June 28. 2021 – Isabel Serpa da Silva

Multilateralism and the Geopolitical Appropriation of the Internet

In the course of the geopolitical appropriation of the Internet, multilateral forums have become a venue for the power-political struggle to shape cyber norms. What form and function can, and should multilateralism take to counteract further fragmentation of cyberspace in the post-liberal era?

Cyberspace is currently undergoing a fundamental transformation, which is largely driven by the security practices of state actors. In this context a new geography of the Internet gradually emerges. Characteristic of this process is its emergence along four correlated lines of development: (1) the perception of interdependence as a threat, (2) the emergence of coexisting cyber powers, (3) the nationalization of Internet policy, and (4) the separation of intersecting interaction with other cultural areas. These developments present new challenges to multilateral cooperation, which have the potential to change both the form and function of multilateralism in the face of a new geopolitics of the Internet.

Against this background, the Federal Government of Germany (2021) emphasized the need for the inclusive opening of multilateral cooperation. In the recently published 'White Paper on Multilateralism', it is being stressed that "the legitimacy of multilateral action derives from its commitment to the rule-based international order. Legitimacy, however, is equally based on representation and participation" (p.24). The inclusion of companies, non-governmental organizations, and expert communities to shape cyber norms would thus, in the perception of the Federal Government of Germany, increase the legitimacy of multilateral decision-making and agreements.

Particularly interesting about this line of argumentation is that the Federal Government of Germany, by emphasizing the need to include multiple stakeholders, resigns from the state-centered understanding of sovereignty in governing cyberspace. Instead, it emphasizes the growing relevance of inclusive multilateral solutions to stabilize the digital order of the future. Considering that the status quo of the existing multi-stakeholder model is currently being challenged even among

Western democracies, this, in turn, seems astonishing. The fact that a necessary reformation of the existing multi-stakeholder model derived from this ambition of an inclusive opening of multilateralism, however, remains completely undiscussed. Nevertheless, the implicit thesis of the genuine democracy-friendliness of the multi-stakeholder model presented in the "White Paper Multilateralism" must be subjected to critical reflection. Providing an insight into the development of the geopolitical appropriation of the Internet as well as the divergent concepts of sovereignty as a challenge for a multilateral cooperation, this article aims to take a stance at the subject of multistakeholderism as a form of inclusive multilateralism.

A New Geography of the Internet – Lines of Development

Currently, we are experiencing a turning point in security policy practice. In this context, the ability to defend digital territory is becoming an increasingly normal phenomenon that joins the common repertoire of modern statehood. This development, however, does not stand alone but goes hand in hand with the growing capacity of both state and non-state actors to use digital tools to inflict harm on opponents. Cyber tools open up new dimensions in the meaning of war, warfare, and violence, as they threaten both vital infrastructures and information resources in potentially devastating ways without using physical violence in the conventional sense (Reuter, 2019). Accordingly, the perception of numerous state actors has been influenced by "the possibly crushing weight of a global crowd of spies, criminals, vigilantes, military units, cuckolded citizens, terrorists and opportunistic attackers attempting to reach anywhere that cyberspace extends" (Demchak, 2011, p.275).

Although one must emphasize that there is a significant gap between the perceived threat from cyberspace and the actual extent of violent cyber incidences, the narrative of cyberspace as a domain of warfare persists. This is due in particular to structural features of the digital space since the immense uncertainty, unpredictability, complexity, interdependence as well as the lack of information and case studies create an almost unmanageable and nonassessable context for state actors. This, however, leads them to overestimate risks associated with the threat of hostile third parties (Gomez/Villar, 2018, pp.62-63). The intertwining of the characteristics of cyberspace with the individual cognitive processes of human actors triggered a development according to which cyberspace, once perceived as

the tool for democratization and liberalization, developed into a *domain of conquest*. It functions as a geopolitical platform for state actors to fight over both the control of critical infrastructures as well as the design of values, interests, norms, and ideas in the context of a new, emerging geography of the Internet.

Contrary to the once clear Westernized cyberspace, this geopolitical process is characterized by a juxtaposition of different cultural areas, which, due to the fusion of economic and security interests, are all striving to expand their cyber powers. Especially significant about this process is that, in line with the ongoing power-political struggle between competing actors, the understanding of digital sovereignty grew into a comprehensive economic concept, which first and foremost aims to extend the state's "autonomy and ability to act" (BmWi et al., 2014, p.4) in the field of "information and telecommunications technology" (ibid.). On that account, cyber tools became a means to an end to protect critical infrastructures and information resources from disruptions by hostile third parties. The ongoing "digitalization of warfare" (Schörnig/Werkner, 2019) must therefore be understood as a symptom of a geopolitical change that is not only limited to the physical space but also beginning to take over the digital realm. However, the digital demarcation process resulting from this geopolitical conversion process is accompanied by a normative change in the perception of cyberspace as a domain of warfare. Consequently, the design features of the Internet – openness, hierarchy freedom, decentralization, and anonymity – are increasingly being challenged in favor of the pursuit of national security.

