RBPI

Revista Brasileira de Política Internacional

ISSN 1983-3121

http://www.scielo.br/rbpi

Jaqueline Trevisan Pigatto[1]

[1]Universidade Estadual Paulista, Faculdade de Ciências e Letras, Araraquara, SP, Brazil (jaqueline.t.pigatto@unesp.br)

ORCID ID: orcid.org/0000-0003-0690-1064

Mark W. Datysgeld[2]

[2]Governance Primer, São Paulo, SP, Brazil (mark@governanceprimer.com)

ORCID ID: orcid.org/0000-0002-5531-2074

Laura Gabrieli Pereira da Silva[3]

[3]Universidade Estadual Paulista, Faculdade de Ciências e Letras, Araraquara, SP, Brazil (laura.gabrieli@unesp.br)

ORCID ID: orcid.org/0000-0002-0784-8990

Article

Internet governance is what global stakeholders make of it: a tripolar approach

DOI: http://dx.doi.org/10.1590/0034-7329202100211

Rev. Bras. Polít. Int., 64(2): e011, 2021

Abstract

This paper seeks to identify the configuration of Internet governance in late 2021, focused on the dispute over institutional representation and legitimacy in which major regional powers find themselves. The United States, the European Union, and China compose a tripolar arrangement, each advancing a distinct mode of governance with unique characteristics that we strive to analyze here.

Keywords: Internet governance; Digital sovereignty; Multistakeholder model; Regulation.

Received: May 31, 2021
Accepted: September 13, 2021

Introduction

With the increasing importance of the Internet in human interaction, the political aspects of our relations are directly affected by the evolution of the network. Communications is a field that has historically created regulatory challenges and brought about changes to transnational agreements, and the Internet is no exception to that trend. The operation of this network requires the commitment of diverse actors supporting its colossal structure, while respecting each other's roles and attributions. A significant part of these interactions happen inside a multistakeholder model (MSM) guided by rough consensus, with the general goal of preserving a single, open, and decentralized Internet.

In the MSM, representatives of national governments, the private sector and civil society, are all responsible for the formulation of the principles, rules and procedures for the usage and development of the Internet (Raymond and DeNardis 2015). Over time, tensions between these actors have resulted in disputes over the stewardship of specific aspects of the network, such as the right to control content, which has largely become a prerogative of the state; and control over the Domain Name System (DNS), which is operated by a private sector not-for-profit organization (Mueller 2002).

To understand the formation of this dynamic, it is important to consider that the core of the Internet was built with governmental resources by academics in partnership with the private sector. The US, UK, and France stand out as nations with an early investment in networking technologies, with much base research carried out by their academic institutions, as was the case of the efforts led by the Defense Advanced Research Projects Agency (DARPA) in North America. From the outset, private actors were the developers and manufacturers of the machines that allowed for connections to take place, and worked mostly in coordination with the networking community to enable the betterment of the technology (Hafner and Lyon 1998).

The admission that all of these actors are important to the Internet's adequate functioning resulted in a model that allows for the participation of the private sector in international policymaking in more direct ways, diverging from classic models studied by International Relations. Internet governance is a novel field that enables observations to be made on the power dynamics that play out between actors in an often-public manner, adding a valuable analysis layer to our understanding of current global challenges.

In the struggle to shape the norms impacting such a key technological resource, tensions between states and transnational companies have proven worthy of investigation over the years. This article proposes that three regional powers and the companies within their sphere of influence have emerged as significant influences on the broader Internet governance arrangement, with distinct modes of governance: the United States (US), the European Union (EU), and China. We understand, therefore, the existence of a tripolar system.

The concept of "polarity" is used in International Relations to describe the distribution of power among actors in the international system. When we propose a tripolar approach to the power relations observable in current Internet governance, we dialogue with methods used in recent analyses by authors such as John Mearsheimer, who posits that "The new multipolar world will feature three realist orders: a thin international order that facilitates cooperation, and two bounded orders – one dominated by China, the other by the United States" (Mearsheimer 2019).

Allowing for some generalization, the US can be said to use a democratic liberal and innovation-first approach that does not take matters such as privacy into great consideration. China takes advantage of its authoritarian regime to organize its tech-oriented companies in ways that are favorable to its interests, backed by a strong domestic market that strengthens national companies and forces the hand of international ones. The EU built its identity on top of a legalistic and (purportedly) humanitarian approach, with emphasis on individual privacy, pushing companies and other states towards a sometimes involuntary alignment with what have become effectively international norms, as was the case with the privacy-focused General Data Protection Regulation 2016/679 (GDPR).

Multiple implications to the power balance around Internet-related matters arise from this arrangement. These modes of governance coexist, feed on each other, and react to each other. While US companies have for a long time exerted a disproportionate global influence, due to their size and relative lack of regulation, in time China has fostered its own set of private actors that work together with the government to create substantial competition. Meanwhile, the EU has an intervening role that moderates and regulates in ways that affect the other actors, particularly in relation to the American continent.

General considerations

Theoretical framework

In Alexander Wendt's (1992) "Anarchy Is What States Make of It: The Social Construction of Power Politics", institutions are defined as structures that bring together identities and interests, which fulfill functions of socialization and participation in collective knowledge. In other words, it is with the help of spaces such as the UN's Internet Governance Forum (IGF), the Chinese World Internet Conference (WIC) or even the European Union (EU) as an entity, that actors gain greater understanding of their counterparts' positions on Internet-related matters. Therefore, we adopt Wendt's assertion that collective identities and structures are mutually constituted.

