farrell, H., & Newman, A. (2016). The new interdependence approach: Theoretical development and empirical demonstration. *Review of International Political Economy*, *23*(5), 713–736. https://doi.org/10.1080/09692290.2016.1247009

Farrell, H., & Newman, A. L. (2010). Making global markets: Historical institutionalism in international political economy. *Review of International Political Economy*, *17*(4), 609–638. https://doi.org/10.1080/09692291003723672

Farrell, H., & Newman, A. L. (2019). Weaponized Interdependence: How Global Economic Networks Shape State Coercion. *International Security*, *44*(1), 42–79. https://doi.org/10.1162/isec_a_00351

Fortune Magazine. (2019). The Fortune Global 500, 2019. *Fortune Magazine*. https://fortune.com/global500/2019/search/

Google LLC, successor in law to Google Inc. V Commission nationale de l'informatique et des libertés (CNIL), (Court of Justice of the European Union 2019).

Google L.L.C. v. Equustek Solutions Inc., (United States District Court, Northern District of California, San Jose Division 2017).

Google LLC v. Equustek Solutions Inc, SCC 34, [2017] 1 S.C.R. 824 (Supreme Court of Canada 2017).

Greenwald, G. (2014). *No place to hide: Edward Snowden, the NSA, and the US surveilance state*. Macmillan.

Greenwald, G., & MacAskill, E. (2013, June 7). NSA Prism program taps in to user data of Apple, Google and others. *The Guardian*. https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

Greenwald, G., MacAskill, E., Poitras, L., Ackerman, S., & Rushe, D. (2013, July 12). Microsoft handed the NSA access to encrypted messages. *The Guardian*. https://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data

Harris, S., & Fish, I. S. (2013, December 2). Accused of Cyberspying, Huawei Is 'Exiting the US Market'. *Foreign Policy*. https://foreignpolicy.com/2013/12/02/accused-of-cyberspying-huawei-is-exiting-the-u-s-market/

Haufler, V. (2006). Global Governance and the Private Sector. In C. May (Ed.), *Global Corporate Power* (pp. 85–103). Lynn Reinner Publishers.

Higgins, V. (2015). Beyond neo-techno-nationalism: An introduction to China's emergent third way: Globalised adaptive ecology, emergent capabilities and policy instruments. In *Alliance Capitalism, Innovation and the Chinese State* (pp. 115–145). Palgrave Macmillan. https://doi.org/10.1057/9781137529657_5

Hills, J. (2002). *The struggle for control of global communication: The formative century*. University of Illinois Press.

Hong, Y. (2017). *Networking China: The Digital Transformation of the Chinese Economy*. University of Illinois Press. https://doi.org/10.5406/illinois/9780252040917.001.0001

Isaac, A. (2019, July 13). US tells Britain: Fall into line over China and Huawei, or no trade deal. *The Telegraph*. https://www.telegraph.co.uk/business/2019/07/13/us-tells-britain-fall-line-china-huawei-no-trade-deal/

Isaac, M., Swanson, A., & Rappeport, A. (2020, July 31). Microsoft Said to Be in Talks to Buy TikTok, as Trump Weighs Curtailing App. *The New York Times*. https://www.nytimes.com/2020/07/31/technology/tiktok-microsoft.html

Kaczmarek, S. C., & Newman, A. L. (2011). The long arm of the law: Extraterritoriality and the national implementation of foreign bribery legislation. *International Organization*, *65*(4), 745–770. https://doi.org/10.1017/S0020818311000270

King, I., Bergen, M., & Brody, B. (2019, May 19). Top US Tech Companies Begin to Cut Off Vital Huawei Supplies. *Bloomberg*. https://www.bloomberg.com/news/articles/2019-05-19/google-to-end-some-huawei-business-ties-after-trump-crackdown

Kirton, D. (2020, February 6). Exclusive: China's mobile giants to take on Google's Play store—Sources. *Reuters*. https://www.reuters.com/article/us-china-mobile-exclusive/exclusive-chinas-mobile-giants-to-take-on-googles-play-store-sources-idUSKBN20018H

