Original Article

Global Media and China
2023, Vol. 8(1) 6–23

DOI: 10.1177/20594364221139729
journals.sagepub.com/home/gch
SAGE

The weaponization of private corporate infrastructure: Internet fragmentation and coercive diplomacy in the 21st century

Juan Ortiz Freuler
University of Southern California Annenberg School for Communication and Journalism, USA; Berkman Klein Center for Internet and Society, Harvard University, USA

Abstract

In the early 1990s, US leaders promoted the internet as post-nation "global information infrastructure." However, throughout the 2000s, critical internet infrastructure became centralized under the tight control of a handful of US-based multinational companies. This paper examines the US government's willingness to leverage its regulatory control over privately run critical infrastructure to exercise massive internet surveillance (*pulling* information from sovereign states), massive influence campaigns (*pushing* information into sovereign states), and, increasingly, to levy unilateral cyber-sanctions on other sovereign states (*cutting* information flows through blockages and digital lock-outs). The US government is now asserting its territorial sovereignty over what it had presented as global infrastructure in order to advance its narrow national goals. I argue that the weaponization of corporate internet infrastructure by the US government marks a new era of internet governance and is one of the key drivers of what is often discussed as internet fragmentation in internet governance forums.

Keywords

internet governance, internet fragmentation, digital infrastructure, public diplomacy, sanctions, cyber-sanctions, surveillance, antitrust, digital lock-out

Corresponding author:
Juan Ortiz Freuler, Berkman Klein Center for Internet and Society at Harvard University; and University of Southern California Annenberg School for Communication and Journalism, 3502 Watt Way, Los Angeles, CA 90089-0040, USA.
Email: ortizfre@usc.edu

Introduction

> *"legislators, regulators, and business people must do this: build and operate a Global Information Infrastructure. This [Global Information Infrastructure] will circle the globe with information superhighways on which all people can travel."*
>
> **-US Vice President, Al Gore,** at the 1994 ITU meeting in Buenos Aires, Argentina (Gore, 1994)
>
> "*We call on all freedom-loving nations and companies to join the Clean Network.*"
>
> **-US Secretary of State, Michael R. Pompeo,** announcing the Clean Network in 2020 (US Department of State, 2020)

In the early days of the internet, the US government representatives portrayed the internet as a *Global Information Infrastructure*. However, now the US is asserting its sovereignty over large swathes of the existing information infrastructure and leveraging legal control over it to coerce governments and shape the process of re-networking of humankind's global information system. These actions, I argue, are a deliberate attempt to carve out an information ecosystem that the US government can keep under greater control, even as its standing as the single global power recedes. This paper dissects the economic and geopolitical drivers of this process, and distills them into three historical phases.

Conceptual Framework

Over the past 30 years, the internet has gone from being the niche technology for academics and programmers in affluent countries, to being used by over 50% of the human population. The evolving characteristics and uses of the internet inevitably impact the ways in which governance over the internet is conceptualized and enacted. Meanwhile, the processes of governance themselves shape the internet as such, meaning that the definition of the internet and internet governance are intertwined, dynamic, and unstable.

Definitions of governance are varied, but typically incorporate formal and realist aspects. Whereas for Drake governance refers to "all the ways in which groups of people collectively make choices"(2000), for DeNardis, governance is "the exercise of power to enact a certain set of public interest goals"(2014). When it comes to governance over the internet, the 2011 World Summit on the Information Society (WSIS) referred to "the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programs that shape the evolution and use of the Internet" (Azmeh et al., 2020).

The implicit points of contention in each of these definitions is who is being represented, how interests are balanced, and how responses to such questions change over time as the internet evolves. The internet went from being a niche US system of information to a cornerstone of global economic development (Cowhey & Aronson, 2018) of which the US population now represents barely 7.5%.[1] That is, over time, the internet has indeed become the *Global Information Infrastructure* that Al Gore alluded to, and, as such, the internet has become more relevant to the world. Meanwhile, and conversely, the US user-base has become relatively less relevant to the internet ecosystem. As a result, the US government's attempts to exercise its sovereignty over the internet are becoming more problematic. Alliances, such as the Shanghai Cooperation Organization (SCO), originally called Shanghai Five,—now comprising China, Russia, India, Pakistan, and other countries that together

have a combined population of more than 3 billion people—have come to agree that they should coordinate against "security threats" that can undermine their "political and social systems'" (Hartley et al., 2017 p.3). Amongst the threats listed in an agreement signed in 2008, the fourth refers to the: "use of dominant position in the information space to the detriment of the interests and security of other countries." The document underlines that this threat is materialized by "embedding hidden features and functions in software and equipment supplied to other countries to monitor and influence the information resources and/or critically important structures of these countries" (Shanghai Cooperation Organization, 2008).

Internet governance scholars believe these geopolitical tensions lead towards a more fragmented internet (Hill, 2012). In a 2016 report, Drake, Cerf, and Kleinwächter found that definitions of fragmentation tended to focus on a lack of technical interoperability between information technologies. However, they argued that these definitions were incomplete and outlined three forms of fragmentation: technical, governmental, and commercial (Drake et al., 2016). This paper focuses primarily on *Governmental Fragmentation:* "Government policies and actions that constrain or prevent certain uses of the Internet to create, distribute, or access information resources." (p. 7)

A key section of this paper focuses on how sanctions fuel and shape the process of fragmentation. The US' reliance on sanctions is not novel. However, over the past 21 years sanctions designations have increased by 933% (U.S. Department of the Treasury, 2021). Furthermore, when it comes to cyber-sanctions, three developments place us within a particularly novel and challenging scenario: The growing dependence on information technology, the growing reliance on cloud computing, and the market dominance of US companies.

In line with this realization, in Weaponized Interdependence (2019), Farrell and Newman argue that the "asymmetric network structures create the potential for 'weaponized interdependence', in which some states leverage interdependent relations to coerce others" (p. 4). This paper expands on this framework by specifically applying it to private corporate infrastructure that is critical to the internet, thus complementing ongoing discussions regarding the geopolitical contests around communication infrastructures (Winseck, 2019) and standards (Becker et al., 2022), amongst others.

Furthermore, I suggest broadening the framework. Farrell and Newman claim that the main goal of sanctions is coercion and conclude that it does not seem to be effective at achieving such overarching goals. Although I agree with such assessment, in this paper I suggest that rather than focusing on the specific action of cutting access to a critical piece of infrastructure in one country in one specific instance, we need to understand how the combination of a full toolkit of push, pull, and cut powers being leveraged over time by different Departments of the US government, leads to a redesign of the network topography. A redesign that the US expects might better secure its commercial and national security interests.

