Policy Brief

August 2022

The Territorialization of Cyberspace and GAFAM Geopolitics: Driving Forces and New Risks in the Wake of the Ukrainian Crisis

By Mohamed Benabid

PB -52/22

Information is among our planet's most coveted resources, calling upon us to examine how it is incorporated as an object of power and domination into national and international political processes. Tensions around this resource arise not only in territories directly controlled by States, but also in contested territories, including the intangible acceptance of these, as occurs in cyberspace. The Russia-Ukraine war epitomizes this. Having "disconnected" Russia and conversely maintained service in Ukraine, the attitude of GAFAMs (an acronym referring to Internet giants - Google, Apple, Facebook, Amazon and Microsoft), effectively becoming stakeholders in the conflict and projecting a new vision of their power, carries profound geopolitical weight. Such developments heighten the sense of mistrust towards cyberspace and echo the debate around Internet governance and cyber sovereignty, areas where major powers are attempting to reassert their strategic authority. For the time being, the stalemate in this conflict further distances any possibility for international consensus.

POLICY CENTER FOR THE NEW SOUTH
THINK • STIMULATE • BRIDGE

GAFAMs sided with the pro-Ukrainian front from the outset of the Russia-Ukraine war, Kiev thereby gaining a valuable ally in its fight against Moscow, adding a novel dimension to international conflicts. Microsoft, Apple and Amazon suspended the sale of physical and dematerialized products in Russia, including the Play Store and Apple Store apps, and Amazon's AWS cloud services. YouTube suspended advertising revenue generation for all Russian state media, and Google deployed a bombing alert system on its Maps app.

Beyond physical measures, social media rallied as never before to maintain service in Ukraine, enabling Kiev to keep communicating and win the international battle of perception. Facebook, Instagram and WhatsApp even bent their rules prohibiting calls to violence, allowing forms of political expression that would otherwise hardly be accepted, e.g., "Death to Russian invaders".

GEOPOLITICAL CONFLICT

It is not the first time Internet protagonists contribute to a redistribution of power or shake up existing regimes. The role played by digital social networks in militancy and activism during the Arab Spring of 2011, the Hong Kong protests of 2019-2020 and the first Ukraine Dombass war in 2014, is well established. More recently during Covid-19, this role continued to expand as the issue of US Gigatechs crept to the forefront amidst the interplay of infodemic stakes and against a backdrop of GAFAMs' overwhelming dominance of the information ecosystem.

While there is nothing radically new in positing parts of cyberspace as a locus of geopolitical conflict, the Russia-Ukraine crisis certainly appears to intensify the issue insofar as Internet companies take a head-on position in the conflict, seeking to weaken a fundamental war strategy component, namely the control of information and communication flows. In fact, the war in Ukraine demonstrated that unprecedented configurations were possible, with the prospect of fully integrated services in control of all areas of cyberspace- as illustrated in the case of Elon Musk, at once a telecom operator with Starlink and, at one point, a potential buyer of Twitter, before pulling out of the takeover bid. Reversing the initial discourse surrounding these companies' original vocation, such developments reaffirm a transition towards new stances where technology increasingly asserts itself as an instrument of power. Often at the sole service of big business. GAFAMs no longer shy away from donning their new robes as they find reassurance in their technological supremacy. This striking power finds its roots in the conceptual foundations of the "network society" as defined by Castell & Cardoso (1996)[1] and the complex arrangements of "control infrastructures" as defined by Kumar (2021)[2], i.e. "norms, conventions and algorithmic modulations" that contribute to regulating "human behavior on the Web" (p.7).

This power is backed by financial performance: $2129 billion in market capitalization for Apple[3] (greater than the GDP of Brazil, Korea or Canada), $1582 billion in market capitalization for Microsoft, $1415 billion for Alphabet, the parent company of Google (nearly the GDP of Spain and greater than the GDP of Australia) and $443 billion for Meta Platforms (Facebook).

1. Castells, M., & Cardoso, G. (1996). The network society (Vol. 469). oxford: blackwell.

2. Kumar, S. (2021). The digital frontier: Infrastructures of control on the global Web. Indiana University Press.

3. As of June 20, 2022

COGNITIVE LAYER

The very essence of these companies raises issues transcending physical infrastructure, and "layers" to borrow cyberspace terminology. The standard typology tends to circumscribe effects to the informational, so-called cognitive layer of cyberspace, which pertains to content production. This layer is not dissociated from other layers: infrastructure, protocols and the so-called logical layer. However, what used to be exceptional is now a permanent landscape feature, turning this layer of cyberspace into a place of rivalry, just like the other three.

