Intervention as Discussant by Daniel Stauffacher, President ICT4Peace

Thank you. Congratulation to Fabrizio and his team for a herculian job in producing the SG's Road Map. We are happy to continue to work together and support you.

Some general comments:

The ICT4peace Foundation has contributed to this process with a Report to the High-Level Panel on Digital Cooperation in 2018 and participated in the Roundtable Groups on Digital Trust and Security, Artificial Intelligence and Digital Human Rights.

These three topics are interconnected and have an impact not only state vs state security, but also on human security which ICT4Peace calls Digital Human Security.

Since Covid-19 we see a increasing number of attacks on health Institutions, facilities and staff. At the same time we witness an increase in mis-disinformation and diffamation campaigns against health institutions, facilities and staff. The second kind of (information) attacks are accelerating and compounding the first (network and critical infrastructure) attacks.

Remember: Peace, trust and security in cyberspace is a conditio sine qua non for digital cooperation; So, its great to finally see the UN getting a mandate, beyond the first UN GA Committee.

ICT4Peace therefore strongly supports a High-Level Political Statement on digital peace, trust and security. That statement should endorse and establish the leading role of the UN and launch a UN process building on existing work like GGE, OEWG etc.

We see a Proliferation of initiatives: Some are not very inclusive and some are duplicating efforts. Practically all Cyber initiatives in the last few years are lead by Governments of the North and IT Companies of the North. The Global South must be included more. That is why the UN should get a full mandate to lead in this field.

In the spirit of building on existing work by the UN and others on norms and a governance for digital peace, trust and security allow me to recall the three ICT4Peace initiatives to promote digital cooperation in this field. Two of them have been submitted to OEWG one of which is building on norms of the UN GGE 2015.

1. **Critical Infrastructure and Offensive Cyber Operations: A Call to Governments**

   https://ict4peace.org/wp-content/uploads/2019/11/ICT4P_CriticalInfrastructure_Call_Final_21102019.pdf

   "ICT4Peace calls upon governments, especially those possessing offensive cyber capabilities, to publicly confirm that they will respect the norm prohibiting cyber operations directed at critical infrastructure. This will provide a proactive means of assuring the international community that these states are committed to acting in a responsible manner in cyberspace."

   This Call concerns a commitment by Governments not to attack **all** Civilian Critical Infrastructure (icluding health) at all times and in peace and war time.

2 **ICT4Peace Proposed "States Cyber Peer Review Mechanism" for state-conducted foreign cyber operations**

   https://ict4peace.org/wp-content/uploads/2020/03/ICT4Peace-Proposed-States-Cyber-Peer-Review-3.pdf

   It has been generally acknowledged that some form of mechanism to hold states to account for their cyber operations affecting other states would be desirable. Such a mechanism would be premised as a cooperative process that would be state-centric, but which would also provide for the input of other stakeholders.

Among existing models, the Human Rights Council's Universal Periodic Review (UPR) mechanism2 is especially relevant to the cyber security context in its combination of state-led mutual examination and NGO input and participation. The proposed CPR would be in support of the proposal by the Mexican delegation to OEWG to establish a review or reporting mechanism to monitor the implementation of norms and to identify and share best practices in this field.

3 Trust and Attribution in Cyberspace: A proposal for an independent network of organizations engaging in attribution peer review.

Most nations share the view that existing international legal rules and ordinances hold in cyberspace. Enforcement of these standards, however, is difficult. Malicious cyber activities are usually shrouded in secrecy and anonymity, making definite attribution difficult and even impossible at times.

ICT4Peace has prepared the following thought piece, that takes into account the technical and political challenges related to effective attribution, and presents a simple proposal for improvement, namely the setting up of an independent network of organizations engaging in attribution peer-review.

Attribution

For laws and norms to be effective in regulating conduct in cyberspace, violations of the former must be detected, and perpetrations attributed beyond reasonable doubt. The process of assigning blame for cyber attacks requires intricate political and technical forensics and skills, "weaving together […] clues concerning past attack methods, current operational techniques, and knowledge of adversaries' geopolitical objectives to identify a likely [culprit]". With a view to achieving higher levels of confidence vis-a-vis ascribing blame for nefarious behavior in cyberspace and introducing accountability, some experts have suggested the creation of an international attribution body similar to established enforcement mechanisms such as the International Atomic Energy Authority. There are, however, profound differences between nuclear and information technologies, and the nature of nuclear arms and cyber weapons, respectively.

Plea for a Global Cyber Attribution Network

In order to curb adverse effects stemming from the misuse of offensive cyber capabilities, effective, technically mature and above all trustworthy attribution

is indispensable. “There are an increasing number of government entities, private firms, and research organisations that have the capability to undertake investigations to attribute the source of cyber attacks. However, these entities do not follow a standardised research methodology and employ different naming conventions for cyber threat actors and confidence metrics for their findings”.

With a view to addressing these inconsistencies and contributing to a more secure and stable digital environment, ICT4Peace proposes the setting up of an independent network of organisations engaging in attribution peer-review. For international legal provisions to be effective and accountability for malicious cyber activities to take hold high levels of confidence and publicly persuasive attribution of responsibility are required. In cyberspace, where establishing proof claims beyond reasonable doubt is still challenging, secrecy and mistrust are prevailing, and multiple factors (economic, political, technical) need to be taken into regard, collaborative attribution practices seem most promising.

Geneva, 15 June 2020