ICT4Peace Statement to Eighth Substantive Session of the UN OEWG (8-12 July 2024), New York

Esteemed Chair, Distinguished delegates, colleagues and friends,

Thank you for this opportunity to deliver these short remarks.

As we stand on the cusp of establishing a permanent mechanism for addressing global cybersecurity challenges, we must ensure our approach is comprehensive, effective and forward-looking.

First, for more than five years ICT4Peace has proposed the implementation of a peer-review mechanism on accountability. Inspired by the Human Rights Council's Universal Periodic Review (UPR) process, this mechanism would enhance transparency and foster trust among nations, promoting respect for international obligations, norms and priciples. By helping to hold states to account, this would strengthen the foundation of our shared digital future.

Secondly, to restate a similarly long-standing call of ICT4Peace Foundation, we call upon all states to make a public commitment to not engage in cyber-attacks against critical infrastructure. Such a declaration would significantly contribute to global stability and protect the essential systems that our societies rely upon.

However, to achieve our aims, we also need to anticipate emerging technolgies and the challenges, threats as well as opportunities they offer. We stand at a critical juncture in technological advancement, one that demands our immediate attention and action. I speak of the advent of quantum computing, a development that holds both immense promise and potential peril for our global cybersecurity landscape.

The power of quantum computing threatens to render obsolete the vast majority of our current cryptographic systems - the very systems that protect nearly all the data stored in our ICT infrastructure. From financial transactions to sensitive government communications, from healthcare records to critical infrastructure controls - all could be laid bare if we fail to act swiftly and decisively.

This is not a distant threat, but an imminent challenge that requires our immediate and concerted effort. Echoing the words of Finland who has spoken most forcfully on this topic, we must take measures now to prevent the potentially disruptive and profound impacts of quantum computing on cybersecurity, invest in the development of quantum-resistant cryptography and begin the monumental task of upgrading our global ICT infrastructure so that we can reap quantum computing's positive transformative impacts, including enhancing and strengthening cybersecurity. This endeavor will require unprecedented levels of international cooperation, knowledge sharing, and resource allocation.

Moreover, we must ensure that all nations, regardless of their current technological capabilities, are included in this quantum transition. The disparity in quantum readiness could create new vulnerabilities and exacerbate existing inequalities in our interconnected world.

As we move forward to create a permanent mechanism, let us ensure it has the flexibility and foresight to address the emerging challenges of quantum computing, AI and the ones we cannot yet name. Let us commit to a framework that not only responds to current threats but that is forward-thinking, nimble and inclusive enough to anticipate and prepare for the technological revolutions on the horizon.

In conclusion, through accountability measures, protection of critical infrastructure, and proactive preparation for the quantum era, we can build a more secure, stable, and equitable digital future for all. The task before us is monumental, but so too are the stakes. Let us rise to this challenge together.

Thank you for your attention.