Mann, M., & Warren, I. (2018). The digital and legal divide: Silk Road, transnational online policing and southern criminology. In K. Carrington, R. Hogg, J. Scott, & M. Sozzo (Eds.), *The Palgrave handbook of criminology and the global south* (pp. 245–260). Palgrave MacMillan. https://doi.org/10.1007/978-3-319-65021-0_13

Menn, J. (2016, October 5). Exclusive: Yahoo secretly scanned customer emails for U.S. intelligence – sources. *Reuters*. https://www.reuters.com/article/us-yahoo-nsa-exclusive-idUSKCN1241YT

Mikler, J. (2011). The illusion of the 'power of markets'. *The Journal of Australian Political*, *68*, 41–61.

Mikler, J. (2018). *The political power of global corporations*. Polity Press.

Monteros Pereda, E. (2019, December 2). TikTok Under Investigation for Posing a Threat to National Security—Is Chinese Tech Running Out of Time in the U.S.? *JOLT Digest*. https://jolt.law.harvard.edu/digest/tiktok-under-investigation-for-posing-a-threat-to-national-security-is-chinese-tech-running-out-of-time-in-the-u-s

Moon, A. (2019, May 19). Exclusive: Google suspends some business with Huawei after Trump blacklist—Source. *Reuters*. https://www.reuters.com/article/us-huawei-tech-alphabet-exclusive/exclusive-google-suspends-some-business-with-huawei-after-trump-blacklist-source-idUSKCN1SP0NB

National Security Agency, and Special Source Operations. (2013).

https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH01f5/323b0a6e.dir/doc.pdf.

Newman, A. L., & Posner, E. (2011). International interdependence and regulatory power: Authority, mobility, and markets. *European Journal of International Relations*, *17*(4), 589–610. https://doi.org/10.1177/1354066110391306

Pancevski, B. (2020, February 12). U.S. Officials Say Huawei Can Covertly Access Telecom Networks. *The Wall Street Journal*. https://www.wsj.com/articles/u-s-officials-say-huawei-can-covertly-access-telecom-networks-11581452256

Pancevski, B., & Germano, S. (2019, March 11). Drop Huawei or See Intelligence Sharing Pared Back, US Tells Germany. *The Wall Street Journal*. https://www.wsj.com/articles/drop-huawei-or-see-intelligence-sharing-pared-back-u-s-tells-germany-11552314827

Pham, S. (2019, November 14). Huawei phones are still red hot in China. But the Google app ban is hurting sales overseas. *CNN*. https://edition.cnn.com/2019/11/14/tech/huawei-sales-mate-30/index.html

Pompeo, M. (2020, August 5). *Announcing the Expansion of the Clean Network to Safeguard America's Assets* [Press statement]. U. S. Department of State. https://www.state.gov/announcing-the-expansion-of-the-clean-network-to-safeguard-americas-assets/

Powers, S. M., & Jablonski, M. (2015). *The real cyber war: The political economy of internet freedom*. University of Illinois Press. https://doi.org/10.5406/illinois/9780252039126.001.0001

Quack, S., & Dobusch, L. (2013). Framing standards, mobilizing users: Copyright versus fair use in transnational regulation. *Review of International Political Economy*, *20*(1), 52–88. https://doi.org/10.1080/09692290.2012.662909

Rogers, M., & Ruppersberger, D. (2012). *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE* [Report]. House Intelligence Committee.

Samuelson, P. (2015). Possible futures of fair use. *Washington Law Reveiw*, *90*(2), 815–868. https://digitalcommons.law.uw.edu/wlr/vol90/iss2/9/

Schumer, C., & Cotton, T. (2019). *Letter to The Honorable Joseph Maguire*. https://www.democrats.senate.gov/imo/media/doc/10232019%20TikTok%20Letter%20-%20FINAL%20PDF.pdf

Shen, H. (2018). Building a digital silk road? Situating the Internet in China's belt and road initiative. *International Journal of Communication*, *12*, 2683–2701. https://ijoc.org/index.php/ijoc/article/view/8405

Smith, C. (2020, January 30). Huawei is done with Google for good. *BGR*. https://bgr.com/2020/01/30/huawei-android-ban-p40-pro-and-other-phones-wont-get-google-apps/