This supremacy that has grown stronger over the years, fascinates as much as it worries. What safeguards are there in the face of organizations capable of connecting 4.6 billion users, over half of the world's inhabitants, yet at the same time dragging a dubious reputation, accused of controlling the very systems through which we communicate, of amplifying hateful content and fake news, and of maintaining the opacity of algorithms at the core of their business models.

These companies are emblematic of global information networks often flouting national and supranational regulatory frameworks, and exert an influence that sometimes exceeds the political weight of States in governing democratic and civic life. These firms are grabbing it all: the bulk of traffic, revenue and attention. Their stranglehold on personal data creates an asymmetry of power to the detriment of users. Cynics will still find it a great showcase for digital capitalism. For alongside an idealized version of the Internet that lowers barriers to entry, enables small entrepreneurs to try their luck and possibly become wealthy influencers, a more subtle picture emerges, where the risk of concentration is high, and primarily favors dominant players, and where algorithms now carry geopolitical overtones.

CONCENTRATION

The concentration of power here is more problematic than in other sectors, given issues at stake for the preservation and/or destabilization of democracy. Despite denying it, these corporations, like the conventional media, have the power to gatekeep[4] information and, consequently, shape public opinion, persuade and influence. This is why we speak of Internet intermediaries and infomediaries in this article5[5], as the usual term "platforms" is not neutral, and is often tied to a discursive rhetoric feeding an elasticity of identity, when not used to disguise the position of actors to at the very least avoid any ad hominem criticism, leading one to believe these companies have no editorial purpose. In fact, it is precisely around these editorial stakes that everything hinges: the capacity to influence the masses, orient what humanity consumes as information and grant or withhold the right to speak. Not only does an editorial purpose exist, but more problematically, curation criteria (i.e. the selection, editing and sharing of content) are concealed, which only adds to the sense of suspicion.

As to their geopolitical status, it exceeds and transcends conventional territoriality and forms of power that are explicit in a State framework. The present analysis does not lose sight of the political character of this influence and of the fact that actors at play are private.

4. This notion, a cornerstone of journalism, refers to the process of filtering and selecting what is publishable.

5. Term referring to third-party actors who mediate digital content and human communities that produce and use the same content.

SUBORDINATE POWERS

As De Gregorio[6], points out, it is not so much technology or algorithmic power that is in question, but the "threats of emerging private transnational powers". A number of works examined the extent to which these practices deserve to be labeled as "anarchic Internet", as they are set up internally, on a discretionary basis.

It is not yet clear whether this power stems from implicit subordination to another power, a state power this time. This assumption, still prevalent in part of the literature, considers the distinction between private interests (as those of GAFAM) and state interests irrelevant, as the former have at one time or other depended on public subsidies for their establishment and/or development. In contemporary times, the role of the Clinton administration in liberalizing the Internet in the late 1990s is undisputed. This strategy was epitomized at the time by Vice President Al Gore and his now legendary concept of the "information superhighway".

Yet this Bourdieusian perception of power should not be endorsed without reservation, as it presupposes an existing agenda (One must go back to the 1930s to see the first US trailblazing structures driven by entrepreneurial State Science) or a higher order guiding the process.

By complacency or fear of compromising the development prospects of initially promising technologies, public authorities in many countries failed to adequately appreciate the scope of these transformations. Many today helplessly witness a quake that jeers at their own prerogatives, as evidenced in the power to censor a head of state (as in the case of Donald Trump, deprived of his Twitter account in 2021)[7], to make or break elections (as happened with the Cambridge Analytica scandal and Facebook's suspicions of manipulating personal data), and to connect or disconnect a country by deliberately taking a stand in a conflict such as that between Russia and Ukraine.

DEGLOBALIZATION

In light of this unprecedented global configuration, it is conceivable that there be threefold consequences. First, the acceleration of Cyberspace territorialization. This new theater for international tensions actually exacerbated negative externalities conducive to the risk of de-globalization. The issue dates back at least to the 2008 crisis, using the global trade openness timeline, and is today specifically focused on telecommunications. It is well established that drawbridge strategies ride on waves of populism and nationalism. This might sound counterintuitive in our age of hyperconnectivity, but today it finds fertile ground with Moscow's ban on Facebook, Twitter, Instagram and Youtube, and vice versa with the EU's exclusion of Russia's main bank, Sberbank, from the Swift system, a major cyberspace communication protocol.