The EU is understood here as a bloc, that is, an Intergovernmental Organization which uses supranational powers of broad interest, incorporating government representatives and other relevant players (Mariano and Mariano 2002). In this study, the EU differs from other institutions in that it is analyzed as an actor, a cohesive whole. Meanwhile, China and the US are understood more objectively in their state forms.

Furthermore, the case of China is notable because of the strong linkage between its private sector and the state, which allows the government to exert profound influence in a company's decision-making process. When businesses grow large enough to challenge the state, they face strong opposition and need to adapt or outright change their plans, as has happened in the recent cases of Alibaba, Didi and Tencent (Tan 2021).

In relation to the Internet itself, it can be said to have evolved from a project by the United States Department of Defense that was basically a communication platform for academics in the 1960s and 1970s, to being today one of the driving forces of political action and social interaction in more than half of the world (Statista 2021). This rapid change produced distinct political consequences that are worthy of targeted study, resulting in the creation of the Internet governance field.

As a regime, Internet governance has features that are somewhat unique, seeing as nation states may at times not be the main deciders in policies that carry global implications. However, its base structure can still be understood to dialogue with Krasner's concept of International Regime[1], considering the following definition by the World Summit on the Information Society (WSIS):

> A working definition of Internet governance is 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 programmes that shape the evolution and use of the Internet (World Summit on Information Society 2005).

In the MSM, it is accepted that states, the private sector, civil society, and the technical community/academia all sit at the same table, theoretically maintaining equal footing. This perspective is often presented in opposition to the "multilateral" approach in which states play the central role while the remaining actors play a supporting role, a model notably defended by China and Russia (Raustiala 2017).

A systemic solution by state actors emerged starting from 2006, after the WSIS, with the assembly of the Internet Governance Forum (IGF), an ecosystem focused on non-binding public debates and making use of United Nations (UN) methodologies. The IGF fundamentally acts as a measure to limit the possibility of non-state actors to engage in decisions related to content, or which could potentially lead to changes in public policy (Datysgeld 2018).

The division of responsibilities between actors varies and overlaps. Governments manage natural and environmental resources, such as land in which fiber optics cables are laid and frequency spectrum allocation; they also generate national and regional laws that often affect the content portion of the Internet. The private sector is responsible for much of the development and implementation of the machine infrastructure (such as antennas and routers), as well as the provisioning of Internet services and platforms, such as hosting, domain names, and social networks. Academia and the broader scientific community have an intervening role in which they work in the research of new technologies, help steer policy decisions, and do tailored projects to facilitate the goals of other actors. Civil society often plays a watchdog role in its scrutiny of the decisions being carried out by others, at times being the bridge that communicates these events to broader non-technical audiences (Kurbalija 2016).

At some point this actor balance might have existed, but in the Internet governance arrangement as it currently stands, some states hold a tight grip over companies and citizens online, using measures such as regulation, access blocking, and policing to make sure the network serves specific purposes that are desirable to them. On the other hand, some companies assume a state-like institutional role of controlling what is permissible or not, mediating interactions at scale. Over time, companies have assumed several functions that previously belonged to the state, such as control over citizen data, cartography, and even serving as direct official communication

[1] For Krasner (1982, 186), international regimes are "[...] sets of implicit or explicit principles, norms, rules, and decision-making procedures around which actors' expectations converge in a given area of international relations".

channels between government officials and their citizens, resulting in an accumulation of functional power (Mariano et al. 2018).

From a critical perspective, the current configuration of the MSM can be understood as unbalanced in at least two ways. From one standpoint, big players from the private sector establish their own modes of governance by means of complex terms of service, potentially evading national regulations and undermining state power; from another standpoint, governments do not feel compelled to comply with expectations such as the protection of human rights and other important social questions, and the other stakeholders lack the power to encourage or coerce them into doing so (Buxton 2019). Although diversity in participation was at the core of the arrangement, in practice, the inclusion or exclusion of the "interested parties", as well as their claims to legitimacy, change according to the situation (Hofmann 2016).

The increasing use of "digital sovereignty" as an argument in policies and political discourse by state actors is a symptom of the entanglement explored in this article. When critical matters such as elections and other major public processes began receiving significant interference from the Internet, new perceptions emerged. Sovereignty, seen in this manner, contradicts previous popular arguments such as that of "cybernetic exceptionalism", the Internet as a catalyst of unalienable freedom, and even the logic of the MSM itself (Pohle and Thiel 2020; Couture and Toupin 2019).

The vision of the Internet as an enabler of personal liberty was the mainstream one during its earlier years, but that premise in itself betrays the tension between the operation of the network and territorial sovereignty, with the Internet holding the potential to undermine the regulatory power of the state with the global nature of its operation. The pursuit of dominance of the digital space by states is a logical progression of the nature of the state itself (Lessig 2006).

Sassen (1997) attributed great impact not to the Internet itself, but to the characteristics it could acquire over time, in the development of its software layer and the increase in its commercialization. Previous phenomena of a political and social nature had already been presenting a threat to the premise of sovereignty as an exclusive feature of the state, such as an increase in the legitimacy of the actions of non-governmental actors and international institutions, and the Internet could potentially accompany that shift.

Historical aspects

In spite of initially having more horizontal power relations and semi-open decision-making processes, conflicts arose within the epistemological community in relation to the US-centric nature of the Internet project, with attempts being made over the years to reduce this dependence. Institutional conflicts around the maintenance of technical aspects of the network still remain relevant today.

Some functions once exercised or connected to government bodies were eventually transferred to non-governmental organizations and companies, fostering decentralization and autonomy of local points of control (Abbate 1999). The commercial opening and subsequent end of the military operation of the network allowed for new uses to be derived from it, and the progressive cheapening of user-friendly devices, from microcomputers to smartphones, resulted in substantial changes that generated demand not only for increased Internet availability, but also a constant rethinking of its underlying protocols, including significant changes to the foundational TCP/IP that are ongoing to this day (Holder 2018).

