Honorable Chair,

cyber peace is not only the central goal of this group. It is also essential for safeguarding a peaceful future for this planet.

Germany is fully aligned with the statement delivered by the European Union and would like to make the following remarks in a national capacity.

Honorable Chair, Germany wishes to thank you and your team for the excellent preparation of this session, which is set to start in one of the gravest moments of our times. We are meeting at a moment when our world is shaken by the terrible war of aggression which is raged by Russia against Ukraine.

Germany condemns Russia’s military invasion of Ukraine in the strongest possible terms. Russia’s aggression constitutes an unacceptable breach of international law and the UN Charta, violating the fundamental principles of state sovereignty, the territorial integrity of states and peaceful conduct among states.

In preparation of Russia’s military invasion we have witnessed an unprecedented use of malicious cyber instruments by Russian state and state sponsored actors. These attacks are still ongoing as the war rages on.

These malicious cyber activities present a massive menace to the security and accessibility of online communication in Ukraine as well as to global cyber peace as we are already seeing alarming spill-over effects of this war into the digital networks of many other state.

These attacks are designed by Russia to erode the existence of Ukraine as a functioning state by directly attacking key digital infrastructure of the Ukrainian government. They are also conducted with a view towards
destroying the digital base of Ukraine’s civil society, media and economy.

While waging cyber war against Ukraine, Russia is also limiting online access to information, social media platforms and other forms of online communication for its own citizens while misusing online media for a fierce and gigantic information war with the intention of concealing the bloody online and offline realities of this war.

The cyber operations put in place by Russia against Ukraine and towards its own population are in flagrant violation of the United Nations framework of responsible state behavior in cyberspace – a framework, which has evolved over many laborious years of negotiations in UN GGEs and has since been endorsed by all UN members including Russia in the General Assembly.

The 2015 UN recommendations for voluntary, non-binding norms have become a much needed world standard to secure cyber peace in our increasingly digitalized world.

There can only be cyber peace if cyber norms are respected. To secure, enforce and strengthen those cyber norms is the goal of this working group. The kind of blatant, illegal misuse of cyberspace we have witnessed in the context of the Ukraine crisis is a severe setback in achieving this goal. Russia’s cyber aggression in the context of its war against Ukraine will have a severe and lasting impact on our work.

The cyber-attacks suffered by Ukraine also underline the importance of the work ahead of us and the relevance of this groups mandate to elaborate universally acceptable guidance on responsible state conduct in cyberspace.

The repeated, massive cyber-incidents of the past days, weeks and months shine a dark light on what irresponsible state actors are bound to do again and again if we fail to secure cyberspace. We have reason to fear that Russia will launch more severe cyber-attacks in the future, not only in Ukraine.
This is why we want to encourage this group to further develop the rules, norms and principles of responsible state behavior and their implementation and, if necessary, to introduce changes to them or elaborate additional rules of behavior.

It is of key importance that the Open Ended Working Group does this with the involvement of the multi-stakeholder community.

Germany fully supports the repeated calls for ensuring an adequate participation of multiple stakeholders in the sessions of the Open Ended Working Group.

Germany also wishes to thank you, honorable chair, for your unwavering endeavours to find a compromise solution to this question which can be supported by all states present.

The internet is neither owned nor controlled by states. It is a public domain which is managed and advanced by a highly complex and efficient range of actors representing industry, civil society and governments.

The participation in this Open Ended Working Group should be fully reflective of this reality. In order to have a real and cyber world impact this group needs to have full access to the expertise and the technical know-how of these multiple stakeholders. Last week’s informal consultation of multiple stakeholders conducted by you, Honorable Chair, has once again proven their high level of interest and relevance for our work.

This group does not operate in a void. Its recommendations in terms of voluntary norms of state behavior, confidence building measures or cyber capacity building must be fully actionable in the context of the world’s IT networks.

Germany does not see how this can be assured without offering the relevant multiple stakeholders the opportunity for adequate participation in the OEWG.
A number of acceptable proposals have been put forward to bring multi-stakeholder participation to an adequate level – both by states and by you, Honorable Chair.

Germany calls on states to show flexibility and converge on a compromise solution that ensures transparency and adequate participation.

This key issue should be resolved as soon as possible to allow us to fully focus our energy on the wide range of pressing cybersecurity items on our agenda.

Until the modalities have agreed our work on the substantial items should continue on an informal basis as is UN practice.

Thank you Mr. Chair for your tireless commitment to this process. Let me assure you that Germany remains in every way ready to engage constructively in the work of this Open Ended Working Group and to ensure this group can make meaningful contributions towards cyber peace.