Key Argument

Taking a realist theoretical lens, this paper dissects the US government's approach towards the internet and internet governance. I argue that the past 30 years can be understood as comprising three distinct phases:

1. **Global Information Infrastructure (1990–2001):** US public officials proclaimed the internet would be a shared and global resource for cultural and economic development;
2. **Consolidation for a networked Global Intelligence Infrastructure (2002–2016):** the market consolidated around a handful US multinational corporations and the US government relied on such

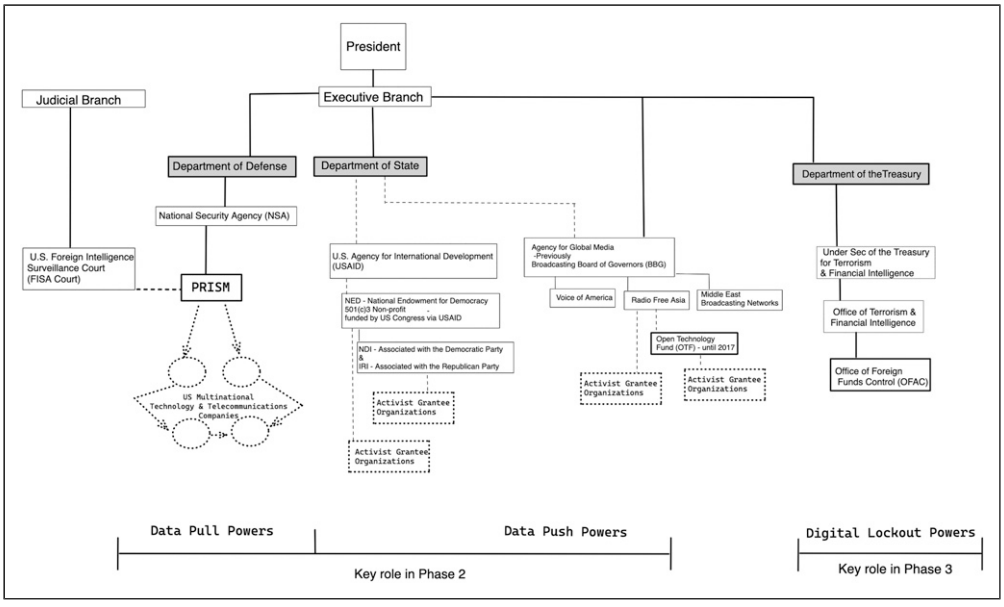

Figure 1. A diagram synthesizing the key agencies that are exercising pull, push, and cut powers within the US.

centralized network to effectively *pull* data from intelligence targets and *push* data into countries striving to limit its circulation;

3. **Realignments and Re-Networking towards a Post-Global Information Infrastructure (2016-Ongoing)**: the US government began to leverage key US companies to deploy unilateral cyber-sanctions against other countries in order to *cut* a target's access to critical data.

The process of observing and narrating past events often creates a mirage of inevitability or the existence of a plan. Though the developments within each phase inevitably shape and preclude events in subsequent phases, political processes are complex. The phases I articulate here are the result, among many other things, of disputes between people within the US Administration (see Figure 1) and beyond. Thus there are juxtapositions and mismatches across the proposed phases.

Furthermore, each act of pulling, pushing and cutting information flows by the US government is best understood as a frame within a larger moving picture. That is, understanding that the internet is in constant evolution, the Departments across the US government (see Figure 1) are exercising push, pull and cut powers that reshape the network topography. Their activity resembles the actions of a curling player: pushing and pulling a stick, cutting into the ice in an attempt to guide the sliding stone closer to the bullseye. Farrell and Newman (2019), by narrowly focusing on single frames of this procedure struggle to shed light on this overarching process. This paper makes the case for using Farrell and Newman's framework to understand not coercion but a procedure through which the internet topography is being modified. Throughout the next three sections, I analyze key events throughout these distinct phases to offer a richer account of a procedure often discussed as fragmentation, but which is best to conceptualize as re-networking.

Phase 1: A Global Information Infrastructure

This first phase takes place as the US emerges victorious from the cold war and is asserting its role as sole superpower under a neoliberal banner that equates democracy to market liberalization. In this post cold war scenario that characterizes the first phase, the US government is promoting deregulation across the world as a way to broaden the markets available to its companies.

Despite the internet being developed in the 1970s, the pace of adoption accelerated after Tim Berners-Lee and CERN agreed to release the web into the public domain in 1993. This decision reassured all interested parties that they could develop without the risk of being locked into a proprietary platform. Berners-Lee later explained this decision by stating that "you can't propose that something be a universal space and at the same time keep control of it" (Berners-Lee, 1998).

The standard narrative in the early days was that the new information networks unleashed horizontal collaboration. The network's logic, it was assumed, would reshape the topography of our social, economic and cultural systems (Castells, 2010). In accordance with the spirit of openness, the Department of Justice launched an investigation into Microsoft's dominance within the market of the PC operating systems. At the time, Microsoft controlled people's access point to the web.

The narrative was that the web was permissionless, and thus, it followed that access to it should not be controlled by a single company. Similarly, the core internet infrastructure was said to be borderless: the laws applicable to servers or engineers were presented as irrelevant facts. All were now networked into a post-nation-state infrastructure.

At the 1994 International Telecommunication Union (ITU) Conference in Argentina, Al Gore, then Vice-President of the United States, called upon the world leaders to embrace a Global Information Infrastructure. He presented it as a distributed system of interconnected servers and then claimed:

> "[it] will be a metaphor for democracy itself. Representative democracy does not work with an all-powerful central government, arrogating all decisions to itself. That is why communism collapsed." (Gore, 1994)

The principles nurturing this idea that big government was the antithesis of democracy would then percolate into the development of the multistakeholder model of internet governance. The underlying spirit was that the interests of the *multinational* corporations would not be properly represented by any particular national government. Within months of Gore's speech, Amazon, Ebay, Yahoo, and Internet Explorer were launched; companies that would become key gateways to the growing information infrastructure.

Two years after this ITU conference, Barlow released the Declaration of Independence for Cyberspace, stating "Governments of the Industrial World…You are not welcome among us." Many of the early internet advocates were not just liberal, but libertarians (Zittrain, 2019; Flew, 2022). And the US officials promoting internet adoption across the world were ready to leverage such a narrative: The internet was not a US project, but a global project. It was not US infrastructure that was going to be developed through collective effort, but a Global Information Infrastructure. A post-nation-state infrastructure for a post-nation-state world.