The Internet Corporation for Assigned Names and Numbers (ICANN) was established in 1998 with the intention of regulating the names (domain names) and numbers (IP numbers) space, promoting competition and allowing for multiple independent actors to engage in the commerce and operation of these resources. Its community is organized around the MSM, with decisions being steered by the community with the support of the ICANN organization.

ICANN initially had deep ties with the US Department of Commerce, but those were progressively loosened with the passing of time. Even before privatization, US government intervention did not go beyond financing and oversight functions, with no public interference in the decision-making process being registered. This was enabled by a general trend of states not paying significant attention to the emerging Internet phenomenon, placing lesser importance on its potential impacts. This can be demonstrated by the lack of early presence of governments in the ICANN community, even though a body for their participation already existed. State presence would only intensify well into the 2000s (Datysgeld 2018).

The "way of networking" created in the US was quickly exported worldwide, with products and services coming pre-packaged with a self-regulation model. This is largely derived from Section 230 of the Communications Decency Act (The United States Congress 1996), in which companies are not held responsible for content generated by third parties. Besides, a "Good Samaritan" provision allowed platforms to moderate content without being held accountable for it.

The 2010s saw both a reduction of the US's role in matters of Internet governance and an increase in relevance from the EU in that area. The 2013 Snowden revelations can be seen as an inflection point in which the formation of the tripolar arrangement posited by this article started to intensify. This was further exacerbated by the election of Donald Trump in 2016, among an international intervention controversy relating to the potential undue influence of social media in his election, facilitated by Cambridge Analytica (Lewis and Helder 2018).

Starting from 2013, the controversial international scenario allowed for Brazil to briefly become a protagonist in the search for a new governance model, which culminated in the multistakeholder event NETMundial (2014), held in São Paulo. During the same general movement, a national law that partially regulated the use of the Internet in the country was also approved: the Brazilian Civil Rights Framework for the Internet ("Marco Civil da Internet"), the first such legislation in the world. The law stands out in relation to issues of content moderation and intermediary liability. It emphasized the protection of personal data and net neutrality, both agendas still in debate around the world today.

NETMundial had substantial plans to reform the way in which the interactions between Internet governance actors were to take place, and generated much debate at the time. This event was another consequence of the Snowden revelations, as ICANN faced intensified pressure in relation to the US's oversight of its functions. The teams of then Brazilian President Dilma Rousseff and then ICANN CEO Fadi Chehadé co-produced a statement of principles which highlighted the roles of stakeholders thus:

> Internet governance should be built on democratic, multistakeholder processes, ensuring the meaningful and accountable participation of all stakeholders, including governments, the private sector, civil society, the technical community, the academic community and users. The respective roles and responsibilities of stakeholders should be interpreted in a flexible manner with reference to the issue under discussion (Netmundial 2014).

This aimed to be a sort of update to the WSIS, defining that non-state actors should have parity with state actors. According to Kleinwächter (2014), NETMundial created the possibility of a third way, conciliating frustrations with the behavior of state actors and the need to maintain a free, open, and human rights-oriented Internet governance model. The event came to the conclusion that a hybrid approach to the multilateral and multistakeholder models was possible, and outlined plans to move that idea forward. However, a severe internal instability in Brazil followed, culminating in Rousseff's removal from power. The the subject gradually deteriorated and lost priority, with the EU stepping up to fill the void left by Brazil and capitalizing on the opportunity to present new approaches to the global Internet community.

Situation as of 2021

When looking into the current context, the meaning of the previously outlined concept of "digital sovereignty" has become twofold, with somewhat distinct definitions. In both cases, there are considerations over content control and less reliance on foreign resources. Digital sovereignty advances steadily in both vectors, varying mostly in terms of intensity. For analysis purposes, the EU and China stand out as good examples of this.

China upholds policies such as that of its national firewall, which selectively blocks certain content deemed inappropriate by the government. Undesirable actions may be punished with police action. Thus, Chinese digital sovereignty emphasizes citizen control. On the other hand, Europe has been arguing for a more contained type of digital sovereignty, in alignment with its privacy-oriented approach, putting emphasis on control over software and hardware under operation in its territory. The difference, therefore, can be traced to the type of regime and the identity each state has attempted to project – we explore these strategies in sections further on.

The European interpretation speaks directly against the concentration of data among select actors from the US, resulting in the EU seeking more autonomy and consequent alternative solutions. This doesn't mean, however, that only China contemplates the possibility of a control-centric approach; governments from around the world progressively give more consideration to how much they should focus policies on either approach, while at the same time getting more involved in oversight and regulation of the network (Chapelle and Porciuncula 2021).

The MSM seems to be losing momentum in face of demands posed by its stakeholders, particularly relating to its lack of capability to solve non-technical matters. The MSM is rather effective in promoting protocols and standards, but political concerns have a more difficult time being dealt with. Meanwhile, the private sector is ceasing to exercise absolute self-regulation in order to be regulated and to regulate together with the state, distancing themselves from the burden of making socially complex decisions.

Although the consequences of extra-territorial laws have been a part of Internet governance debates for a long time, a gap remains between the objectives and values of global governance in relation to national and extra-territorial regulatory effects. The "myth" of cyberspace as a neutral agent of globalization and unification is fading away, and subjects such as the protection of personal data (Torre and Brown 2020) and antitrust actions (Edelman 2021) are becoming relevant even in the liberal environment of the US.

