My name is Wolfgang Kleinwaechter. I am a retired professor for Internet Policy and Regulation of the University of Aarhus. I was a member of the ICANN Board and a Commissioner in the Global Commission on Stability in Cyberspace. But I am speaking here in my personal capacity. I have three points.

1. In his report about the first „informal OEWG consultations“ (December 2019) Ambassador David Koh from Singapore, wrote: “The different perspectives provided by States, industry, civil society and academia were enriching and the concrete ideas put forward were constructive and innovative“ Also the final OEWG report (March 2021) recognized „the expertise, knowledge and experience shared by representatives from inter-governmental organizations, regional organizations, civil society, the private sector, academia and the technical community.“ UN-Resolution 75/240 (December 2021) says that the OEWG „may decide to interact, as appropriate, with other interested parties, including businesses, non-governmental organizations and academia.“ It seems that there is now a general agreement that security in cyberspace can be achieved only, if all stakeholders contribute in their respective roles and work hand in hand. However, the details on the „how“ remain unclear. There are different ideas as to what is „appropriate“ and how to organize the „interaction.“ The „How“ is about access and speaking rights for business, civil society and the technical community. It is about the possibility of non-state actors to table their own proposals or to comment officially on governmental drafts. It is about the duty of governments to rationalize their decisions in public. Some governments want to keep the non-state actors at arm’s length, others have no problems with including them in formal discussions. This looks like a procedural issues. But the way in which non-state actors will be included in the forthcoming OEWG negotiations will have substantial effects on possible outcomes. Insofar my first point is: Mr Chairman, tear down this wall between informal multistakeholder consultations and intergovernmental negotiations. Nobody questions the special role of governments for a secure cyberspace. But in cyberspace we do have more the 193 national governments. There are thousands of technical experts, millions of businesses and billions of Internet users. Without including their perspectives into your discussions, you will fail to reach sustainable results.

2. My second point refers to one of the recommendation of the Global Commission on Stability in Cyberspace (GCSC) to protect the public core of the Internet. In our final report we proposed the following norm: „State and non-state actors should neither conduct nor knowingly allow activity that intentionally and substantially damages the general availability or integrity of the public core of the Internet, and therefore the stability of cyberspace.“ We did see the „public core of the Internet“ as something like the „common heritage of mankind“ which belongs to everybody. Our recommendations did say, don’t pull the management of critical Internet resources into geo-political conflicts. Domainnames, IP adresses, Root Servers are the air of
the Internet. There is no „Chinese Air“ or „American Air“ in the real world, there is only clean and fresh air or polluted air. In our complicated world, full with traditional and new conflicts, including this incredible sad and illegal Russian aggression of Ukraine, there is a risk, that the „virtual Internet air“ gets polluted. My plea is, keep the public core of the Internet out of this political conflicts. The statements made by leaders of the technical community as ICANN, RIPE NCC and ISOC are well drafted. Please, take not i fit. If you can offer help, send it to the civil society Internet organisations in both Ukraine und Russia as well to other underserved communites. This will strengthen the multistakeholder model, not undermine it. And by the way, if some governments have mistrust into the multistakeholder approach, if they have doubts whether the public core of the Internet can be managed by the global multistakeholder community, they should remember the experiences of the Covid-19 Pandemic since early 2020. The Pandemic triggered an explosive growth of the use of the Internet as homeoffice, online shopping, distance learning and zoom conferencing etc. Internet traffic doubled and trippled globally, but the public core of the Internet remained stable. It delivered, what was needed for all stakholders, regardless of frontiers. This was an incredible stressfest for the multistakeholder approach. But the results were very encouraging. Thy system worked. There was no shortage on domain names or IP adresses, the root and name server system, the routing and peering, that is the whole mechanism to manage the public Internet core, did work.

3. My final point is related to the IGF. As you know, next week the Finish Permanent Mission in New York will host high level consultations about the future of the Internet Governance Forum (IGF). In his „Roadmap on Digital Cooperation“ UN Secretary General Antonio Guterres has proposed to enhance the IGF into an IGF+, inter alia by introducing a Special UN Tech Envoy, a Leadership Panel and a Parliamentarian Track. The IGF is not a decision making body. It has demonstrated since 2006, that it is a excellent multistakeholder discussion platfform. What is missing are links to the various international platforms, where decisions are made. My recommendation to the OEWG is to reach out to the IGF. There is an „IGF Best Practice Forum on Cybersecurity“ (BPF CyberSec), which discusses all your agenda items. And there is an „IGF Dynamic Coalition on Schools of Internet Governance“ (DC.SIG@IGF), where dozens of educational institutions are collaborating to enhance cyber capacity building. There is no need to reinvent the wheel or to duplicate what is already availabe. As an academic person, I have observed over the years that there is a special knowledge gap between law makers and code makers. Governmental experts and parliamentarians, responsible for drafting legislation of Internet related public policy issues, very often do not have the needed technical expertise to understand the unintended side effects of the laws they propose for adotion. On the other side, technicians are often not aware, that their codes and protocols have political, economic, social and cultural implications. To build bridges between those two communites should be a key guideline for your agenda item „cyber capacity building“. Our Summer School on Internet Governance in Meissen/Germany (EURO-SSIG), the first which started special high level courses already 16 years ago, is planning a new high level course to bring governmental cyberambassadors and leaders of the technical community together in January 2023. This is an offer and I hope you will make use of it.