Working Paper
SWP Working Papers are online publications within the purview of the respective Research Division. Unlike SWP Research Papers and SWP Comments they are not reviewed by the Institute.

SWP

RESEARCH DIVISION GLOBAL ISSUES | WP NR. 02, NOVEMBER 2019

One World, Two Visions, Multiple Nets?

November 2019

Daniel Voelsen

The theme of this year's Internet Governance Forum (IGF) is “One World. One Net. One Vision”. The theme does not describe the world we live in. In fact, powerful actors today deliberately provoke a fragmentation of the Internet all the way down to its technical core. The bleak prospect is that we might soon find ourselves in a world of multiple nets, with powerful gatekeepers controlling the links between them. It is not too late, yet, to respond to these developments. Doing so, however, will require significant and concerted efforts. The IGF’s theme, it turns out, is an urgent call to action.

One World

Over the last few decades, the Internet has developed into a unique global communications system. It is a sad truth that billions of people—most of them living in developing countries—still do not have access to the Internet, and to all the political, economic and personal opportunities that it provides. In principle, however, the Internet has the potential to connect the whole world.

The Internet is unique because it is a network of networks. The sub-units of this network are owned and operated by different actors and serve a wide array of purposes. The Internet connects all these different sub-units and thus facilitates the global exchange of information. Historically, it has developed around a set of basic network protocols. These protocols, for example, create a global addressing system (e.g. IP, DNS) and mechanisms for transferring data (e.g. TCP, BGP). They are the foundation of the global Internet as it exists today.

Stiftung Wissenschaft und Politik
German Institute for International and Security Affairs

Two Visions

The development of the Internet has been accompanied by intense political controversies over its global infrastructure. These controversies are often portrayed as a clash of two distinct visions of the Internet.

The first of these emphasizes open standards and protocols, decentralized control and voluntary cooperation of different stakeholders. Open standards and protocols guarantee global technical interoperability. In principle, this is the foundation that allows all parts of the Internet to communicate directly with each other. It is this logic of decentralized control that is meant to secure the free flow of information. When the need for coordination emerges, the preferred mode is to do so through open and voluntary multistakeholder governance.

The second vision aims to structure the Internet around instances of centralized authority. This vision is reflected in attempts to replicate the traditional structures of the Westphalian state order digitally. On this account, states are the prime political units and, thus, their authority should also extend to the digital sphere, which is structured along the territorial borders of states. Accordingly, the Internet is understood as a network of sovereign state networks. In this network, users cannot connect directly to each other but need to use state-controlled gateways. As part of their external sovereignty, it is up to the states to decide whether and how to open these gate-ways for exchanges with other networks. The institutional blueprint for this vision of the Internet is the traditional system of global telephone communication where national telecommunications were subject to state authority and linked with each other based on state treaties.

The distinction between these two visions of the Internet is useful because it highlights the conceptual alternatives, and, thus, also helps to understand many of the long-standing political conflicts in Internet Governance. Yet, political practice does not fit this clear-cut distinction. Whatever their public rhetoric may suggest, few states are fully committed to one of the two visions. Even the strongest proponents of open standards and multistakeholder governance often enough insist on their own national sovereignty also in matters of Internet Governance. Vice versa, even within states committed to the state-centred vision of Internet Governance, there are societal actors pushing in the other direction.

Multiple Nets: The Threat of Fragmentation

For a long time, the clash of the two visions has focused on two global institutions: The Internet Corporation for Assigned Names and Numbers (ICANN) and the International Telecommunication Union (ITU). The proponents of the first vision see ICANN as the quintessential embodiment of their commitment to open standards and multi-stakeholder governance. In contrast, those states proposing a more state-centred control of the Internet perceive the ITU as the rightful place of authority in matters of Internet Governance.

What has changed is that a growing number of states explore alternative ways of realizing the state-centred model of Internet Governance. They focus particularly on disentangling their national infrastructure as much as possible from the global infrastructure. They do

so by creating national Intranets that are only connected to the global Internet through state-controlled border-gateways. This process of deliberate fragmentation takes place on all levels of the infrastructure: from basic protocols for addressing and data transfer to physical infrastructure such as landlines, undersea cables, mobile networks – and, possibly, as a next step, Internet satellites in lower earth orbit.

For many states, this focus on the infrastructure is attractive because it effectively circumvents the stalemate in the institutional debates about the respective roles of ICANN and ITU. Crucially, unlike with these global institutional debates, no one can stop states from pursuing this path.

It is not only states, however, who drive the fragmentation of the Internet. The growing concentration of economic power in the hands of transnational tech companies also brings with it the prospect of entire networks controlled by these companies. In fact, many of the big tech companies increasingly invest in creating their own physical infrastructures, as well as in developing their own standards and protocols. This expands the control of these companies over their users' interactions with other users, other networks, as well as other companies.

It is unlikely that fragmentation will lead to the collapse of all global communication. Certainly, technical ways will be found to enable an exchange across the borders of different networks – just as it is possible today to connect to the Internet in China or to services within the Tor network.