Facebook's Oversight Board is a relevant part of this discussion, being one of the first cases, and probably the most notable, of decision outsourcing by a big tech company. It fundamentally operates as an independent institution, reviewing sensitive cases of content moderation taking place in the platform and then issuing global decisions. The Board has a diverse composition that seeks to reflect the different global stakeholders, similar to the MSM. We explore this organism better further on.

Keeping track of how this type of oversight mechanism will dialogue with other components of the global governance environment and contribute towards (or destabilize) existing arrangements is relevant to future studies. If successful in the mediation of the platform's powers with those of state legislation, such governance tools could serve as a model for digital platforms in general (Polido 2019). It could, conversely, also prove the ineffectiveness of the approach.

Given these considerations, Internet governance proves to still be a field of institutional experimentation. New practices have been consistently initiated by these three regional powers and stand out in the current contours of the ecosystem. Initiatives such as New IP from China; GAIA-X and the Digital Services Act (DSA) from the EU; the Clean Network and Clarifying the Lawful Overseas Use of Data Act (CLOUD Act) of the US; as well as several others, surround the discussion around technical aspects of the Internet and the definition of public-private capabilities in terms of regulation (Dekker and Okano-Heijmans 2020). These disputes will likely have a significant impact on the manner in which the network is structured over the coming years.

A Tripolar Approach

USA

Rooted in the liberal tradition, the originators of the network have benefited from being the physical and abstract center of the Internet. Its companies were able to expand largely unimpeded for a significant amount of time, innovating in equipment and code, until (somewhat ironically) most of their hardware production was outsourced to Asia in the pursuit of higher profit margins (Rapoza 2019). This eventually led to a loss of competitive edge in the hardware front, with software development remaining the key strategy to be pursued.

A changing political environment combined with a rude awakening in regard to the country's lack of dominance over 5G technology, as well as microchip production, recently put the US in a position of attempting to reestablish some control over the agenda. The state and national companies need to rethink positions and prove that they can offer an environment that is more in tune with contemporary demands for accountability, as well as developing cybersecurity solutions that do not threaten its allies.

Even with these considerations, the network remains fairly rooted in US territory, due to its concentration of physical infrastructure and services. Many popular platforms also have their canonical servers located there, and much of the world's data eventually flows in its direction regardless of data localization laws (Blum 2012). This is precisely what enabled global espionage programs to be carried out by the state, a fact that, once discovered, imploded any perception of the viability of maintaining the US as the central Internet actor. As previously mentioned, this lack of trust led to what came to be known as the IANA Stewardship Transition.

In simplified terms, the IANA functions control the "names and numbers" portion of the Internet's core, and ICANN was granted stewardship over them in 1999 under contract from the National Telecommunications and Information Administration (NTIA). While promises were made of a progressive transition of control, these were delayed several times, and only after much pressure, in 2016, ties were formally severed with the government, although ICANN itself remained a California-based not-for-profit company (Datysgeld 2018).

It was not only at the institutional level that the US faced significant pressure. In recent years, internal conflicts between the state and its major national tech companies have been escalating. A previous sense of co-dependence between these actors made it so that only on occasion did they meddle in each other's affairs, and the aforementioned Section 230 served as a cornerstone of private regulation by the private sector. However, the mobilization of antitrust actions against several tech companies and an increased demand for responsibility are showing consequences.

Facebook's Oversight Board started to act in October 2020, receiving more than 20.000 cases for evaluation since October of the same year. Cases that have a global reach, that are important for public discourse, or that raise relevant questions about Facebook's policies, are prioritized.

Among the first selected cases were photos of the refugee crisis in Syria, photos that violated Facebook's policy for nudity but were actually part of a breast cancer awareness campaign, and a disinformation video about the COVID-19 pandemic (Oversight Board 2021a).

The most notorious reviewed case so far relates to the suspension of former US president Donald Trump, days after the invasion of the US's Capitol building by alleged supporters. Facebook's Oversight Board eventually endorsed the suspension, asking however that the terms of the suspension be changed from the original "for indefinite time" to a finite term (Oversight Board 2021b). The company responded by determining his suspension to be of 2 years. The decision was later criticized for "giving back" the final word to Facebook, with the company being the one to effectively make the decision, with the oversight mechanism acting as more of a ratifier to the process (Clegg 2021).

The US's position in the international system is still one of superiority, with an affluent internal market and the capacity to shape the markets of others with the use of several instruments, such as their stock market, the dollar currency, military presence, and so on. However, its post-Cold War dominance is giving way to a reality in which the state needs to evaluate its position, and think up new strategies to maintain said superiority.

The coming years will offer plenty of opportunities for the US to attempt to find its footing, but the "early bird advantage" seems to have been lost, as the other regional powers from the tripolar arrangement make steady advances in consolidating their own models of governance. The outcomes of the disputes between state and the private sector should be an indication of a potential path forward, although the US is unlikely to cripple its companies in the same way that China has at times done. Its attempt seems to be more at asserting its power and creating some minimal internal boundaries, rather than fundamentally restructuring the companies in its territory.

European Union

In spite of its relatively high level of development, the EU's capacity to produce tech companies of global reach has proven limited. While private actors with moderate reach exist, there are no examples that rival in scope or influence players such as Google, Yandex, or Alibaba; although Spotify and Klarna can be cited as important tech companies from the EU, and the number of unicorns in the region has been increasing, pointing towards future possibilities (Pojuner 2021).

If the global reach of European-based companies is limited when compared to its competitors, it is conversely succeeding in creating principles and models of regulation and legislation with broad impact and global reach. Although this approach has consolidated in recent times, its roots can be traced back to previous European Commission cases against US companies. This is notable due to how early some of these disputes were taking place, putting at odds an International Organization with important overseas software companies, signaling disquietude over the subject.