Subsequently, a consequence of the above is a likely re-assessment of two other questions, that of Internet governance and that of cyber-sovereignty. The first is on the diplomatic

6. De Gregorio, G. (2022). Digital constitutionalism in Europe: Reframing rights and powers in the algorithmic society. Cambridge University Press.

7. While these companies deserve credit for opening up unprecedented spaces of freedom of expression, the manifestations of this power on issues of content moderation are not matched by clear and transparent guarantees for the protection of user rights.

agenda since the World Summit on the Information Society of Geneva in 2003 and Tunis in 2005. Overwhelmed by the promise of digital technology, Internet governance remained a weak link in constitutionalism for a long time, governed solely by market considerations. As it usually advocates for self-regulation as the preferred Internet mechanism, the US approach confirmed this status quo. The difficulty lies in the absence of consensus on the ideal legal architecture, as the international legal landscape hides a complex mix of European Romanist conceptions of law and Anglo-Saxon common law, where norms emanate from practices and customs. From the outset, US public policy was one of laissez-faire, with the hope of self-regulation, which ultimately never materialized.

To the celebrated principle of a global Internet, in principle independent of political power, Russia and China have for years opposed a "sovereign Internet" where States have a say through mechanisms to be devised under the guidance of the United Nations and/or the International Telecommunication Union (ITU). The issue of ICANN (Internet Corporation for Assigned Names and Numbers), the body that manages domain names, long under US domination, initially crystallized most of the discussions. In 2008, the debate resurfaced with the election of Obama, whose victory was attributed, in part, to massive recourse to social networks and harnessing the opportunities afforded by Web 2.0.

CYBER-SOVEREIGNTY

Starting in 2010, the rising importance of social media shifted the Internet governance debate from the periphery to the center, albeit not in the direction sought by the US administration, weakened in 2013 by Edward Snowden's whistle-blowing on NSA (National Security Agency) surveillance systems. These revelations came as a bombshell and brought privacy and personal data protection challenges to the core of the matrix we call the "geopolitics of the Internet".

The second issue, cyber-sovereignty, is not unrelated to the first. The battle rages for control of the lucrative data market, now a main area of confrontation between superpowers and of the many applications of AI. The fact that Gigatechs strongly covet underwater cable infrastructure (three quarters of which is owned by GAFAMs) supports this view. In the race to secure supplies, China and the United States have been at loggerheads over the semiconductor industry, and more recently the "Chips Act", a plan presented by the European Commission in February 2022[8], similarly reflects this competition. US supremacy seemed unassailable so far. But for how much longer? China's desire to outperform the US is clear on a number of fronts. Beijing aims to be at the heart of the global economy by 2049, the 100th anniversary of Communist China, and to do so, is focusing on these technologies as a primary development strategy. On the issue of social networks specifically, it is mainly the meteoric rise of China's TikTok, the world's most downloaded application in 2020, ahead of Facebook that is notable. This success has not gone down well in the US, with Washington considering a TikTok ban from major stores, Appstore and Playstore, officially on grounds that Beijing could use it for espionage purposes. Attacks not unlike those on another Chinese company, Huawei. Today, this singular saga puts its CEO, Zhang Yiming, and its parent company, Byte Dance, on the list of top case studies to be studied in business schools, as per Apple with Steve Jobs, Tesla with Elon Musk and Facebook with Mark Zuckerberg.

8. It aims to quadruple Europe's production capacity by 2030.

Cybersecurity has emerged as a major issue for China over the past decade, with Beijing aiming not only to become a cyberpower, but also to enter the race for norm-making in cyberspace.[9] Here, too, and as with Internet governance, China favors a level playing field where every state has a say in deciding the rules and norms that govern cyberspace globally.[10] This is also the position of Russia, which has on several occasions sought to spearhead an international movement that gives national governments primacy in shaping cyberspace standards.