When it is commonly accepted among state actors that critical systems can no longer be trusted as they are connected to the open, global web, they begin to find a way to counter potential threats to their national territory through cyberspace. This requires that state actors increasingly take the lead in governing cyberspace so that they can reorganize or even separate the interacting interfaces to other cultural spaces that are perceived as potential threats. What may seem bizarre at first, however, does, from a historical point of view, not constitute an unusual reaction to maintain sovereign control as the hallmark of functioning statehood (Demchak, 2011, p.276).

Competing Conceptualizations of sovereignty as a challenge for multilateral cooperation

As Müller (2017, p.3) pointed out, the conflict over internet governance in the post-liberal era translates into a complex, multidimensional power struggle that focuses on the task of (re-)shaping national sovereignty in times of digitalization. In this context the multilateral process on cybersecurity grew into a central element of the power-political struggle in establishing a normative order of the internet. This process mainly centers around divergent cyber powers (USA, EU, China, Russia), which all pursue the goal of establishing norms for the autonomy and self-determination of the state in governing cyberspace. By doing so, however, different cyber powers act according to different normative standards and ordering principles, which makes it difficult to reach a multilateral consensus.

The Chinese conception of Internet sovereignty, for instance, centers around the idea of implementing territorial borders in the digital space through state control mechanisms such as filtering measures and censorship as well as the construction of an externally delimited digital space. However, it is not just an inward-looking concept since, especially in recent years, a new development has become apparent, as Beijing is increasingly aiming to export norms to shape the digital order. This is particularly evident in the promotion of the Chinese model of Internet governance in forums of multilateral debate (e.g., UN GGE, Internet Governance Forum, ITU). At the same time, the concept of Internet sovereignty fulfills a double function for Beijing: on the one hand, to influence emerging cyber practices and the meaning of statehood in the course of the digital revolution, and on the other hand, to increase the legitimacy of the Communist Party, which sees itself strengthened by the fact that more and more governments of the Global South are joining the Chinese normative framework (Chen et al., 2017, pp.452-453).

Like China, Russia also propagates an authoritarian conception of Internet sovereignty that focuses on the use of technical capabilities to create an information space that can be decoupled from global events. Thereby, the logic of Russia to secure the internet is significantly linked to the definition of the terms 'information' and 'information security', while simultaneously considering the digital information space to be a part of the physical territory. Similar to the Chinese model, the concepts of sovereignty and territorial integrity here are inherently linked to the

regulation of digital information flows (Kovaleva, 2018, pp.141-142). On the international stage, this conception emphasizes international law principles to preserve state sovereignty in cyberspace, for instance, the principle of non-intervention, which, according to the Russian image, should be transferred from the physical to the digital sphere, has been discussed (Claessen, 2020, p.146). This shows above all Moscow's domestic political ambition to protect the authority and responsibility of the state from developments in the information space to guarantee "the stability of the constitutional order, sovereignty, and the territorial integrity of the Russian political, economic and social stability in the unconditional provision of law and order and the development of equal and mutually beneficial international cooperation" (Doctrine for Information Security, 2000, quoted from Claessen, 2020, p.146).

Although the facets of the Russian and Chinese conception of Internet sovereignty vary, they are united by numerous semantic patterns of interpretation and strategic goals in their quest for isolation. Consequently, both states use multilateral forums not only alone but also jointly to expand their power radius. In this manner, they aim to underpin the demand for more state agency in the digital space by submitting reform proposals that undermine the hegemony of the multi-stakeholder model. This, however, already initiated a discursive reinterpretation of how cyberspace should be perceived and therefore governed. Hence, the (Western) image of the Internet as a free and global information and communication medium already is dissolving, while both Russia and China are strategically using existing forums of cooperation and at the same time initiating new forums for themselves, e.g., the World Internet Conference (WIC) and the Shanghai Cooperation Organization (SCO), which have an exclusively Central Asian character (Deutsche Gesellschaft für die Vereinten Nationen e.V., 2019, p.2).

While investigating the discourses among Western democracies, it is already noticeable by the terms 'digital sovereignty' and 'cybersecurity', in contrast to 'Internet sovereignty' and 'information security', that Western conceptions of cyberspace rely on a divergent foreign-policy vocabulary. This division reflects specific future visions of cyberspace, which seem difficult to reconcile within one framework of global digital order. Even though, for instance, the debate on digital sovereignty in Germany and other Western countries is based on some elements

that also share Chinese and Russian conceptions (e.g., autonomy and technological sovereignty), it is conducted under completely different auspices. In this regard, especially the discursive linking of 'digital sovereignty' and 'cybersecurity' with the pursuit of human and fundamental rights must be emphasized. This framework focuses on a foreign policy approach that establishes norms, rules, and principles and thus enables states to act responsibly in cyberspace as the top priority (Claessen, 2020, p.152).