In 1998, this narrative, however, came into stark contrast with the US government's decision to position ICANN, the Internet Corporation for Assigned Names and Numbers that manages the root server system, under the control of the Department of Commerce (Castells, 2009). This decision triggered discontent and distrust from the international community that had been sold liberal and libertarian narratives. This decision marks the beginning of the end of this first phase of internet

governance: The global hegemon indeed still believed in the nation state and wanted a key chokepoint to be under the control of its own government officials.

The liberal narrative suffered a fatal blow at the beginning of the new millenia: the attack on the Twin Towers. Although the attacks could have been framed as an attack on the global financial system that the building housed, it was given a nationalist spin: the US had powerful enemies targeting the US as a nation (Bush, 2001). This choice of narrative led to a quick switch from openness and liberalism, to tighter governmental control and nationalism. By 2003, the US Department of Defense had updated its 1996 Information Operations Roadmap, which now included statements such as that "the Department will 'fight the net' as it would a weapons system" (US Department of Defense, 2003; Winseck, 2019).

Phase 2: Global Intelligence Infrastructure: Consolidation into and Within the Internet. Deployment of Techniques to Push and Pull Data Across Territories.

> *"On their own, new technologies do not take sides in the struggle for freedom and progress, but the United States does. [...] We are also supporting the development of new tools that enable citizens to exercise their rights of free expression by circumventing politically motivated censorship."*
>
> **- US Sec. of State, Hillary** Clinton, 2010

> *"..the companies themselves are American and are subject to American law. The problem is, they're also subject to classified American policies that pervert law and permit the US government to surveil virtually every man, woman, and child who has ever touched a computer or picked up a phone."*
>
> **- Edward Snowden, 2019** (Snowden, 2019)

If the first phase was one of openness, characterized by the proposal of collectively building a big tent everyone would then benefit from, phase 2 saw the US government exploiting such infrastructure to pursue the achievement of national goals.

In particular, phase 2 was characterized by two processes:

1. The US government allowing the market of internet platform and service providers to consolidate around a handful of US corporations;
2. The US government re-conceptualizing the internet as a tool for strategic coercion; one through which information could be
   2(a). secretly pulled *from* targets (PRISM; Patriot Act) by the Department of Defense; or
   2(b). pushed *onto* targets where states might be trying to limit its circulation (ToR, Open Tech Fund, Zunzuneo) by the Department of State;

To unfold this second phase, it is best to begin with the process of market consolidation, which was key to the effectiveness of the push and pull technologies described throughout this section.

A good starting point for this second phase is 2005, the year in which the US giant Ebay purchased the rising star of the European startup scene, Skype. This changed the laws governing Skype from the EU (Luxembourg) to the US. This purchase took place the year after the US Court of Appeals approved the settlement the Department of Justice was seeking with Microsoft, thus closing the investigation for its monopolistic behavior. This was the last big antitrust investigation within the tech sector until recent times (Khan, 2017). Six years later, in June 2011, while Skype's private

investors were negotiating its acquisition by Microsoft, Skype became a key component within the NSA's surveillance program, PRISM. By 2011, Skype was estimated to have 0.7 billion users, giving the NSA access to almost half of the 2 billion internet users worldwide (Statista, 2022). In October of 2011, Skype's acquisition by Microsoft was made public, the product was integrated into Microsoft, replacing the back-end of Windows Live Messenger, increasing Skype's reach, and with it, that of the NSA.

The year 2005 was also the year Yahoo acquired the photo-sharing platform Flickr and Google acquired the Android operating system. By controlling the Android operating system, Google secured a key gateway for the promotion and mass distribution of its growing suite of apps, like Gmail, Chrome, and others, which often came pre-installed on Android devices. Later, in 2019, once the Android operating system and its bundled apps were global market leaders, Google would comply with a US government order and revoke the Chinese company Huawei's Android license, undermining Huawei's prospect for global growth (Williams, 2019).

After acquiring Android in 2005, in 2006 Google acquired video sharing platform YouTube, which became central to the sharing of information during the so called Arab Spring (O'Donnel, 2011). In October 2007, Microsoft purchased 1.6% of Facebook, unleashing $240 million for the development of the nascent company (CNN, 2007). Just 3 years after the settlement of antitrust investigations, and 1 month after purchasing a part of Facebook, Microsoft became the first major company to join the NSA's PRISM surveillance program.

The processes of market consolidation and surveillance are intertwined in two ways. On the one hand, consolidation reassured agencies like the NSA that the key information being shared across the globe by its targets would most likely be recorded by a company that was subject to US jurisdiction and pressure. On the other hand, consolidation meant that the NSA would have fewer companies with which to negotiate access to such data. This intertwinement does not require the NSA or other US agencies to have supported or facilitated the process of market consolidation. However, without such consolidation, it is unlikely that the program would have been able to achieve the breadth it effectively did. According to internal slides released by Snowden, the massive surveillance program enacted through PRISM was costing the US government just $20 million a year (Washington Post, 2013). In his book, "Permanent Record" (2019), Snowden states: "so much of the infrastructure of the Internet is under US control that over 90 percent of the world's Internet traffic passes through technologies developed, owned, and/or operated by the American government and American businesses..."

If in Phase 1 the US representatives were presenting the internet as Global Information Infrastructure, the slides released by Snowden outline how in this second phase the Department of Defense does not see a post-nation-state infrastructure, but rather how the entire world was sitting on top of US infrastructure. Or, to use the phrasing from one of the released slides, the "U.S. as World's Telecommunications Backbone" (Washington Post, 2013).

At this point it is important to acknowledge that the US government is not alone in the deployment of surveillance techniques through the internet. China, Russia, and a broad range of other state and non-state actors also leverage the internet to *pull* information (Inkster, 2016; Perlroth, 2021). What is specific to the US is, first, the breadth of control its multinational companies hold over critical infrastructure globally; and second, that this consolidation was exploited by the US government to forward a narrow nationalistic agenda, in contradiction with the libertarian narrative the US leaders originally endorsed and promoted as a guiding principle for other countries to enable and support the development of internet infrastructure within their territories. The gap between the US' original narrative throughout phase 1 and its actions in phase 2 is particularly sizable.