The EU first litigated against US tech companies back in the 2000s, when it raised concerns over what it perceived to be monopolistic behavior being carried out by Microsoft, particularly in the way its Operational System (OS) behaved. Windows came bundled with additional Microsoft software that offered added value to the essentials needed for normal computer usage, which the EU found to be a practice that limited competitivity, particularly the bundling of the Internet Explorer browser, which was even integrated into the OS's basic functions, reducing consumer choice (European Commission 2009).

Microsoft's defense presented arguments that the measure actually enhanced consumer experience, but the EU litigators were specific in their demands for less bundling of software. The proceedings unfolded over the course of several years, and eventually favored the EU, resulting in Microsoft needing to pay fines, as well as offering consumers from the region the option to install the browsers of competitors straight from a menu within the OS, instead of needing to search for those on the Internet.

This and other actions taken against the company in the EU, as well as some carried out within the US itself, resulted in Microsoft making several changes to its structure and operation, eventually decelerating activities and opening space for other actors to consolidate, particularly Apple. In other words, the EU (or state power more broadly) exerted transnational pressure and managed to influence the operation of a big tech company in such a way that it arguably even allowed for one of its competitors to grow. Financial costs and pressure for operational adjustments also impacted other actors, such as Google, criticized for similar reasons, such as the bundling of its own apps in the Android mobile system (Leurquin and Anjos 2021).

The emphasis on consumer agency and right to privacy made the region emerge as a purported champion of human-centered values, standing in some form of opposition to the liberal and control-centric approaches. The next decade proved even more significant in the EU's attempt to expand its reach over tech companies transnationally, with the development of the General Data Protection Regulation 2016/679 (GDPR). This marked the transition toward a broader enforcement of its vision, effectively making the approach transnational and causing ripple effects across the legislative environments of countries the world over.

GDPR is one of the main examples of what Bradford (2020) calls the "Brussels Effect", with the EU establishing parameters that are globally adopted, with a unilateral regulatory power that does not necessarily depend on coercion or direct intervention. In the case of GDPR, this process of regulatory globalization originates from the legal demand of states that want to share personal data with the EU needing to have an equivalent data protection law with similar values, leading to a "Europeanization of the global regulatory environment" (Bradford 2020, 132).

During IGF's 2018 opening ceremony, French President, Emmanuel Macron, brought up the GDPR as an example of a global standard in legislation and the European answer to the growing need for regulation in the digital field, aimed at the protection of the universal rights of citizens (Datysgeld and Pigatto 2019). This type of measure would allow for national governments to exercise their democratic attributions alongside the roles played by other stakeholders – basically using processes of co-regulation, where the state isn't the only one to regulate on an issue. This new path, according to the President, was a much required deviation from the binary options of "a Californian form of Internet" or a "Chinese Internet" (Macron 2018).

The power that the GDPR exerted over other stakeholders defined the way forward for the EU, with effects impacting not only states, but also institutions such as ICANN, which was forced into a long process of rethinking its public names database (Internet Corporation for Assigned Names and Numbers 2021). The EU is proceeding to develop other directives and laws that enable it to exert transnational control over policies and generate cascade effects.

As an example, the Gaia-X initiative, led by France and Germany, was framed as being able to possibly help the European market to compete with American and Chinese companies, as well as guaranteeing digital autonomy and data sovereignty. It was developed around the idea of a cloud infrastructure operated by European providers, in accordance with European regulations. In addition to having the intent of creating a common data infrastructure that would serve as a model, it was characterized as a state-driven initiative seeking to directly influence the cloud market, empowering data sovereignty (Pohle and Thiel 2020; Braud et al. 2021).

China

China has taken a leading role in the international system over the past decade, with a growing presence in international forums like Davos and even traditional spaces such as the United Nations. This has been interpreted as a consequence of Chinese development coupled with a multilateral approach, as well as a potential path toward upending the status quo and displacing existing actors (Öterbülbül 2021).

Internet development in China has been at odds with the West and some of its biggest companies. Google is a notable example, entering China in 2006 with a local version of its search engine, but departing four years later. This was reported as being a "cyberlibertarian" act that put freedom of expression above the Chinese government's requests for censorship. In fact, there was not only a progressive increase in demand for censorship, but also a series of cyber attacks on the company's intellectual property, which combined with state pressure, created a difficult operational environment for the company (Morozov 2011).

Since then, the Chinese digital sector has grown exponentially and became even more profitable. Google attempted to come back with a search engine that could meet Chinese government demands, with increased vigilance powers, named project Dragonfly (Gallagher 2018a). A journalistic article detailing the initiative caught the attention of activists and even the White House, with requests for the company to end it. As far as it is known, the project was eventually canceled (Gallagher 2018b).

With the Internet sector increasingly linked to the country's economic development, China began to promote its own cyberspace governance event (a term used by China in lieu of "Internet governance"). The World Internet Conference (WIC) is co-organized by the International

Telecommunications Union (ITU), and has attracted actors from the world over from governments and the private sector, in a forum that discusses emerging subjects in technology and the Internet, as well as featuring a technology showcase and even an award for technological innovations, always highlighting Chinese progress in areas such as Artificial Intelligence and connectivity.

The event has been held annually since 2014 (a year after the Snowden revelations), generally at the same time of the year as the IGF. The WIC does not focus on governance standards, but on the establishment of partnerships and cooperation, building upon a global governance discourse. Over the years, interventions made within this space can be summarized in terms of respecting digital sovereignty, as well as advancing cooperation in security and the digital economy. Thus, the WIC can be seen as a counterpoint to the IGF.

