: Global Governance Spotlight
4 | 2020

sef:

An Update for the Internet
Reforming global digital cooperation in 2021

Matthias C. Kettemann
Alexandra Paulus

In 2021, the international community has the chance to radically reform global digital governance. The aim should be to guarantee a global, open, free, stable and secure Internet while promoting responsible State behaviour in cyberspace. Mapping the two strands of this policy – improving models for cooperation on the collective development of Internet governance, and implementing the cyber norms already adopted – is a matter for the United Nations (UN). A reformed architecture for digital cooperation has the potential to make Internet governance more inclusive and effective, while new mechanisms can help to advance the currently divided debate on cyber norms and enhance the predictability of State behaviour in cyberspace. The promising proposals already put forward are the focus of this Global Governance Spotlight.

UN Norms of Responsible State Behaviour in Cyberspace

1 Interstate cooperation on security	2 Consider all relevant information	3 Prevent misuse of ICTs in your territory	4 Cooperate to stop crime & terrorism
5 Respect human rights & privacy	6 Do not damage critical infrastructure	7 Protect critical infrastructure	8 Respond to requests for assistance
9 Ensure supply chain security	10 Report ICT vulnerabilities	11 Do no harm to emergency response teams	Note: 3, 6 and 11 are limiting norms, all others positive obligations.

Sources: Development and Peace Foundation (sef:), https://www.dfat.gov.au/sites/default/files/un-norms-responsible-bookmark.pdf and https://undocs.org/A/70/174.

It is the right time for these reforms: the Internet is still evolving at a rapid pace; power struggles in cyberspace have intensified in recent years; and some states are even attempting to mark out their "territory" on the Internet. Growing amounts of data, the deployment of machine learning to optimise its mining, algorithms that draw users' attention to specific platform content and the deployment of the Internet of Things all show how important it is for policy-making to keep pace. Where do we stand with regard to the protection of individual rights in data-driven platform economies? What about cybersecurity in networked systems, or the impact of Internet-mediated communication on social cohesion? The existing architecture for cooperation in this field dates back to the formation of the Internet Governance Forum (IGF) in 2005. Key cyber norm-setting processes take place in the Group of Governmental Experts (GGE), a working group first convened in 2003. Almost 20 years is a long time for the Internet.

In recent years, different tracks have emerged in the global governance of cyberspace. Within the United Nations General Assembly, cybersecurity issues are a matter for the First Committee, while the Second Committee examines the economic and social dimensions of Internet policy and the Third Committee deals with human rights aspects. In addition, substantial contributions are made by specialised agencies of the United Nations. The annual meeting

of the IGF, which brings together stakeholders from politics, the private sector and civil society, serves as a kind of focal point for ideas, but has been unable, thus far, to help cluster and consolidate the various processes that aim to regulate cyberspace. As a result, it has attracted growing criticism for being too Western-oriented, too elitist, lacking in sustainability – a kind of talking shop for a select group.

New architectures for cyber cooperation

In 2018, UN Secretary-General António Guterres recognised the need to update the architecture for global digital cooperation and convened a High-level Panel for this purpose. After the panel had presented its report in 2019, Germany and the United Arab Emirates were tasked with conducting multi-stakeholder consultation processes across the globe with a view to developing options for implementation of those recommendations that related to the future of the IGF. After open consultations during the first six months of 2020, which set new standards for inclusion and allowed the voices of citizens to be heard, Germany and the UAE presented an options paper on the future of global digital cooperation to the Secretary-General in autumn 2020. The proposals set out in the paper will substantially influence the institutional reform of Internet governance. As the basic concept, the IGF, as the central discussion platform for all stakeholders around the Internet, should be strengthened and developed into a more inclusive and effective format ("IGF+"). The new forum should prioritise inputs from national and regional IGFs (such as the European Dialogue on Internet Governance [EuroDIG] and IGF Germany) and focus on achieving practical results such as policy recommendations and outcome reports. There should be more involvement of representatives of the Global South; capacity development will therefore be required. Direct institutional links to the UN should be strengthened by associating the IGF Secretariat with the Office of the United Nations Secretary-General. In terms of its agenda, the IGF+ should link up global digital governance processes and create synergies among the UN specialised agencies. Responsiveness to citizens is important for the legitimacy of Internet governance, so MPs and government representatives should be involved to a much greater extent than before, not least in order to ensure linkage with topics on national legislative agendas.

More rules for a more stable system

Alongside the global architecture for digital cooperation, a state-led process at the UN aims to define and elaborate cyber norms, i.e. agreed-upon international standards for responsible State behaviour in relation to information and communication technologies (ICTs). These norms can entail positive obligations for governments, requiring them, for example, to share information about threats with other states, or establishing limits to State behaviour by, inter alia, prohibiting governments from carrying out cyber operations targeting other countries' critical infrastructures.

Cyber norms receive increased attention because other types of regulatory mechanism are difficult to apply to ICTs: an international treaty would be challenging to enforce, as it would require the attribution of cyber operations to their perpetrators – almost impossible to achieve beyond reasonable doubt. In recent years, there have been repeated efforts to extend traditional arms control to cyberspace. However, these efforts have failed because malware – often described incorrectly as "cyberweapons" – is different from conventional and nuclear weapons. As it is, cyber norms are the only available mechanism to advance towards the goal of rules-based digital governance.