This second phase is characterized by the US making an effort to "extend sovereign access to, and control of, data beyond national borders" (Taylor, 2020) p. 3). To effectively achieve such extraterritorial sovereignty, it first needed to penetrate into foreign territory. For its data collection, the NSA's PRISM program relied heavily on consumer-facing US multinational corporations, including Microsoft, Google, and Facebook (Washington Post, 2013). However, it also benefited from access to a much broader network of business-to-business companies operating infrastructure, mostly unknown to the public. As stated by Snowden, "It's not just the Internet's infrastructure that I'm defining as fundamentally American—it's the computer software (Microsoft, Google, Oracle) and hardware (HP, Apple, Dell), too. It's everything from the chips (Intel, Qualcomm), to the routers and modems (Cisco, Juniper), to the Web services and platforms that provide email and social networking and cloud storage (Google, Facebook, and the most structurally important but invisible Amazon, which provides cloud services to the US government along with half the Internet)" (Snowden, 2019 p.128).

The second aspect of this rehashing of the internet as a tool for information warfare involved not *pulling information from* the networks, but *pushing it through the networks*. At the height of the so called war on terror, the US developed the digital versions of the Cold War's Voice of Americ*a*: socio-technical systems designed to ensure information could penetrate into—and be distributed throughout—the territory of other states.

To push information the US government leveraged a wide range of actors and strategies: from its connections with key multinational companies, to funding software development through USAID, to the funding of advocacy groups that (knowingly or not) would forward the Department of State's agenda against the attempts by adversary governments to control the flows of information (see Figure 1).

Within this phase, the US government began developing projects like Tor (2002), the browser that helps people circumvent blockages of websites enacted by the local internet service providers (ISP). Some years later, in 2012, Radio Free Asia, launched the Open Technology Fund (OTF), which would finance the development of technology aimed at facilitating the circumvention of local attempts to exercise sovereignty. For example, among the several dozen projects on the OTF website is *oLink*. OLink is described as "a firewall circumvention open-source tool set [which] enables content providers from a free country like the US to target their audience in China." (OTF | OLink, 2022). The oLink system mirrors the content that is being blocked at the domain level (i.e., an ISP blocking the URL of a website) hosting a copy of it within "a platform such as github.com that the adversary cannot afford to block" (sic). That is, the oLink strategy consists in mirroring the banned content onto a platform that is both i) equated to critical infrastructure in the sense that it will not be taken down in an attempt to control information flows *and* ii) is a US multinational corporation, and would therefore most likely not interfere with such mirroring, at least not proactively. Like with the *pull powers*, the process of consolidation was central to the effectiveness of push powers. It must be noted that Microsoft purchased GitHub in 2018, thus cementing the US government's jurisdiction over it.

In 2006, the first UN Internet Governance Forum (IGF) meeting was held. Among the key grievances it was expected to address was the US government's control over ICANN (UN, 2005). The concerns regarding the ways in which the US was exercising—and could exercise—its power over critical components of the internet infrastructure would become a central feature of the last part of Phase 2.

This last part of phase 2 found the US handling the fallout associated with Snowden's revelations, which documented the breadth of *data pull* powers being exercised by the Department of Defense. The public outcry allowed world leaders to more decisively demand the *Global* Information

Infrastructure be operated as such, fueling an agenda for the formalization and institutionalization of global internet governance mechanisms. This redistribution of power would be at the expense of what had been revealed to be an invisible mesh of US' institutions and corporations, operating arbitrarily to forward narrow US geopolitical and commercial interests (Figure 1).

The Post-Snowden Fallout

To get a sense of the depth of the fallout, in 2014, weeks after the revelations, Brazil's president Dilma Rouseff stated before the UN: "Without respect for [a nation's] sovereignty, there is no basis for proper relations among nations." (Clark, 2013) As an immediate reaction to the revelations, Brazil called for the NetMundial conference. Fadi Chehadé, CEO of ICANN stated, "the trust in the global Internet has been punctured, and now it's time to restore this trust through leadership and institutions that can make that happen" (Clark, 2013). Two years later ICANN would be released from the oversight of the US Department of Commerce. A grievance dating as far back as 2005 (UN, 2005) was finally resolved.

The US' fallout can also be appreciated through changes to the physical infrastructure Snowden had mentioned was crucial to the operations of intelligence agencies. This includes Brazil's decision to finally begin the construction of a fiber optic cable that would allow South America to exchange traffic with the EU without having to pass through the US. Being able to circumvent the US in its exchanges with the EU became a matter of security after the Snowden revelations, according to the chief of Brazil's state run telecom company at the time (Boadle, 2015).

In the EU, the Snowden revelations triggered legal challenges to the storage of data from EU citizens in the US, a practice most US platforms engage in. The argument was that US corporations were in no position to guarantee that such data would not be arbitrarily surveilled by the US government. In 2015, the EU courts adopted such a position and struck down the legal instrument upon which data from EU citizens was being transferred to the US. The consequences of this fallout continue to this day: in 2021 EU courts also struck down its successor, Privacy Shield (ECJ, 2020). These decisions create uncertainty and thus strong incentives for companies to localize data by underlining that alternative arrangements could become subject to recurrent judicial scrutiny. In May 2021, Microsoft announced "we will not need to move your data outside the EU" (Smith, 2021).

End of a Phase: Trump Victory and a New Approach: Isolation and Re-Networking

In November 2016, Trump was elected President. His electoral platform was characterized as a reaction to the negative consequences of the process of globalization the United States had championed since the 1980s (Castells, 2018). The internet, and the networked systems of information that were central to the process of globalization, would thus become a key concern for his Administration. Phase 3 is characterized by the US government's attempt to reorganize the network topography to ensure it will protect and forward US interests into the future.

By the end of Phase 2, in 2016, over 43% of the world's human population was online.

Phase 3: Blockages, Lock-Outs, and Network (Re)Alignments

Congressman Gaetz, Rep. of Florida (R): *Do any of the rest of you take a different view? That is to say that your companies don't embrace American values. It's great to see that none of you do. Mr. Pichai, I'm*

worried about Google's market power, how it concentrates that power, and then ultimately how it wields it (...) My question, Mr. Pichai is, did you weigh the input from your employees when making the decision to abandon [Project Maven] with the United States military?

Mr. Pichai (CEO of Google): *Congressmen thanks for your concern. As I said earlier, we are deeply committed to supporting the military and the US government*

- Excerpts from the transcript ofa Congressional Hearing, Rev (2020)

"We are building a coalition of nations to advocate for and invest in trusted 5G technology and to better secure our supply chains""

- Statement by President Joe Biden on Cybersecurity Awareness Month, 2021

If phase 2 was characterized by the US government allowing US companies to centralize the internet and the Departments of the US government relying on such centralized systems to both *pull* and *push* data, this third phase incorporates a new phenomenon: cutting the access of adversaries to critical internet infrastructure through blockages or digital lock-outs. This is a distinct tool in the hands of the Department of the Treasury (see Figure 1) and has the particularity of seemingly compromising the ability of other Departments to exercise the pull and push powers described in the previous section. Far from being resolved, this contradiction is what might explain an apparent lack of consistency or a seemingly erratic approach to the of this *cutting* power.

