German Statement at the March OEWG, Agenda Item 5d)

(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 fully aligned with the statement of the EU and wishes to add the following points in a national capacity.

Guarding cyber security in today’s interconnected work is the pre-condition for the functioning of our states, economies and societies. It is also the pre-condition for international peace and security. For this reason it is important that this group also focuses on analyzing the current threat landscape.

With regards to current threats Germany is seeing a wide range of cyber challenges to its national security originating from state and non-state actors. Threats can be categorized as targeting state interests such as protection of our democratic processes, the protection of government data including that of our citizens.

Private sector threats include cyber-attacks against critical infrastructure, economic espionage with a focus on hi tech companies and ransomware attacks.

However the most concerning current cyber threats for Germany are spill-over effects from the cyber-attacks which Russia continues to launch on Ukraine in the context of its war of aggression.

What concerns us most is that we see these spill-over-effects causing disruption to critical infrastructure in Germany, most notably our energy sector.

We are also seeing a concerning wave of hacktivism in the context of the war in Ukraine, adding another level of risks and instability to our networks.
We should be mindful of the interconnectedness of our world. The Non-Petya-attack has sent a warning call of how a major cyber-attack can cause massive damage across continents. The current level of cyber-attacks and hacktivism seen in the context of Russia’s war against Ukraine is clearly putting networks worldwide at risk.

This makes it imperative for us in the OEWG as the central UN body dealing with cybersecurity and tasked with elaborating solutions to advance stability and security in cyberspace to focus on the cyber-effects of the war in Ukraine on the world community at large.

In this volatile situation and responding to the chair’s guiding questions Germany sees it as necessary to advance our discussions towards measures that allow states around the world to strengthen their national cybersecurity – be it via cyber capacity building, sharing of best-practices or dedicated cyber security training.

Confidence building measures can make a direct contribution to security and stability in this complex landscape and are more relevant than ever in the fragile situation of international security we find ourselves in. Germany looks forward to sharing more thoughts on this under the dedicated agenda item.

The UN and this OEWG can play a role in by promoting these cooperative measures and offering a platform for implementation as outlined by Under Secretary General Izumi Nakamitsu in her opening remarks. We look forward to defining this UN role more closely as part of the work of this group.

In reacting to the statements made by other delegations Germany welcomes the level of technical detail displayed applied by Malaysia in describing the evolving threat landscape, as well as the encouraging information on international cooperation shared by Jordan and the update on national cyber security measures given by Iraq. Germany also welcome the thoughts offered by the Republic of Korea on building an implementation architecture at the UN level.

Finally Germany whishes to make a request to secretariat: In addition to the explanations given by the chair could the secretariat circulate to
member states information in writing on the implications of the informal mode of this meeting and what this means for the status of our contributions made during this session. This could offer additional reassurance to member states that the work done during this week is fully recognized and will be reflected in any report or outcome document of this OEWG.