German Statement at the July OEWG, Agenda Item 5, Section B)

(Continue to study, with a view to promoting common understandings, existing and potential threats in the sphere of information security, inter alia, data security, and possible cooperative measures to prevent and counter such threats)

Honorable Chair,

Germany is fully aligned with the statement of the EU as well as with the statement of the Czech Republic and Canada on multi-stakeholder participation.

Germany wishes to thank the Chair and his team for compiling the draft progress report, which we see as a sound basis for discussion. We welcome the action-oriented structure focusing on next steps and concrete initiatives for implementing the existing global framework of responsible state behavior in cyberspace.

We have a number of suggestions for the text of the section on existing and potential threats:

Germany considers it essential to use this section to describe and raise full awareness about the existing threat landscape and to focus discussions in the OEWG on the most harmful threats to international peace and security seen today.

Since the last session we have seen destabilizing trends in cyberspace continue, most strikingly the use of cyber-attacks by Russia in its war of aggression against Ukraine. Reverberating effects of these attacks can be felt in networks all over Europe including in Germany.

Russia’s action are in flagrant violation of international law and the UN framework of responsible state behavior in cyberspace, which was agreed in this building precisely to ensure that cyberspace is not misused as a domain of warfare.

The spill-over effects we are seeing as a direct result of Russia’s cyberwar against Ukraine have had direct disruptive effects on
Germany’s critical infrastructure, namely our renewable energy sector as well as key distributors of fuel.

Another concerning development is the increase of hacktivism in the context of the war in Ukraine. Hacktivists aggravate risks and instability and have added another level of unpredictability to cyberspace. Cybercrime and in particular Ransomware attacks continue at a level that can pose direct threats to international peace and stability as was highlighted this morning by Costa Rica and further outlined by Brazil.

With regards to the First draft, Germany suggests including direct references to military use of ICTs, hacktivism and cybercrime in the section summarizing current threats. Germany also supports proposal by the United States to cover new threats posed by emerging technologies in this section.

With regards to the *the rules, norms and principles section*, Germany supports the proposals in the draft annual report concerning transparency and information-sharing regarding national views on specific norms, rules and principles. Such open discussions should aim at developing a joint understanding of these norms and at protecting international peace and security.

As an action point, Germany would like to propose a concrete reference in the report regarding attribution. Jointly with other states we have pointed out the high value we see in deepening inter-state exchange and the sharing of best practices regarding the attribution of cyber incidents. Attribution is not only a key instrument to ensure accountability, but also essential to prevent future malicious cyber activities as already underlined in the report of the 2021 GGE. As such, Germany would support action-oriented recommendations in para 8e) of this section.

In closing, let me assure you, that Germany is ready to engage constructively on finalizing a substantive progress report by the end of this week in order to guide the further OEWG process in a transparent and action-oriented manner and to strengthen international peace and stability in cyberspace at a time when we find that both peace and
stability are being challenged by the acute security crisis in Europe. Thank you.