In this phase, the US is no longer *just* seeking to push and pull information over the internet and *into or from* foreign territories, but threatening to leave countries *out* of critical spaces of the internet. The US government is transforming its jurisdiction over critical infrastructure into gatekeeping power over access to platforms upon which key sectors of government and private companies have come to depend upon. To understand this shift, we need to acknowledge two key and somewhat intertwined underlying processes:

(i) The relative decrease of the US user base as a proportion of the global internet user base;
(ii) The US' failure to assert its unilateral control over the internet or achieve its desired outcomes in the existing forums.

The combination of these factors might explain the US government's interest in accelerating a process typically discussed as fragmentation, to ensure it can dictate the terms of the re-networking process that can be expected to ensue.

The Decreasing Relevance of the US User Base

The challenge posed by this phenomenon is two-fold: On the one hand governments from across the world have reasons to see the US government's attempts to exercise extraterritorial sovereignty as less legitimate and more problematic the more their own populations depend on it, and the smaller the number of US citizens relying on it becomes as a proportion of the whole. On the other hand, US multinational corporations serving a global market are starting to see that the US is becoming a relatively small market, and one that, with its political and legal requirements, is capable of jeopardizing their access to a lucrative global market.

In terms of the objective metrics, by 2008 China already had surpassed the US in its absolute number of internet users, and by 2014 so had India. But perhaps more relevant to the global internet governance challenges, whereas until 1997 the US had been the home to over 50% of all internet

users, by 2021 its relevance had been watered down to a mere 7.5%.[2] A similar decline has also been documented in the US' share of autonomous system numbers (ASN), which are used to identify each individual network that is part of the network of networks that we call the internet: Whereas 56% of all ASNs were located in the US in 1997, by 2018 this figure had already dropped to 31%. This means that the US' physical footprint is also diminishing in relative terms (Winsek, 2019).[3] These shifts certainly underline the challenges the US begins to face as it continues to play what many now see as an outsized role in internet regulation and governance fora.

Acknowledging the unease of governments across the world, US multinational companies themselves are beginning to express discomfort towards the expectations US government officials set upon them. The Republican representative whose quote is included at the beginning of this section asking Google's CEO to comment on his company's allegiance to the US government and its military, is the reaction to this process of *de-americanization*. The US government seems increasingly concerned that its own homegrown companies often are detached from projects linked to US national goals (e.g., Google not bidding to provide hosting for the Pentagon (BBC, 2018) or pulling out of a joint project with the military (Statt, 2018)). In short, companies are still worried about being perceived as "instruments of government" and seemingly less willing to cooperate with the US government. The reaction to this corporate shift is perhaps best synthesized by President Trump underlining that TikTok's US business had to be sold to "a very American company"(CBS News, 2020). The message was clear, in the (commercial) war with China, and the broader procedure of re-networking, the spoils would be awarded to the loyal.

The US' Failure to Assert Unilateral Control Over the Internet or Achieve its Desired Outcomes in the Existing Forums

If we adopt a realist theoretical lens, multinational corporations and governments can be said to be in a constant exchange: Corporations are expected to create jobs and provide goods to the local population, whilst the government is expected to correspond by securing the conditions for them to operate profitably, which includes securing favorable conditions for their expansion into other countries.

Perhaps a key turning point was the decision of newly elected President, Donald Trump, to pull out of the Trans-Pacific Partnership (TPP) the Obama administration had been working on as a way to contain the growth of China and secure markets for US companies in the pacific (Naughton et al., 2015). Perhaps more relevant to the issues at stake, the TPP was "the first trade agreement to include a binding commitment on free cross-border data flows, a ban on data localization policies, a ban on source code transfer requirements, rules on encryption key requests, and rules on electronic authentication" (Azmeh et al., 2020). In an astonishing turn of events, in 2021 China began bidding to join the TPP and in 2022 China plans to see the entry into force of a separate but similarly ambitious regional trade deal (Shaw, 2021).

This pull out from the TPP by the US was followed by a World Trade Organization meeting in 2017, in which the US government failed to achieve what its tech corporations saw as the preferred outcome in terms of digital trade: the broadening of the concept of digital services (as opposed to digital goods) in a way that would have spared companies from having to comply with the regulatory regimes designed by each country, including data localization policies and its associated operational costs (Azmeh et al., 2020). And "states who are dissatisfied with existing multilateral institutions might create new multilateral forums with new rules, practices, or membership"(Azmeh et al., 2020, p.4).

The Secessionist Agenda

It is in this context that the US is creating a new forum where it can dictate the conditions for entry. This is, ultimately, what Trump's Secretary of State, Mike Pompeo, was promoting under the banner of a *Clean Network*. (US Department of State, 2020). In other words, if China had built a firewall around itself throughout the 1990s (Flew, 2022), now that it was seeking to move beyond its walls and operate globally, the US seemed determined to build a wall around China by calling on its partners to exclude Chinese vendors from all the layers of the internet stack. This is a radical departure from Al Gore's global information infrastructure, "on which all people can travel."

Although Pompeo is out of office, the secessionist agenda continues. In November of 2021, a draft document entitled "The Alliance for the Future of the Internet" was leaked. The draft, shepherded by the State Department, underlines that the goal of the alliance is "to advance democratic values and the rule of law by offering the benefits of an open Internet for those who adhere to basic principles and protections, while declining those benefits to non-adherent nations" (Politico, 2021). This language echoes Pompeo's *Clean Network*. While the final text, released in April 2022, eliminated that section, the goal of coordinating the exclusion of China seemed to remain (U.S. Department of State, 2022).

These continuities in policy despite a change in the ruling party suggest that carving out a portion of the internet for the US has become state policy. In August 2022, Biden signed the Chips and Science act, which includes a clawback provision aimed at stopping beneficiary companies from engaging in any form of "joint research or technology licensing effort" with China (White House, 2022). At the time of writing, on October 2022, this was further reinforced with export controls announced by the Department of Commerce that extended restrictions beyond companies and on "U.S. persons to support the development, or production" of chips in China (US Department of Commerce, 2022), which is designed to further undermine China's technological industry.