Negotiations around root DNS servers, a crucial piece of hardware that enables data redirection via domain names (thirteen root DNS servers are currently in existence worldwide), clearly illustrate the magnitude of the stakes. Beijing advocates for a multilateral, not multi-party, negotiation framework to minimize any chance of the United States retaining control. Other areas of strategic competition include the battle over 5G and the Internet of Things, where both China and the United States seek to impose their standards. The old continent also seeks to impart its rhythm through initiatives for upgrading the existing corpus around digital commons, including the Digital Services Act and Digital Market Act.

A topic related to cyber sovereignty discussions is the extent of state responsibility in the event of a cyber incident with cross-border effects, as well as the degree of control they are expected to exercise over infrastructure located on their territory.

One section of Western doctrine assumes, at this level, that rules applicable to the physical world are also valid for cyberspace and that it is therefore sufficient to transpose them. This approach is in line with the Tallinn Manual recommendations, a guide published in 2013 by a North Atlantic Treaty Organization (NATO)-mandated working group, that adopted an expansive interpretation of conventional international law on sovereignty.

In the wake of this, the issue of sovereignty in cyberspace touches on a still gaping wound, that of the backwardness of developing countries consigned to mere user/consumer status, but who still hold out in hope of being able to include their voices in multilateral negotiations, provided that changes to the international political and security context do not dictate otherwise.

In a world that will remain, at least in the medium term, scarred by the throes of the Russia-Ukraine crisis, chances for an optimistic scenario are slim, but still there. They presuppose that cyberspace be considered as an international common good and, therefore, be free from any exclusive sovereign control.

9. Shen, Y. (2016). Cyber sovereignty and the governance of global cyberspace. Chinese Political Science Review, 1(1), 81-93.

10. Ibid

Conclusion

The geopolitical role of GAFAMs is particularly relevant in analyzing the Russia-Ukraine war. While it does not fundamentally alter conflict outcomes, as wars are primarily won on the ground, this role creates novel problems in international relations history, calling for technology companies to be considered as instruments of foreign policy on which the great powers, and not only the United States, implicitly and explicitly build their supremacy. The eruption of a digital component to the Russia-Ukraine war could revive the battle for cyberspace hegemony, with the risk of accelerating its territorialization. Questioning these issues therefore implies reiterating the major principles that govern the foundations of the Internet, particularly with regard to issues of governance and cyber-sovereignty, and exploring the resolutely institutional and political nature of GAFAMs motivations and decisions. As they emanaeg from non-state actors in true hybrid warfare tradition, their practices create legal and ethical dilemmas because of their cross-border effects.

About the Author, Mohamed Benabid

Mohamed Benabid est enseignant à la Faculté de gouvernance, sciences économiques et sociales (FGSES) de l'Université Mohammed VI polytechnique. Lauréat de l'Ecole de journalisme de Strasbourg, titulaire d'un doctorat en sciences de l'information et de la communication de l'Université Paris VIII et d'un doctorat en science de gestion de l'ISCAE, il compte à son actif près de 30 ans d'expérience dans l'industrie des médias. Son parcours pluridisciplinaire l'a conduit à couvrir depuis plusieurs années un large éventail de sujets : veille et intelligence économique, Médias/journalisme, Knowledge Management, géostratégie d'entreprise, géopolitique, communication politique, gestion et communication de crise entrepreneuriat, management stratégique, méthodologie de la recherche en sciences de gestion.

About the Policy Center for the New South

The Policy Center for the New South (PCNS) is a Moroccan think tank aiming to contribute to the improvement of economic and social public policies that challenge Morocco and the rest of Africa as integral parts of the global South.

The PCNS pleads for an open, accountable and enterprising "new South" that defines its own narratives and mental maps around the Mediterranean and South Atlantic basins, as part of a forward-looking relationship with the rest of the world. Through its analytical endeavours, the think tank aims to support the development of public policies in Africa and to give the floor to experts from the South. This stance is focused on dialogue and partnership, and aims to cultivate African expertise and excellence needed for the accurate analysis of African and global challenges and the suggestion of appropriate solutions. Read more

Policy Center for the New South

Building C, Suncity Complex, Al Bortokal Street Hay Riad - Rabat
Email : contact@policycenter.ma
Phone : +212 (0) 537 54 04 04 / Fax : +212 (0) 537 71 31 54
Website : www.policycenter.ma

POLICY CENTER FOR THE NEW SOUTH
THINK • STIMULATE • BRIDGE