Cyber norms in focus

Although businesses and civil society organisations have played a key role in the debate via private sector initiatives such as Tech Accord, initiated by Microsoft, and multi-stakeholder formats like the Paris Call for Trust and Security in Cyberspace, the key discussions about cyber norms are currently taking place within the UN framework. The topic is dealt with by the First Committee, which is responsible for disarmament and international security. In 2003, the UN General Assembly set up the first Group of Governmental Experts (GGE), as mentioned above, to deal with cybersecurity; further mandates followed. These representatives of initially 15 and later 25 states were tasked with raising awareness among social stakeholders for cybersecurity issues and developing joint definitions and cyber norms. The three GGE reports were important milestones on the path towards cyber norms: They documented the agreement that ICTs can pose a threat to international security (2010) and that international law is applicable in cyberspace (2013); finally, a set of 11 cyber norms was presented (see Figure 1), which, according to the United Nations General Assembly, should guide the behaviour of all states (2015). Collectively, these three GGE reports constitute the acquis for cyber security and form the basis for international efforts to establish cyber (security) norms.

Political differences cause division

This progress was followed by a perceptible loss of momentum in the UN debate on cyber norms. The GGEs always meet behind closed doors and only produce a final report if all members reach con-

sensus. This proved impossible under Germany's lead in 2017, when dissent hindered outcomes. The disagreement concerned the application of certain provisions of international law, but really emanated from fundamental differences between Russia (and, less vocally and increasingly distanced, China) on the one side, and the US and like-minded countries, including the EU member states, on the other. These differences were likely rooted in the broader dispute over trade and political dominance but spilled over into the debate on cyber norms.

In 2019, these differences culminated in the division of the UN dialogue on cyber norms into two separate processes: alongside the GGE, a new format, the Open-ended working group on developments in the field of information and telecommunications in the context of international security (OEWG), was established at Russia's initiative. Unlike the GGE, it meets in public and is open to all member states as well as to non-governmental organisations with accredited consultative status with the United Nations Economic and Social Council (ECOSOC). Diplomats from the US, the EU and like-minded countries participate in both forums, whereas Russia and China focus their efforts on the OEWG. The publication of the OEWG's report, scheduled for 2020, was postponed until 2021 due to the COVID-19 pandemic.

Assuming that a consensus is reached, the sixth GGE is due to submit its final report to the General Assembly in 2021. The sixth GGE was established on the basis of a resolution sponsored by the US and is therefore perceived by some countries as Western-dominated. At present, little is known about the status of the negotiations. According to some reports, the group is currently negotiating commentaries that explain each of the 11 norms (see Figure 1) in more detail and developing guidance on implementing the norms.

No prospect of bridging the divide

The division of the UN debate on cyber norms into two parallel processes is problematic. This dual-track approach ties up human and financial resources that some countries, particularly in the Global South, struggle to mobilise. Furthermore, the relationship between the two formats has yet to be clarified. Although both forums are meant to develop the acquis further, some states believe that the OEWG could potentially amend it – although the discussions do not appear to be heading in that direction at present. In a worst case, the division could lead to a loss of credibility for the UN dialogue on cyber norms.

In view of these problems, in October 2020, a group of countries led by France and Egypt proposed a Programme of Action (PoA) to replace the GGE and the OEWG. This PoA would combine a multi-stakeholder dialogue on the further development of cyber norms with specialised discussions on aspects such as implementation. However, on 9 November 2020 – before there was an opportunity to formally propose the establishment of such a forum – the First Committee approved a draft resolution, sponsored by Russia, to establish a new open ended working group for the period 2021-2025. At the same time, the Committee adopted a second resolution, sponsored by the US and the EU member states, which proposed that a decision on the future of the cyber norms debate be postponed until after the UNGGE and OEWG had presented their findings to the General Assembly, thereby implicitly creating scope for a new format such as the PoA. A Non-Paper by Germany and five other EU member states, dated 19 November 2020, also expresses support for a PoA. In theory, it is possible that the strands of the debate will converge in the new OEWG from 2021 onwards, but, in view of the ongoing political differences, this seems unlikely. In terms of content, these two resolutions on the future of the UN debate on cyber norms are contradictory, highlighting and reinforcing the ongoing divide.

2021: Utilising the momentum …

The foundations of Internet governance have existed for 15 years, but in 2020, significant progress was achieved in relation to the global cooperation architecture, consolidation of cyber norms and cyber diplomacy. This momentum should be maintained while mitigating the impacts of parallel processes.

If 2020 was all about the theory, 2021 may be the year for practical action. The positive proposals for an IGF+ should be implemented swiftly on the basis of the German options paper. No new agreements are needed for this. The UN Secretary-General and his Multistakeholder Advisory Group can implement all the recommendations on the basis of existing mandates: more integration of the Global South, an expanded secretariat, more contact with the world's parliamentarians, and a team to develop recommendations. Poland, which will host the IGF in 2021, had already made very good progress with planning the meeting by the time the coronavirus pandemic delayed matters. This means that there is more time to lay the groundwork for the IGF+ – in consultation with countries such as Brazil, Germany, Sweden, France and Switzerland, which have consistently advocated for a stronger IGF.