Following this line of argumentation, it becomes clear that the multilateral practice of state actors in governing cyberspace can be described as a discursive process characterized by the rhetoric of divergent cyber powers taking contrary stances at the meaning of national sovereignty in the course of the digital revolution: on the one hand, the principle of non-interference and the control of the state over the information space, on the other hand, the need for collective responsibility while designing a secure and resilient cybersecurity architecture stand in the foreground (Barrinha/Renard, 2020, pp.757-758). Obviously, there is a need for a multilateral approach towards a cooperative cybersecurity policy, still cooperation attempts to this day are often limited to the bilateral level. Institutionally, these semantic disparities are already manifested in the development of two separate working groups within the UN: (1) the UN Group of Governmental Experts (UNGGE), which puts the principle of responsible collective state action at its core and is essentially led by the USA, and (2) the Open Ended Working Group (OEWG), which, although it officially has a different function, aims to realize the authoritarian idea of sovereignty in cyberspace and is under Russian leadership.

Rethinking Multilateralism, Reforming Multi-Stakeholder Governance?

In addition to divergent conceptualizations of sovereignty, shifting narratives are also significant for the geopolitical process in which a new geography of the Internet arises. This is derived from the fact that state actors are taking over more and more control in Internet governance by shifting debates on secure and stable infrastructures to intergovernmental or bilateral agreements. The prevailing multi-stakeholder model, which allows civil society and industrial actors to play a role in shaping Internet governance, thus sees itself increasingly replaced or displaced by cyber-diplomatic dialogues. As more and more Western governments are challenging the status quo of the multi-stakeholder system, the trend of pursuing

state control in governing cyberspace which has once solely been assigned to authoritarian states, therefore is in disintegration (Barrinha/Renard, 2020, p.759). These developments must be viewed critically since the interaction of governmental and non-governmental as well as technical and policy-oriented networks of experts prove to be essential to maintain an open and inclusive digital space (Liaropoulos, 2016, pp.22-23).

In addition, involving non-state actors in the multilateral process of developing cyber norms is necessary since a normative framework, which is negotiated exclusively among state actors, is also exclusively geared to the needs and practices of those same actors. It is not explicitly tailored to guide the actions of companies and civil society actors in confronting threats from cyberspace. Nevertheless, companies are increasingly threatened by cybercrime and cyber espionage, while particularly the larger players (e.g., Microsoft) can counter these threats (Butler/Lachow, 2012, p.3). In the process of creating norms of behavior in cyberspace, the private sector must be integrated in a way that considers its undeniably important role in and intertwining with global cyber concerns.

However, such an integration of non-state actors into multilateral cooperation would also, and especially regarding the corporate sector, require further developments. In this respect, the naive idea of multi-stakeholder governance as an inherently democracy-friendly system must finally be banished. Hence, a critical discourse among theorists and practitioners must be initiated while focusing on the use of the term 'multi stakeholderism', as it is all too often used as rhetorical means to legitimize and solidify existing power asymmetries in the policy process. In the context of a constitutional reformation of multi-stakeholder governance, research must, furthermore, explicitly deal with the danger of a depoliticization of the norm-building process in favor of corporate interests and the associated developments of a digitalizing neo-liberalism (Palladino/Santaniello, 2021, p.153).

The expansion of multilateral cooperation to include non-state actors would therefore raise a multitude of new questions for politics and science. Those would not only center around new forms or functions of multilateralism, but also around the associated structural change of multi-stakeholder governance. In this context, it is not only necessary to develop new procedures, but also to critically reflect to what extent these new procedures are able to fulfill rather than undermine democratic

norms of equality, participation, and inclusion.

Against this background, it becomes all too clear that we are confronted with a difficult undertaking; however, regarding the disruptive transformation that the digital space is currently experiencing, it cannot be an easy solution that counteracts further fragmentation and polarization. In this respect, the multi-stakeholder model should not be devalued too quickly when it comes to questions of multilateral cooperation and Internet governance. It should rather be placed in a more democratic context, including new actors and future demographic trends in the development of cyberspace. Especially given the current divergence of cyber powers and the dwindling monopoly of the global North, it is important to emphasize this aspect once again. A framework convention, a reform of participatory procedures, the involvement of non-state actors (especially from the civil society sector), and a will to involve governments of the Global South in cyber diplomatic negotiations are therefore at least required if an inclusive governance model is to be implemented that can counteract current trends in the securitization of international cybersecurity policy.

Summing up, it currently seems even more urgent to find inclusive multilateral solutions that involve both state and non-state actors to develop a comprehensive framework of norms and confidence-building measures that enable a "post-liberal internet governance system". However, given the existing power antagonisms between those stakeholders, the states, who have the authority and resources to regulate a range of activities in cyberspace, such a vision of an inclusive post-liberal Internet governance system seems nearly utopian. Rather, the emerging picture points in the direction of a system of 'multi-order governance' (Barrinha/Renard, 2020, p.765), in which multilateral cooperation functions as a bridge between different blocks that have acquired their own system of Internet governance over time.