In a sense, this is another "mirror" institution from the Chinese international strategy, same as the Development Bank, which mirrors the World Bank. Also, the Chinese Internet went from "mimicking" Western apps such as with Baidu (a search engine like Google), AliExpress and TaoBao (retailers like Amazon), and Weibo (like Twitter), to creating its own platforms, sometimes even with more innovation packed into them (Dudarenok 2017).

The most notable case is the TikTok app, which impacted the posting and editing of videos, especially in the mindshare of younger people. Popularization of TikTok boosted the trend of short videos globally, in an indication of Chinese success in the appropriation and development of products with widespread cultural appeal, breaking regional barriers in a universe dominated by Western companies up to that point (Wang et al. 2020; Wade and Shan 2019).

The first edition of the WIC produced a statement which called for respect of Internet sovereignty in all countries, which ended up not being released in spite of being drafted (Shu 2014). In 2015, the subject was brought back up and reinforced. A speech by president Xi Jinping mentioned "building a cyberspace community of shared destiny", with the aim of establishing a multilateral governance structure and generating a global "cyber order" (China Daily 2015).

In 2017, the WIC highlighted the Belt and Road Initiative, as a series of multilateral partnerships in cooperation with neighboring countries, forming a digital "Silk Road". Examples include the partnership between China and Pakistan in fiber optic projects, as well as an undersea cabling system connecting Asia, Africa and Europe. In 2018, the establishment of the EU-China Connectivity Platform for cooperation in infrastructure boosted foreign investment opportunities (Reding 2018), being later complemented in 2021 by the approval of China's data protection law, in a similar tone to the GDPR (Ikeda 2021).

China still finds room to engage in other fora of global Internet governance. In addition to data protection (Chen 2021) and antitrust (Tan 2021) regulatory actions, there is also an eye toward protocols and infrastructure issues. The Chinese participation in the ITU is remarkable, as is the proposal of New IP (Gross and Murgia 2020), a protocol that would supersede the original fundamental Internet protocol, TCP/IP, created in the 1970s in the United States and in use to this day.

Thus, China uses both a strategy of inserting itself in more traditional institutions and an innovative strategy in the promotion of the WIC. China attempts to dialogue with all actors of interest, fulfilling the objective of bringing to the table the concerns and identities of each stakeholder who has access to the space. As stated by Wendt (1992), the system ends up being shaped by this socialization and formation of collective knowledge among the actors, which in turn will form the perceptions that each stakeholder has of the other.

Conclusion

When the UN convened the WSIS, at the time the only intergovernmental mechanism that dealt with Internet-related issues, an increasing harmonization of practices and regulations was expected due to the Internet's global nature. Today there is a plurality of fora, institutions and agendas that are not restricted to specialized spaces dedicated to Internet and communications, inside and outside traditional international relations institutions. This confirms Internet governance as an important arena of global power, and reinforces the role of the Internet itself as a power resource.

In the tripolar dispute for Internet governance, states deploy a variety of measures to advance their positions, including regulation. While the US maintains its liberal posture, it can also be observed that it puts progressive emphasis on limiting or overseeing the technologies that can be used within its territory, as is the case of the Clean Network Initiative. While this is not considered digital sovereignty by the state itself, it recalls aspects of the Chinese and EU approaches.

Given the EU's current legitimacy, its ability to generate transnational regulation has proven viable, convening actors around certain positions such as that of data protection norms. In effect, what this has amounted to is a mechanism that can be used to further objectives in Internet governance. However, the unique characteristics of this bloc make it so that this is not easily reproduced by other players, and in the long term, there are no guarantees to the stability of this approach, considering how reliant it is on the bloc's common understanding of issues and its overall stability.

This could potentially echo Brazil's momentary leadership in Internet governance. Changes in the political landscape had a direct impact in the continuity of the effort, even though many internal outcomes remain relevant, such as the aforementioned Marco Civil, which was built using the MSM approach and is still a notable national achievement. Had the scenario evolved differently, a Global South leadership in the agenda might have coalesced, but it would amount to guesswork to estimate the consequences that might have generated.

It is then interesting to evaluate China's quick development, built on the back of becoming the world's factory, now giving way to a strategy that puts more emphasis on cutting-edge research, and the achievement of greater international political impact. The state seeks avenues to express its voice, be it in existing institutions or new ones. This position in Internet governance might be a fraction of a broader phenomenon of assertion of Chinese sovereignty, digital or otherwise.

Despite political, social, economic and cultural differences, states maintain a belief in the power of international institutions as a venue to promote their governance models and influence other actors, shaping expectations, as Wendt would have it. In this scenario, the large digital technology actors play an important role in governance models, adapting to local needs or building policymaking spaces that aim to be supranational – as in the case of Facebook's Oversight Board. Co-regulation, that is, a regulation that is not exclusive to the state but is shared with non-state actors, has evolved into a key mechanism in contemporary International Relations.

Meanwhile, other states attempt to find their own approaches to Internet governance, while still remaining beholden to the positions of these three key players. It is not the case that there aren't other viable methods of governance, but rather that said methods either derive or depend on those presented by the tripolar approach. Authoritarian regimes will use some variation of China's control system, for example. The option to avoid these methods and the states that spearhead them are limited, and would cause severe consequences, such as would be the case of a state ignoring the EU's GDPR and the consequent decrease in access to the bloc's wealthy market.

The tripolar approach to Internet governance presents a new interpretation to phenomena that have unfolded during the geopolitical evolution of the network's ecosystem. Power dynamics are in constant flux, and the implications for the longer term of this arrangement are difficult to estimate. Due to that, we see great value in continuing to pursue the study of this interpretation of events, while still observing the role of the MSM and its processes on the broader agenda. Regardless of the governments in power, the role of international institutions remains, and carries specific expectations and histories that will continue to inform the setup of global Internet governance.

