UN Open-ended Working Group on security of and in the use of information and communications technologies

March 2022 informal virtual dialogue meeting hosted by the Chair
24 March 2022

Delivered by Raman Jit Singh Chima (Senior International Counsel and Global Cybersecurity Lead)

Thank you Chair, Ambassador Gafoor:

At the start, I want to thank you for your frank opening comments at the start of this meeting around the importance of the UN as a confidence building measure. We agree with you - and have ourselves said in the previous iteration of the OEWG - that the OEWG itself is a crucial confidence building measure when it comes to global cybersecurity.

The wider geopolitical developments of today, and the reality of cyber disruptive activities being perpetrated against vulnerable communities, increases the importance of this process. But it also emphasizes the importance of seeing how we can advance our global consensus around cyber stability and peace, and in ensuring that we "walk the talk".

We must recognise how recent events in Ukraine demonstrate to us that digital right violations enable and escalate offline violence, and the calculated attacks targeting digital systems essential to people's safety and wellbeing are unacceptable.

On February 18, 2022, we joined together in a civil society statement calling for solidarity with Ukraine's human rights defenders in guarding against cyber threats. In that statement, we made the following three calls to action, which we believe have wider bearing on the work of the OEWG:

1. Tech companies, nonprofits, and funders to provide direct support to journalists, civil society, and human rights defenders in strengthening their resilience against cyber threats;

2. UN bodies and other international organizations to establish and uphold clear, people-first cybersecurity standards; and
3. Policymakers, platforms, and other relevant stakeholders to guard against attempts to escalate and exploit current tensions.

As one of my preceding colleagues mentioned, we need to focus on the quality of our discussions and move past the deadlock on the participation of the wider cybersecurity global community in this crucial working group. Indeed, other UN processes in related realms of international ICT issues are demonstrating that ways ahead are possible. I would also suggest that we can consider the option of more focused discussions on the specific areas that the Chair has identified framing questions for. The informal meetings can be structured to take these up in a dedicated manner, longer sittings beyond one day, and focusing on bringing in inputs and ideas from experts with open, engaged dialogue with states, in a manner that can be brought on record and used to bolster the discussions of the OEWG. We again note the leadership demonstrated by Singapore in its organization of the informal intersessional multi-stakeholder session in the past iteration of the OEWG.

In particular, we believe that the OEWG would benefit from hearing from humanitarian actors, human rights defenders, and the digital security community that assists civil society around the new threat actors and cyber disruptive activity they have faced as 2022 has advanced. We agree with the comments made by our colleagues at the ICRC, who noted that hacking the data of the world's most vulnerable is an outrage. We therefore suggest that the OEWG Chair and Secretariat consider the possibility of a focused discussion on the topic of the current status of cyber threats to humanitarian actors and human rights defenders for discussion in a future meeting of the OEWG, as part of the substantive sessions or an informal discussion.

Another issue I hope to bring your attention to is a growing part of the cyber threat ecosystem, namely the uptake in cyber mercenary and cyber attack for hire operators. We believe it should be part of the agenda of the OEWG's substantive work, including the framing questions posed by the Chair. Specifically, we believe that this should respond to the specific recommendation made by the OHCHR expert group on Mercenaries in its October 2021 report, where it said that: "The Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security and the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security should further address human rights concerns arising from the involvement of mercenaries and related actors in cyberoperations".

We endorse the suggestions being made to encourage further voluntary efforts around inputs, guidance, and statements around the implementation of the norms of responsible state behavior. An additional opportunity for collaboration and progress is the topic of coordinated vulnerabilities disclosure. We have seen repeated statements by several states as well as civil society and industry actors around the importance of increasing global cooperation channels around coordinated vulnerabilities disclosures - and indeed that there is appetite to support this. This is a concrete area of work that the OEWG should take up; voluntary efforts to help advance working global consensus on increasing cyber stability and building trust. We can begin by encouraging states to release and share their policy approaches towards vulnerabilities disclosure, and by bringing in the non-state cybersecurity community to share their practices and recommendations for improved international cooperation on this tangible area for improving global cybersecurity.

Thank you Chair and Secretariat, and we look forward to today's discussions and the forthcoming substantive session.