The state policy nature of this agenda also becomes apparent by observing the *whole-of-government* approach that is taking place. The head of the Department of the Treasury, Janet Yellen, even coined a term to characterize the agenda: *friend-shoring*. (Foroohar, 2022). The goal is to segregate and fragment the global economy—and more importantly the internet—into smaller blocks so that the US can claim one for itself.

But how can such splintering be achieved in a system that is so deeply interconnected? The US government has been relying on the Department of the Treasury to execute targeted exclusions that are slowly carving the network into shape. Blockages and digital lock-outs that operate as a signaling mechanism to other governments and companies as to where the fault lines lie.

In 2019, GitHub stopped Iranians from accessing its services. This lock-out, implemented only months after Microsoft purchased the company (Warren, 2018), lasted approximately 2 years. On October 7, and only months after GitHub announced it was locking Iranians out of their accounts, Adobe announced that it would lock Venezuelans out of their accounts (Lee, 2019a). This time, however, the company was granted a special license before the lock-out materialized (Lee, 2019b).

The 2021 report from the Treasury's Office of Foreign Assets Control (OFAC) seemed to acknowledge a lack of clarity in how sanctions were being communicated and deployed, and released a framework aimed at "modernizing" the use of sanctions (U.S. Department of the Treasury, 2021). The framework sets out a 5-point checklist for the deployment of sanctions, which GitHub's digital lock-out seems to fail to comply with on all accounts except for the reversibility. Understanding the lock-out of Iranians as part of a broader procedure through which government agencies signal to third parties, refine tools and work towards the renetworking of the internet becomes a more plausible explanation.

The OFAC also acknowledged that, as the US market becomes less relevant for the tech sector, key multinational companies are starting to be more wary of the ways in which the US policies undercut their ability to close concrete business deals abroad (U.S. Department of the Treasury, 2021, p. 2).

The process of renetworking is indeed triggering exits from the US jurisdiction. An example of this dynamic is RISC-V, an open standard instruction set architecture, which a lot of chips increasingly depend upon, including those from major providers such as Intel. Although the project was launched and is led by the University of California, Berkeley, in November 2019 they moved their legal headquarters to Switzerland, citing concerns from members regarding potential US trade curbs and "possible geopolitical disruption"(Nellis & Alper, 2019). A second example is the Eclipse Foundation, which stewards a major open software development community. In May 2020 the Foundation announced it had moved its legal domicile from the US to the EU, stating that "Europeans want to operate under European law" (Speed, 2020).

Although exits are a constitutive element of the process of renetworking, as with any process of change, there is always a risk of applying too much pressure. This is most likely a regular debate between the agencies exercising push, pull, and cut powers. The imposition of sanctions on Russia by the US, for example, operated as a focal point for the concerns of India, China, Brazil, South Africa and others who recognized in the tandem of sanctions the articulation of a threat to their own sovereignty (Adler, 2022). The growing concerns have led to calls for the rekindling of the non-aligned movement (Ortiz Freuler, 2020; Avila, 2020; Couldry & Mejias, 2021).

This process of re-networking is already taking place via decoupling of information systems in sensitive areas. Examples: The Chinese government ordering state offices to remove foreign hardware and software only months after the GitHub lockout against Iran (Coldeway, 2019a); Russia working towards the development of an intranet capable of dampening the effect of potential digital lock-outs (Coldeway, 2019b), and governments in the EU and beyond deploying variations of these techniques and technologies themselves (Tambiama, 2020).

Since the OFAC states it will strive to "adapt and modernize the underlying operational architecture by which sanctions are deployed", we can expect the key tensions described throughout this paper will continue to unfold over the years to come. We might come to see each sanction and lock-out as a stroke of the brush within the much broader process of renetworking of humankind's global information system. A process that involves testing the effectiveness and side effects of different tools, as well as somewhat invisible political negotiations between multinational corporations and different Departments of the US government.

Conclusion

The network topography evolves as the result of many intersecting processes, including technical, economic, and political decisions. In this paper, I have focused on the role played by political decisions, in particular those by the US government.

The first conclusion is conceptual: Internet fragmentation should not be conceptualized as a full *decoupling* of networks, but rather as a process of *re-networking* that shapes the topography of the internet in ways that modify the flow of data between different nodes. The US government is at the heart of this re-networking process, which is shaped by the push, pull, and cut powers being exercised by different Departments of the US Executive branch.

By observing the tensions between (and within) the US government, US multinational companies and the governments of other countries as a dynamic process, it is possible to identify the critical role the US government assigns to the proactive influence campaigns enacted by the State

Department through its push powers. By incorporating these push powers into Farrel and Newman's (2019) framework on weaponized interdependence, it is possible to expand it beyond the binary and static observation of coercion (cut) and surveillance (pull) elements. As such, this now tripartite and dynamic framework can better explain the unstable balance of powers that leads Treasury to use its cut powers through sanctions that seem to be retracted even before they are fully deployed (e.g., Adobe lockouts in Venezuela). Furthermore, this dynamic approach might not only allow us to project this framework beyond the period of US hegemony it was designed to analyze, but leverage it as a lens through which to interpret the US government's actions throughout this ongoing process of renetworking.

This leads to a second set of conclusions, which are political. The more recent actions by the US government aimed at *re-networking* reflect fears that the centralized machine upon which it has relied to exercise the pull, push, and cut powers might eventually fall into the hands of another government.

In this sense, Winseck (2019) seems to have correctly identified the many ways in which US control over key infrastructure has been receding, and how this might lead to changes to the current model of internet governance. Perhaps what he did not see (or could not see at the time of writing) was that the US government would be accelerating this shift instead of striving to protect an internet governance model that served a single and universal internet.

If the US government's concern is indeed that this centralized machine that enables the effective exercise of pull, push, and cut powers might end up controlled by another actor, perhaps the international community should actively support the implementation of Khan's (2017) agenda for the development and enforcement of antitrust rules against critical tech oligopolies within the US. In this way, Khan's argument regarding the incompatibility of oligopolies and democracy at a national level could be expanded to explain the shortcomings of our global internet governance system. Mirroring antitrust activity at a national level, at an international level the US could embrace a policy of *technological disarmament* that promotes decentralization and rules against the development of socio-technical systems that could enable effective pull, push, and cut powers by any actor globally.