References

Abbate, J. *Inventing the Internet*. Cambridge, MA: MIT, 1999.

Blum, A. *Tubes: a journey to the center of the internet*. New York, NY: Ecco, 2012.

Bradford, A. *The Brussels effect: how the European Union rules the world*. New York, NY: Oxford University, 2020.

Braud, A., G. Fromentoux, B. Radier, and O. Le Grand. "The road to European digital sovereignty with Gaia-X and IDSA." *IEEE Network* 35, no. 2 (2021): 4-5.

Buxton, N. *Multistakeholderism: a critical look*. Amsterdam: Transnational Institute, 2019. (Workshop Report)

Chapelle, B., and L. Porciuncula. *We need to talk about data: framing the debate around free flow of data and data sovereignty*. Paris: Internet and Jurisdiction Policy Network, 2021. Available from: https://www.internetjurisdiction.net/uploads/pdfs/We-Need-to-Talk-About-Data-Framing-the-Debate-Around-the-Free-Flow-of-Data-and-Data-Sovereignty-Report-2021.pdf

Chen, A. "A close reading of China's data security law, in Effect." *China Briefing*, September 1, 2021. Available from: https://www.china-briefing.com/news/a-close-reading-of-chinas-data-security-law-in-effect-sept-1-2021/

China Daily. "China's proposals on world's biggest issues in 2015." 2015. Available from: http://www.chinadaily.com.cn/world/2015chinaproposal/index.html

Clegg, N. "In response to oversight board, trump suspended for two years: will only be reinstated if conditions permit." *Facebook Newsroom*, June 4, 2021. Available from: https://about.fb.com/news/2021/06/facebook-response-to-oversight-board-recommendations-trump/

Couture, S., and S. Toupin. "What does the notion of "sovereignty" mean when referring to the digital?" *New Media & Society* 21, no. 10 (2019): 2305-22. doi: https://doi.org/10.1177/1461444819865984

Datysgeld, M. "Understanding the Role of states in global internet governance: ICANN and the question of legitimacy." *SSRN Electronic Journal,* August 20, 2018. doi: https://doi.org/10.2139/ssrn.3235470

Datysgeld, M., and J. Pigatto. "A União Europeia quer uma nova Internet: do discurso de Macron à busca de outros caminhos para a rede." *Revista Mundorama*, January 25, 2019. Available from: https://mundoramanet.wpcomstaging.com/?p=25091.

Dekker, B. and M. Okano-Heijmans. *Europe's digital decade? Navigating the global battle for digital supremacy*. Amsterdam: Clingendael Institute, 2020. Available from: https://www.euagenda.com/upload/publications/report_europes_digital_decade_october_2020.pdf.pdf

Dudarenok, A. "Chinese social media platforms: a comprehensive overview of the top performers." *Medium*, December 15, 2017. Available from: https://medium.com/@ashleydudarenok/chinese-social-media-platforms-a-comprehensive-overview-of-the-top-performers-7d905ef35bcc

Edelman, G. "Biden is assembling a big tech antitrust all-star team." *Wired*, March 9, 2021. Available from: https://www.wired.com/story/lina-khan-ftc-antitrust-biden-administration/

European Commission – EC. "Antitrust: commission market tests Microsoft's proposal to ensure consumer choice of web browsers; welcomes further improvements in field of interoperability." *Press Corner*, October 7, 2009. Available from: https://ec.europa.eu/commission/presscorner/detail/en/MEMO_09_439

Gallagher, R. "Google plans to launch censored search engine in China, leaked documents reveal." *The Intercept,* August 1, 2018a. Available from: https://theintercept.com/2018/08/01/google-china-search-engine-censorship/

Gallagher, R. "Google's secret China project 'effectively ended' after internal confrontation." *The Intercept*. December 17, 2018b. Available from: https://theintercept.com/2018/12/17/google-china-censored-search-engine-2/

Gross, A., and M. Murgia. "China and Huawei propose reinvention of the internet." *Financial Times*, March 27, 2020. Available from: https://www.ft.com/content/c78be2cf-a1a1-40b1-8ab7-904d7095e0f2

Hafner, K., and M. Lyon. *Where wizards stay up late: the origins of the internet*. New York, NY: Simon and Schuster (1998).

Hofmann, J. "Multi-stakeholderism in internet governance: putting a fiction into practice." *Journal of Cyber Policy* 1, no. 1 (2016): 29-49. doi: https://doi.org/10.1080/23738871.2016.1158303

Holder, D. "Blockers to IPv6 Adoption." *Ripe Labs*, June 7, 2018. Available from: https://labs.ripe.net/author/david_holder/blockers-to-ipv6-adoption/

Ikeda, S. "New data protection rules from chinese government targeted squarely at limiting power of tech giants." *CPO Magazine*, April 27, 2021. Available from: https://www.cpomagazine.com/data-protection/new-data-protection-rules-from-chinese-government-targeted-squarely-at-limiting-power-of-tech-giants/

Internet Corporation for Assigned Names and Numbers – Icann. *System for standardized access/disclosure operational design phase*. Los Angeles, CA, 2021. Available from: https://www.icann.org/ssadodp

Kleinwächter, W. "NETmundial: divisor de águas na regulamentação da Internet?" *PoliTICs*, no. 18 (2014): 25-46. Available from: https://politics.org.br/sites/default/files/downloads/poliTICS_18.pdf

Krasner, S. "Structural causes and regime consequences: regimes as intervening variables." *International Organization* 36, no. 2 (1982): 185-205. doi: https://doi.org/10.1017/S0020818300018920

Kurbalija, J. *An introduction to internet governance*. Geneva: DiploFoundation, 2016.

