Submission by ICT4Peace to the Open-Ended Working Group (OEWG) on security of and in the use of information and communications technologies 2021-2025[1]

As this new iteration of an OEWG on ICT use in the context of international security gets underway it is important to recall and build on progress made in the past. The First Committee mandate of the OEWG reminds all that its focus will remain on international peace and security and the implications for that primordial goal represented by ICT use on the part of both state and non-state actors.

There is wide recognition of the need in addressing the challenges posed by malicious activity in cyberspace to draw upon the views and contributions of all stakeholders. ICT4Peace has from the beginning advocated for equitable and meaningful provisions for relevant non-governmental stakeholders to participate in the work of the OEWG.

In our view, the OEWG should not await the end of its mandate to deliver an outcome but seek to generate discrete products during the course of its activity to address pressing topics in a timely fashion.

Following are some areas we deem merit priority attention:

- the lack of accountability;
- the impact on human security of malicious cyber activity;
- cyber capacity building and
- the UN's "institutional deficit" on cyber matters.

The lack of accountability[2]

In his *Securing our Common Future: An Agenda for Disarmament,* Secretary General Antonio Guterres stated "We must foster a culture of accountability and adherence to norms, rules and principles for responsible behaviour in cyberspace". Norms divorced from any mechanism to

[1] See Compilation of ICT4Peace inputs to the UN OEWG 2019 – 2021: https://ict4peace.org/wp-content/uploads/2021/04/ICT4Peace-2021-OEWG-Final-Report.pdf

[2]See ICT4Peace analysis: "The OEWG Final Report: Some Progress, Much Remains Unresolved» https://ict4peace.org/wp-content/uploads/2021/04/OEWG-FinalReportAnalysisMar212021PM.pdf

monitor their implementation are likely to yield meagre results. Sooner rather than later the OEWG should look to developing an accountability mechanism that will provide a common and equitable process to scrutinize state conduct. ICT4Peace has proposed a "Cyber Peer Review Mechanism" modeled on the Human Rights Council's Universal Periodic Mechanism that would provide a state-led process while allowing for input from non-governmental stakeholders.

The impact on Human Security

There is an emerging consensus that the OEWG should pursue a human-centric approach to its work while respecting its origins as a First Committee forum. We believe that the application of the "human security" concept is appropriate in this context as it highlights that individuals and communities frequently suffer from malicious cyber activity. Regrettably, the scope and magnitude of this activity including offensive cyber operations conducted by states has been steadily growing throughout the period that the UN has discussed norms of responsible state behaviour. A key norm among the eleven agreed to in 2015 is not targeting by cyber means critical infrastructure on which the public depends. Despite this agreed norm such infrastructure has been the target of damaging cyber operations.

ICT4Peace has therefore advocated that states possessing offensive cyber capabilities make a public pledge never to engage in operations directed against critical infrastructure. Such action would reinforce the strength of the original normative injunction and provide a transparent affirmation of a state's commitment to act responsibly in cyberspace. Similarly, ICT4Peace would endorse the call by the FIRST organization that "[cyber] incident responders should not be attacked and not be attacking"; an additional major norm of the 2015 consensus.

Cyber Capacity Building

ICT4Peace has consistently stressed the importance of building cyber capacity among all UN member states. This capacity should be viewed as going beyond issues of technical cyber security matters to include diplomatic capacity in order that states are able to participate meaningfully in the variety of international processes that are developing international cyber security policy. To encourage donors to come forward ICT4Peace together with Estonia and Switzerland have advocated for cyber capacity building programs to be granted Official Development Aid status via the OECD's Development Assistance Committee (DAC) and would ask the OEWG to take a similar stance and communicate it to the DAC members.

ICT4Peace has since 2014 carried out 29 Cybersecurity Policy and Diplomacy Courses in the ASEAN, OAS, OSCE, AU Regions and at the UN in New York and Geneva.

Overcoming the UN's Cyber "Institutional Deficit"

It has been 24 years since ICT use and implications for international security was put on the UN General Assembly's agenda. While discussion of cyber security has progressed by means of UN Groups of Governmental Experts (GGE) and Open-Ended Working Groups (OEWG) it is fair to

say that these deliberations have not kept pace with the militarization of cyberspace and the growth of malicious cyber activity. If the UN is to effectively come to grips with the challenges of cyber security, it will need to move from temporary *ad hoc* arrangements and establish an on-going forum for handling cyber issues. ICT4Peace has already suggested that the time has come to create a dedicated Cyber Committee under the authority of the UN General Assembly and ensure secretarial support through a UN Office of Cyber Affairs.

This institutional arrangement could also facilitate co-ordinating the various cyber-related activities of the First, Second, Third and Sixth Committees. The idea of a permanent UN forum for cyber matters was a feature of the "Programme of Action" proposal put forward at the previous OEWG and we would support early attention by states to agreeing on this or a similar framework to ensure a tangible and more *operationally relevant* outcome from this OEWG.

ICT4Peace looks forward to interacting with participating states and non-government stakeholders alike in helping to develop and sustain the "open, stable, accessible and peaceful ICT environment" we all aspire to.

ICT4Peace Foundation, January 2022