*Nedan följer en sammanfattning från sommaren om det senaste inom arbetsgruppen för cybersäkerhet. Sammanfattningen är skriven av ICC:s **Timea Suto**, Global Policy Lead.*

FOR INFO: Updates on UN OEWG on Cybersecurity

The 3rd Substantive Session of the OEWG took place on 25 – 29 July in New York. After four days of extensive conversations, member states reached the adoption of both the First Annual Progress Report of the OEWG and the Procedural Report of the OEWG. The report will now be presented to the General Assembly via the First Committee for adoption.

The main elements of the adopted report, as well as major sticking points during the discussions were:

Threats
While the report recognizes that the severity of cyberattacks is on the rise – especially as it relates to critical infrastructure (CI) – the report does not include specific reference to ransomware despite strong support by several member states for this to be considered by the OEWG.

Rules, norms and principle
The report includes strong language on security of supply chains, based on the 2021 GGE report. It also calls for more transparency measures on the implementation of norms through mechanisms such as surveying.

Divergences persist between delegations on whether the OEWG should be a venue to discuss the implementation of existing norms or creation of new norms. Ultimately, the report notes that the two are not mutually exclusive.

International law
Debate focused on the applicability of international humanitarian law in cyberspace. A number of states proposed a reference to international humanitarian law, including a specific mention of the International Committee of the Red Cross (ICRC).

States continue to express mixed views on the need for new legally binding obligations for state behaviour in cyberspace. A majority do not see the need for nor the feasibility of developing a new legal instrument, while a few see this as a priority for the OEWG.

Capacity building
Cyber capacity building continues to be a topic of great interest, including for the Chair and his team. Several calls were made for more focused discussions on capacity building at the upcoming sessions of the OEWG.

Confidence building measures (CBMs)
Several states voiced support for a clear reference to CERT-to-CERT communication between states as part of CBMs and establishing a PoC directory. States also called for more focused discussions on CBMs at the upcoming meetings of the OEWG. A major output of the report is the recommended next step to produce a global Points of Contact directory.

Regular Institutional Dialogue
The main point of debate was around the reference to the proposed cyber Programme of Action (PoA) and how the report should recommend using future OEWG sessions to discuss the PoA. In the end, the report includes a reference to the PoA, which although much broader than was originally proposed, includes a commitment for future focused discussions.

Participation by stakeholders
Several states expressed their disappointment with Russia's decision to veto certain non-governmental stakeholders' participation in the OEWG. Several of the same states also noted the importance of including stakeholders' input across all topics discussed by the OEWG.

For a more detailed overview of the meeting and the annual progress report, I recommend consulting this analysis prepared by Reaching Critical Will, the disarmament programme of the Women's International League for Peace and Freedom (WILPF).