Lessig, L. *Code: And other laws of cyberspace*. 2nd ed. New York, NY: Basic Books, 2006.

Leurquin, P., and L. Anjos. «Condenações da Google pela aplicação do Direito da Concorrência da União Europeia." *Revista de Defesa da Concorrência* 9, no. 1 (2021), 104-24.

Lewis, P., and P. Hilder. "Leaked: Cambridge Analytica's blueprint for Trump victory." *The Guardian*, March 23, 2018. Available from: https://www.theguardian.com/uk-news/2018/mar/23/leaked-cambridge-analyticas-blueprint-for-trump-victory

Macron, E. *IGF 2018 Speech by French President Emmanuel Macron*. Paris: Unesco, 2018. Available from: https://www.intgovforum.org/multilingual/content/igf-2018-speech-by-french-president-emmanuel-macron

Mariano, M., and K. L. P. Mariano "As teorias de integração regional e os Estados subnacionais." *Impulso* 13, no. 31. (2002): 47-69.

Mariano, M., J. T. Pigatto, and R. A. R. Almeida. "Atores internacionais e poder cibernético: o papel das transnacionais de tecnologia na era digital." *Monções* 7, no. 13 (2018): 199-229, doi: https://doi.org/10.30612/rmufgd.v7i13.8723

Mearsheimer, J. J. "Bound to fail: the rise and fall of the liberal international order." *International Security* 43, no. 4 (2019): 7-50. doi: https://doi.org/10.1162/isec_a_00342

Morozov, E. *The net delusion: the dark side of internet freedom*. New York, NY: Public Affairs, 2011.

Mueller, M. *Ruling the Root: Internet Governance and the Taming of Cyberspace*. Cambridge, MA: MIT, 2002.

NETMundial. "NETmundial Multistakeholder Statement." April 24, 2014. Available from: https://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf

Öterbülbül, S. "Rebranding China's global role: Xi Jinping at the World Economic Forum." *E-International Relations*, February 20, 2021. Available from: https://www.e-ir.info/2021/02/20/rebranding-chinas-global-role-xi-jinping-at-the-world-economic-forum/

Oversight Board. "Announcing the Oversight Board's first case decisions." January, 2021a. Available from: https://oversightboard.com/news/165523235084273-announcing-the-oversight-board-s-first-case-decisions/

Oversight Board. "Case decision 2021-001-FB-FBR." May 5, 2021b. Available from: https://oversightboard.com/decision/FB-691QAMHJ/

Pohle, J., and T. Thiel. "Digital sovereignty." *Internet Policy Review* 9, no. 4 (2020): 1-19. doi: https://doi.org/10.14763/2020.4.1532

Pojuner, I. "Europe now has 70 startup unicorns." *Sifted*, May 10, 2021. Available from: https://sifted.eu/articles/europe-unicorns-2021/

Polido, F. "Facebook oversight board: um tribunal global para a internet?" *JOTA Info*, September 4, 2019. Available from: https://www.jota.info/opiniao-e-analise/artigos/um-tribunal-global-para-a-internet-04092019

Rapoza, K. "Why American companies choose China over everyone else." *Forbes*, September 3, 2019. Available from: https://www.forbes.com/sites/kenrapoza/2019/09/03/why-american-companies-choose-china-over-everyone-else/?sh=639094671de2

Raustiala, K. "An internet whole and free: why Washington was right to give up control." *Foreign Affairs* 96, no. 2 (2017): 140-7. Available from: https://www.foreignaffairs.com/articles/world/2017-02-13/internet-whole-and-free

Raymond, M., and L. DeNardis. "Multistakeholderism: anatomy of an inchoate global institution." *International Theory* 7, no. 3 (2015): 572-616. doi: https://doi.org/10.1017/S1752971915000081

Reding, V. "Let's build bridges between China and Europe." *China Daily*. September 11, 2018.

Sassen, S. "On the Internet and sovereignty." *Indiana Journal of Global Legal Studies* 5 (1997): 545-59.

Shu, C. "China tried to get world internet conference attendees to ratify this ridiculous draft declaration." *TechCrunch*, November 20, 2014. Available from: https://social.techcrunch.com/2014/11/20/worldinternetconference-declaration/

Statista. "Global digital population as of January 2021 (in billions)." January, 2021. Available from: https://www.statista.com/statistics/617136/digital-population-worldwide/

Tan, J. “China orders Tencent to give up exclusive music licensing rights as crackdown continues.” *CNBC*, July 24, 2021. Available from: https://www.cnbc.com/2021/07/24/china-crackdown-antitrust-regulator-orders-tencent-music-to-give-up-music-label-rights.html

The United States Congress. *Title 47 United States code. Communications Decency Act of 1996. Section 230*. Washington, DC, 1996.

Torre, L., and G. Brown . “What is the California Privacy Protection Agency?” *IAPP*, November 23, 2020. Available from: https://iapp.org/news/a/what-is-the-california-privacy-protection-agency/

Wade, M., and J. Shan. “TikTok - China’s first globally successful app.” *Business Times*, January 12, 2019. Available from: https://www.businesstimes.com.sg/garage/news/tiktok-chinas-first-globally-successful-app

Wang, J., Y. Shen, and J. Hong. “The emergence, development, and evolution of chinese social media.” In *China in the Era of Social Media: An Unprecedented Force for an Unprecedented Social Change*, edited by Hong, J., 9-38. Lanham, ML: Lexington, 2020.

Wendt, A. “Anarchy Is What States Make of It: The Social Construction of Power Politics.” *International Organization* 46, no. 2 (1992): 391-425.

World Summit on Information Society – WSIS. *WSIS: Tunis Agenda for the Information Society*. Geneva: International Telecommunication Union, 2005. Available from: https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html