Soltani, A., Peterson, A., & Gellman, B. (2013, December 10). NSA uses Google cookies to

pinpoint targets for hacking. *The Washington Post*. https://www.washingtonpost.com/news/the-switch/wp/2013/12/10/nsa-uses-google-cookies-to-pinpoint-targets-for-hacking/

Starrs, S. (2013). American Economic Power Hasn't Declined—It Globalized! Summoning the Data and Taking Globalization Seriously. *International Studies Quarterly*, *57*(4), 817–830. https://doi.org/10.1111/isqu.12053

StatCounter. (2020). *GlobalStats*. https://gs.statcounter.com/

Suttmeier, R. P., Yao, X., & Tan, A. Z. (2009). Standards of power? Technology, institutions, and politics in the development of China's national standards strategy. *Geopolitics, History, and International Relations*, *1*(1), 46–84.

Trump, D. J. (2019). *Executive Order 13873: Securing the Information and Communications Technology and Services Supply Chain*. Homeland Security Digital Library. https://www.hsdl.org/?view&did=825242

Trump, D. J. (2020a). *Executive Order on Addressing the Threat Posed by TikTok*. The White House. https://www.whitehouse.gov/presidential-actions/executive-order-addressing-threat-posed-tiktok/

Trump, D. J. (2020b). *Executive Order on Addressing the Threat Posed by WeChat*. The White House. https://www.whitehouse.gov/presidential-actions/executive-order-addressing-threat-posed-wechat/

Tusikov, N. (2016). *Chokepoints: Global Private Regulation on the Internet*. University of California Press. https://doi.org/10.1525/california/9780520291218.001.0001

Tusikov, N. (2019a). How US-made rules shape internet governance in China. *Internet Policy Review*, *8*(2). https://doi.org/10.14763/2019.2.1408

Tusikov, N. (2019b). Regulation through "bricking": Private ordering in the "Internet of Things". *Internet Policy Review*, *8*(2). https://doi.org/10.14763/2019.2.1405

United Nations Conference on Trade and Development. (2019). *World Investment Report: Annex table 19. The world's top 100 non-financial MNEs, ranked by foreign assets, 2018*. World Investment Report: Annex Tables. https://unctad.org/Sections/dite_dir/docs/WIR2020/WIR2020Tab19.xlsx

United States Department of Commerce. (2019a, May 20). *Department of Commerce Issues Limited Exemptions on Huawei Products* [Press release]. https://www.commerce.gov/news/press-releases/2019/05/department-commerce-issues-limited-exemptions-huawei-products

United States Department of Commerce. (2019b, August 19). *Department of Commerce Adds Dozens of New Huawei Affiliates to the Entity List and Maintains Narrow Exemptions through the Temporary General License* [Press release]. https://www.commerce.gov/news/press-releases/2019/08/department-commerce-adds-dozens-new-huawei-affiliates-entity-list-and

United States Department of Commerce. (2020, May 15). *Department of Commerce Issues Expected Final 90-Day Extension of Temporary General License Authorizations* [Press

release]. https://www.commerce.gov/news/press-releases/2020/05/department-commerce-issues-expected-final-90-day-extension-temporary

Vinocur, N. (2019, December 12). We have a huge problem': European tech regulator despairs over lack of enforcement. *Politico*. https://www.politico.com/amp/news/2019/12/27/europe-gdpr-technology-regulation-089605

Willsher, K. (2019, October 17). France accuses Google of flouting EU copyright law meant to help news publishers. *Los Angeles Times*. https://www.latimes.com/business/story/2019-10-17/france-accuses-google-ignoring-copyright-law

Woodhouse, A. (2018, February 23). US blocks Chinese takeover of semiconductor equipment company. *Financial Times*. https://www.ft.com/content/b3ad7274-1842-11e8-9376-4a6390addb44

FOOTNOTES

1. Browser market shared based on volume of internet usage. Market share shown is the average of the monthly market share in 2019.

2. This was later expanded to 114 affiliates on 19 August 2019 (US Department of Commerce, 2019a)