Yet, fragmentation of the Internet's infrastructure will mean a considerable shift of power in favour of new, and old, gatekeepers. Already, states and private companies try to control what happens within "their" subnetworks. However, most of this is still happening at the level of Internet applications. These applications rely on the shared infrastructure of protocols and standards. Neither states nor private companies can fully control this part of the infrastructure. Citizens, thus, have different means to evade state control and censorship. And even powerful companies cannot prevent competitors from challenging them on the basis of a common technical infrastructure. If, however, states or companies were to control the infrastructure level too, they would be in a position to close down these remaining spaces of political freedom and economic competition.

Defending a free, open and truly global Internet

Many states routinely commit to a free and open Internet, and to the free flow of data. For example, in their final declaration, the participants of this year's G20 Ministerial Meeting on Trade and Digital Economy in Tsukuba, Japan, expressed their commitment to multistakeholder formats such as the IGF as a crucial element for the global digital society. They explicitly linked this commitment to the global spread of the digital economy and the need for interoperability. The G7 "Biarritz Strategy for an Open, Free and Secure Digital Transformation" follows along this path, emphasizing the importance of "cross-border flow of data, information, ideas and knowledge". The strategy acknowledges that this global exchange raises complicated political and economic issues and encourages efforts towards interoperability of different legal frameworks.

These statements are positive signs. They show that despite all the political differences that we witness today, it is still possible to convince large parts of the international community of the benefits of a truly global digital society.

Such abstract commitments, however, can be interpreted very differently. Indeed, one can also read them as compatible with a world of multiple nets whose separate infrastructures are owned, operated and controlled by powerful states and private companies. The challenge, thus, is to transform these abstract commitments into concrete and sustainable actions to preserve the Internet as an open and free global communications platform. This is not a task that can or should be carried out by states alone. Yet, it is the responsibility of states to create political conditions, domestically and globally, that enable private actors to do their part.

1 Preserve the Internet's public core

It is legitimate for states to extend their authority to the digital sphere. Yet, they should not do so at the expense of a global infrastructure that benefits all.

There is a growing consensus that states should refrain from attacking the Internet's public core. The Global Commission on the Stability of Cyberspace (GCSC) has proposed the principle of "non-interference with the public core", and many states have committed to this principle. Essentially, the idea is that states should refrain from any attacks on those systems necessary for addressing and routing.

As important as this principle of non-interference is, those states that want to defend a free and truly global Internet should do more. In particular, they should also refrain from misusing the Internet's public core for their purposes. When states exploit weaknesses in the addressing and routing systems to carry out attacks against other states (e.g. BGP hijacking), or when they use these systems for surveillance and espionage, they thereby erode trust in these systems. This directly contradicts the goal of preserving the Internet's public core.

2 Protect ICANN's core functions, and recognize the organization's limits

ICANN provides crucial coordination services regarding the allocation of IP addresses and domain names. Since 2016, it has also assumed responsibility for the DNS root zone by integrating the Internet Assigned Numbers Authority (IANA). Through these activities, ICANN maintains some of the most important elements of the Internet's global technical foundations. Regarding these core functions, ICANN is widely perceived as legitimate – and should be defended by all those who want to preserve a truly global Internet. Indeed, having a unified addressing and routing scheme is necessary to further deepen the kind of cross-border data flow that the G7 Biarritz strategy calls for.

Defending ICANN, however, will also require recognizing the organization's limits. In particular, it must be accepted that ICANN does not have the legitimacy to decide on controversial political issues. The conflicts about the compliance of the WHOIS system with European data protection laws, or the ongoing debate about the allocation of the AMAZON domain illustrate the limits of ICANN's mandate. It will not be possible for ICANN to avoid all such controversies. Yet, in order to ensure that ICANN can continue to provide its core services, all stakeholders, as well as the organization itself, should resist the temptation to carry out political controversies within ICANN.

3 Support efforts to increase the reliability and security of the Internet's global foundations

The way we use the Internet evolves rapidly. This also creates new demands for global technical foundations. In order to defend these foundations, it is also necessary to continuously update the Internet's basic standards and protocols. The development of Internet protocols and standards takes place in multistakeholder institutions such as the Internet Engineering Task Force (IETF) or the World Wide Web Consortium (W3C). These institutions provide fora that allow for expert exchanges and produce standards that are freely available for everyone to use.

States should support the work of these institutions. They can do so directly by providing financial support, by sending their own experts, or by publicly defending these institutions. Moreover, in many cases, there are well-developed proposals for increasing the reliability and security of the Internet's global infrastructure. States should not prescribe in detail which of these solutions to adopt. Yet, they should promote efforts by private actors as well as public institutions to implement such new solutions. States can do so, for instance, by financially supporting such efforts, or by facilitating an exchange on the experiences with such new solutions.

Support for multistakeholder standard development, however, can also come in the form of addressing some of the long-standing criticisms that these institutions face: For instance, states can actively support broader participation by civil society and academia as a counter-weight to the dominance of private companies. Further, states can support efforts to make the work of these institutions more transparent and accessible.

Dr. Daniel Voelsen is Associate in the Global Issues Division.

SWP
Stiftung Wissenschaft und Politik
German Institute for International and Security Affairs

Ludwigkirchplatz 3–4
10719 Berlin
Telephone +49 30 880 07-0
Fax +49 30 880 07-100
www.swp-berlin.org
swp@swp-berlin.org