The Unease is not Specific to the US

Governments across the world are increasingly uneasy about the existence of an information system that has become critical for their economies and political life but over which they have little leverage through the existing governance mechanisms. Countries with low income or population see these challenges exacerbated by a limited bargaining power, which is likely going to spur new processes of coalition building across the so called global south. Perhaps even the resurgence of a (digital) non-aligned movement.

Further research could focus on the past and analyze how pull, push, and cut powers might have been exercised by the colonial powers managing the infrastructures of the early 20th century, like the telegraph, and how these actions might have shaped our current understanding of internet governance. Research could also focus on ongoing processes and map the ways in which the different sectors that make up the multistakeholder system are taking steps to adapt to this changing scenario. For example, in the case of the private sector, the extent to which, like Chinese company ByteDance has separated Douyin (抖音) from TikTok to increase trust within the US (CNBC, 2019), the US multinational companies begin to split and spin out their companies into legally independent branches across the globe, each with a distinct identity and subject to the jurisdiction of a key country in each region. That is, mapping how US multinationals take steps to strengthen the

perception that (i) they will comply with the legal obligations set out by host countries; and (ii) are less likely to bend under the pressure of the US government.

Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

ORCID iD

Juan Ortiz Freuler https://orcid.org/0000-0001-8691-5786

Notes

1. Assuming 4.1 billion internet worldwide, 313 million of which are in the US
2. Assuming 4.1 billion internet worldwide, 313 million of which are in the US(Statista, 2021 and World Bank Databank)
3. According to Winseck (2019) this under-represents the true nature of the US decline, since "the number of ASNs in China is not well captured because they are hidden behind the country's "great firewall"" (p. 104)

References

Adler, D. (2022). *The west v Russia: Why the global south isn't taking sides*. The Guardian. https://www.theguardian.com/commentisfree/2022/mar/10/russia-ukraine-west-global-south-sanctions-war

Avila, R. (2020). Against digital colonialism. In *Platforming equality* (p. 13). Autonomy.

Azmeh, S., Foster, C., & Echavarri, J. (2020). The International Trade Regime and the Quest for Free Digital Trade. *International Studies Review*, *22*(3), 671–692. https://doi.org/10.1093/isr/viz033

BBC. (2018). *Google drops $10bn battle for Pentagon data contract*. BBC News. https://www.bbc.com/news/technology-45798153

Becker, C., Ten Oever, N., & Nanni, R. (2022). The standardisation of lawful interception technologies in the 3gpp. Interrogating 5g and surveillance amid Us-China competition. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4167105

Berners-Lee, T. (1998). *Frequently asked questions by the Press*. https://www.w3.org/People/Berners-Lee/FAQ.html

Boadle, A. (2015). *Brazil to boost internet speed through Europe*. Reuters. https://www.reuters.com/article/brazil-telebras-idINL1N11N12920150918

Bush, G. W. (2001). *September 11, 2001: Address to the nation on the terrorist attacks*. https://millercenter.org/the-presidency/presidential-speeches/september-11-2001-address-nation-terrorist-attacks

Castells, M. (2009). *Communication power*. Oxford University Press.

Castells, M. (2010). *The rise of the network society*. (2nd ed.) Wiley-Blackwell.

Castells, M. (2018). *Rupture: The crisis of liberal democracy*. Polity Press.

CBS News. (2020). *President Trump said he set a September deadline for TikTok to be sold to "a very American company," or it will be shut down in the U.S. And he wants the federal government to get a cut of the sale*. https://cbsn.ws/3goK7z6

Clark, L. (2013). *Brazil to try shielding itself from NSA with national secure e-mail*. Ars Technica. https://arstechnica.com/tech-policy/2013/10/brazil-to-try-shielding-itself-from-nsa-with-national-secure-e-mail/

Clinton, H. (2010). *Remarks on internet freedom*. U.S. Department of State.

CNBC. (2019). *TikTok owner moves to separate app from Chinese operations amid U.S. probe*. CNBC. https://www.cnbc.com/2019/11/27/tiktok-moves-to-separate-app-from-chinese-operations-amid-us-probe.html

CNN. (2007). *Microsoft strikes ad deal with Facebook*. CNN. https://money.cnn.com/2007/10/24/technology/msft_facebook/

Coldeway, D. (2019a). *China moves to ban foreign software and hardware from state offices*. TechCrunch. https://social.techcrunch.com/2019/12/09/china-moves-to-ban-foreign-software-and-hardware-from-state-offices/

Coldeway, D. (2019b). *Russia starts testing its own internal internet*. TechCrunch. https://social.techcrunch.com/2019/12/26/russia-starts-testing-its-own-internal-internet/

Couldry, N., & Mejias, U. A. (2021). The decolonial turn in data and technology research: What is at stake and where is it heading? Information. *Communication & Society*, 1–17. https://doi.org/10.1080/1369118X.2021.1986102

Cowhey, P. F., & Aronson, J. D. (2018). Digital trade and regulation in an age of disruption. In: *UCLA journal of international law and foreign affairs* (Vol. *29*). Springer.

DeNardis, L. (2014). *The global war for internet governance*. Yale University Press. https://doi.org/10.12987/yale/9780300181357.001.0001

Drake, W. (2000). Rise and decline of the international telecommunications regime. In *Regulating the global information society* (1st ed., p. 54). Routlege.

Drake, W. J., Cerf, V., & Kleinwächter, W. (2016). *Internet fragmentation: An overview (future of the internet initiative white paper* (p. 80). World Economic Forum.

ECJ. (2020). *The Court of Justice invalidates decision 2016/1250 on the adequacy of the protection provided by the EU-US data protection Shield*.

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

Flew, T. (2022). *Regulating platforms*. Wiley.

Foroohar, R. (2022). *It's time for a new Bretton Woods*. Financial Times. https://www.ft.com/content/b437fd60-7817-490e-b456-eb7ef1565f13

Gore, A. (1994). *VP remarks at the international Telecommunications union*. https://web.archive.org/web/20010528184855/https://clinton1.nara.gov/White_House/EOP/OVP/html/telunion.html

Hartley, J., Montgomery, L., & Siling Li, H. (2017). A new model for understanding global media and China: 'Knowledge clubs' and 'knowledge commons. *Global Media and China*, *2*(1), 8–27. https://doi.org/10.1177/2059436417705919

Hill, J. (2012). *Internet fragmentation: Highlighting the major technical, governance and diplomatic challenges*. Harvard Belfer Center for Science and International Affairs. https://www.belfercenter.org/sites/default/files/files/publication/internet_fragmentation_jonah_hill.pdf

Inkster, N. (2016). *China's cyber power*. Routledge; The International Institute for Strategic Studies.