… and innovative implementation instruments

In the global debate about cyber norms, Germany and Europe should adopt a dual-track approach, in the best sense of the word, in 2021. Constructive progress on refining the existing norms or developing new ones can only be expected once the fundamental

political differences between both camps have been overcome. As long as a majority of countries are interested in continuing the dialogue within the UN framework, Germany and Europe should keep the channels of communication open; their focus, however, should be on achieving progress in implementing existing cyber norms. There is a consensus within the international community that more confidence-building measures for cybersecurity are required, along with the integration of capacity-building into international development cooperation. Regional organisations such as the Organization for Security and Co-operation in Europe (OSCE) und networks like the Global Forum on Cyber Expertise (GFCE) have already established processes and instruments to address both these aspects and should be given more support.

There are still no established instruments for the implementation of cyber norms; however, there are several innovative proposals which Germany and Europe should advance in 2021. Several countries, including Canada and Australia, have published reports in which they show how they are interpreting and implementing the 11 norms. Australia and Mexico have produced a voluntary survey on national implementation of cyber norms. Participating countries will report regularly on the action they are taking, including their interpretations of how international law applies to the use of ICTs; they will also provide information on confidence-building measures and international cooperation in capacity development. And lastly, Singapore, together with other members of the Association of Southeast Asian Nations (ASEAN) and with support from the United Nations Office for Disarmament Affairs (UNODA), will produce a checklist of the steps that countries will need to take to implement the cyber norms. The diverse focal points of these three worthy proposals – encouraging all states to participate, promoting international comparability and giving consideration to the specific needs of developing countries – can do much to advance the debate about cyber norms so that the divisions within the process can be overcome in the long term.

2021 offers an opportunity not only to revitalise the IGF but also to use innovative instruments to narrow the cyber norm gap. This is especially important in order to keep pace with the rapid evolution of information and communication technologies and to uphold the commitment to the goal, described at the start of this paper, of a global, open, free, stable and secure Internet that serves the interests of all stakeholders.

Authors

PD Dr Matthias C. Kettemann, LL.M. (Harvard) | a visiting professor at the University of Jena, is leader of various research groups, focusing on the law of the Internet, at the Leibniz Institute for Media Research | Hans-Bredow-Institut, Humboldt Institute for Internet and Society, Berlin, and the Sustainable Computing Lab at Vienna University of Economics and Business. @MCKettemann

Alexandra Paulus | a Non-resident Fellow for International Cyber Security Policy at Stiftung Neue Verantwortung (SNV). She is currently pursuing a Ph.D. in Political Science at Chemnitz University of Technology in Germany, analysing how states shape international cyber norms, focusing on the case of Brazil. @ale_paulus

References

UN General Assembly (2015), Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: Note by the Secretary-General (A/70/174) (includes the UNGGE's report with 11 cyber norms), https://undocs.org/A/70/174, 22.07.2015.

Report of the UN Secretary-General's High-level Panel on Digital Cooperation, The Age of Digital Interdependence, June 2019, https://digitalcooperation.org/wp-content/uploads/2019/06/DigitalCooperation-report-web-FINAL-1.pdf.

Road map for digital cooperation: implementation of the recommendations of the High-level Panel on Digital Cooperation – Report of the Secretary-General, UN Doc. A/74/821, 29.5.2020.

Germany (BMWi)/UAE, Options for the Future of Global Digital Cooperation, 3.9.2020, https://www.global-cooperation.digital/GCD/Navigation/EN/The-Options-Paper/the-options-paper.html.

Germany (Federal Foreign Office), Non-Paper on EU Cyber Diplomacy by Estonia, France, Germany, Poland, Portugal and Slovenia, 19.11.2020, https://www.auswaertiges-amt.de/blob/2418160/206b3bf9aa4ef45a2887399231840d23/201119-non-paper-pdf-data.pdf.

Imprint

The Development and Peace Foundation (sef:) was founded in 1986 on the initiative of Willy Brandt. As a cross-party and non-profit-making organisation, the sef: provides an international high-level forum for shared thinking on urgent peace and development issues.

Global Governance Spotlight is a policy-oriented series whose purpose is to critique international negotiation processes from a global governance perspective.

Published by
Development and Peace Foundation (sef:)/
Stiftung Entwicklung und Frieden (sef:)
Dechenstr. 2 : 53115 Bonn : Germany
Phone +49 (0)228 959 25-0 : Fax -99
sef@sef-bonn.org : @sefbonn
www.sef-bonn.org

Editor
Larissa Neubauer

Translation
Hillary Crowe

Design Basic Concept
Pitch Black Graphic Design
Berlin/Rotterdam

Layout
Gerhard Süß-Jung

Contents do not necessarily reflect the views of the publisher.

ISSN 2566-624X