Khan, L. M. (2017). Amazon's antitrust paradox. *Yale Law Journal*, *126*(3). https://www.yalelawjournal.org/note/amazons-antitrust-paradox

Lee, D. (2019a). *Adobe is cutting off users in Venezuela due to US sanctions*. The Verge. https://www.theverge.com/2019/10/7/20904030/adobe-venezuela-photoshop-behance-us-sanctions

Lee, D. (2019b). *Adobe restores service in Venezuela, adds three months for free as an apology*. The Verge. https://www.theverge.com/2019/10/28/20936214/adobe-venezuela-sanctions-us-executive-order

Naughton, B., Kroeber, A., de Jonquieres, G., & Webster, G. (2015). *What will the TPP mean for China?* Foreign Policy. https://foreignpolicy.com/2015/10/07/china-tpp-trans-pacific-partnership-obama-us-trade-xi/

Nellis, S., & Alper, A. (2019). *U.S.-based chip-tech group moving to Switzerland over trade curb fears*. Reuters. https://www.reuters.com/article/us-usa-china-semiconductors-insight-idUSKBN1XZ16L

O'Donnel. (2011). *New study quantifies use of social media in Arab Spring*. UW News. https://www.washington.edu/news/2011/09/12/new-study-quantifies-use-of-social-media-in-arab-spring/

Ortiz Freuler, J. (2020). *The case for a digital non-aligned movement*. OpenDemocracy. https://www.opendemocracy.net/en/oureconomy/case-digital-non-aligned-movement/

OTF oLink. (2022). https://web.archive.org/web/20220418061910/https://www.opentech.fund/results/supported-projects/olink/

Perlroth, N. (2021). *This is how they tell me the world ends: The cyberweapons arms race*. Bloomsbury Publishing.

Politico. (2021). The Alliance for the Future of the Internet. *https://www.politico.com/f/?id=0000017c-e71b-d8e1-a57c-efffa3810004*. Politico.

Shanghai Cooperation Organisation. (2008). *Agreement on cooperation in ensuring international information security between the member states of the Shanghai cooperation organization*.

Shaw, K. A. (2021). *China is racing ahead to lock in asian trade. Time to worry*. Barrons. https://www.barrons.com/articles/china-rcep-trade-deal-51638479544

Smith, B. (2021). *Answering europe's call: Storing and processing EU data in the EU*. EU Policy Blog. https://blogs.microsoft.com/eupolicy/2021/05/06/eu-data-boundary/

Snowden, E. (2019). *Permanent Record*. Pan Macmillan.

Speed, R. (2020). *Total Eclipse to depart: Open-source software foundation is hopping the pond to Europe*. https://www.theregister.com/2020/05/12/eclipse_moves_to_europe/

Statement by President Joe Biden on Cybersecurity Awareness Month. (2021). *The white House*. https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/01/statement-by-president-joe-biden-on-cybersecurity-awareness-month/

Statista. (2021). *Most internet users by country*. https://www.statista.com/statistics/262966/number-of-internet-users-in-selected-countries/

Statista. (2022). *Estimated Skype user numbers worldwide 2009-2024*. https://www.statista.com/statistics/820384/estimated-number-skype-users-worldwide/

Statt, N. (2018). *Google reportedly leaving project Maven military AI program after 2019*. The Verge. https://www.theverge.com/2018/6/1/17418406/google-maven-drone-imagery-ai-contract-expire

Tambiama, M. (2020). *Digital sovereignty for europe* (p. 12). European Parliamentary Research Service.

Taylor, R. D. (2020). Data localization": The internet in the balance. *Telecommunications Policy*, *44*(8), 102003. https://doi.org/10.1016/j.telpol.2020.102003

UN. (2005). *Report of the working group on internet governance*. https://www.wgig.org/docs/WGIGREPORT.pdf

US Department of Commerce. (2022). *Commerce implements new export controls on advanced computing and semiconductor manufacturing items to the people's Republic of China (PRC)*. https://www.bis.doc.gov/index.php/documents/about-bis/newsroom/press-releases/3158-2022-10-07-bis-press-release-advanced-computing-and-semiconductor-manufacturing-controls-final/file

US Department of Defense. (2003). *Information operations Roadmap*. https://nsarchive2.gwu.edu/NSAEBB/NSAEBB177/info_ops_roadmap.pdf

US Department of State. (2020). *The clean network*. United States Department of State.

U.S. Department of State. (2022). *Declaration for the Future of the Internet*. U.S. Department of State. https://www.state.gov/declaration-for-the-future-of-the-internet/

U.S. Department of the Treasury. (2021). *The treasury 2021 sanctions review* (p. 9). https://home.treasury.gov/system/files/136/Treasury-2021-sanctions-review.pdf

Warren, T. (2018). *Here's what GitHub developers really think about Microsoft's acquisition*. The Verge. https://www.theverge.com/2018/6/18/17474284/microsoft-github-acquisition-developer-reaction

Washington Post. (2013). *NSA slides explain the PRISM data-collection program*. http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/

White House. (2022). *Fact sheet: Chips and science act*. The White House. https://www.whitehouse.gov/briefing-room/statements-releases/2022/08/09/fact-sheet-chips-and-science-act-will-lower-costs-create-jobs-strengthen-supply-chains-and-counter-china/

Williams, A. (2019). *What google's huawei ban means for millions of android owners*. Wired. https://www.wired.co.uk/article/huawei-google-ban-uk-android

Winseck, D. (2019). Internet Infrastructure and the Persistent Myth of U.S. Hegemony. In B. Haggart, K. Henne, & N. Tusikov (Eds.), *Information, technology and control in a changing world: understanding power structures in the 21st century*. Springer International Publishing. https://doi.org/10.1007/978-3-030-14540-8

Zittrain, J. (2019). Three eras of digital governance. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3458435

Rev (2020). https://www.rev.com/transcript-editor/shared/_FX24Jlb75YkV0wn0tdgEzn7hr3YnKHiYFRaJHC36cpuN8-hRZCoC_eanIZkNRqAAoCUFtC5429mmv3rvjnTX3PpTLo?loadFrom=PastedDeeplink&ts=4121.04

Author biography

Juan Ortiz Freuler is an affiliate at the Berkman Klein Center for Internet and Society at Harvard University, a co-initiator for the non-aligned tech movement, and a PhD student and the Wallis Annenberg Fellow in Communication at the University of Southern California. His research interests include Internet governance, algorithmic governance, and the way in which geopolitics and public diplomacy might shape internet and other information infrastructures.