Excellencies, Ladies and Gentlemen, Dear Colleagues,

It's a great honor to have been invited to speak in this plenary session on the theme of "Current problems of ensuring international peace and maintaining sustainable development in the global information society".

I remember fondly my participation in the International Conference on Cyber-stability in Moscow that took place in December 2019 at the Ministry of Foreign Affairs of the Russian Federation.

At that time we also discussed our joint project and report called METHODOLOGICAL ISSUES OF THE APPLICATION OF NORMS, RULES AND PRINCIPLES OF RESPONSIBLE BEHAVIOUR OF STATES edited by Prof Anatoly A. Streltsov and Dr. Eneken Tikk

This report has now been published. ICT4Peace is proud to have been part of this rare cooperative effort by Russian & Western experts to explore the future of cyber norms with partners from Russia, United States, Estonia and Switzerland.

****

You wouldn't be surprised that as the President of the civil society organization ICT4Peace I approach this topic with the vision that has animated ICT4Peace from the start; that of a cyberspace devoted to peaceful activity. Despite the sad record of malicious and offensive cyber operations undertaken by states and non-state actors alike, we should never forget that the unique, human-created environment of cyberspace can be preserved for peaceful purposes if collectively we advocate for this.

One of the few accomplishments of the United Nations with respect to restraints on offensive cyber operations was the agreement in 2015 on a set of norms of responsible state behaviour in cyberspace. The eleven norms were the consensus product of a UN Group of Governmental Experts (GGE) and were subsequently supported in a UN General Assembly resolution (adopted by consensus) that encouraged states to be guided by the GGE outcome in their use of Information and Communication Technology (ICT).

Prominent amongst these norms was one that prohibited cyber attacks against critical infrastructure on which the public depends. The fact that this norm was developed by members of a GGE that included representatives of all five permanent members of the UN Security Council (all powers possessing significant offensive cyber capabilities) provided grounds for hope that this norm of restraint would be respected in practice.

Unfortunately, this hope does not appear to have been borne out, as almost daily there are credible reports of cyber penetrations and a times actual damage of critical infrastructure as a result of offensive cyber operations, many of which state sponsored or conducted.

The fact that the health care sector was targeted extensively during the current COVID 19 pandemic was a cause for justified outrage on the part of many around the world. But we must avoid reducing the general prohibition on targeting critical infrastructure to only those elements which have a medical logo attached to them.

.

Of course, the health care sector is a crucial element of critical infrastructure, but if we only cite it as a public service meriting protection, we detract from the commitment to safeguard all critical infrastructure. One does not need to be a cyber security specialist to appreciate how devastating for society cyber attacks against infrastructure such as energy grids, water treatment plants, transportation hubs and nuclear facilities could be.

This vital norm of restraint on state conduct in cyberspace needs to be upheld in its totality and civil society organizations alongside responsible governments and companies must publicly insist on this protective status for all critical infrastructure.

ICT4Peace has advocated for a pro-active confirmation by states of their commitment to respect the norm of non-targeting of critical infrastructure. Last fall we initiated a "Call to Governments" to put their states on record as honouring this key norm.

At a time when the international community is distracted by the pandemic, it is crucial that the protection of critical infrastructure norm is reinforced rather than eroded.

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) mechanism could be relevant to the cyber security context in its combination of state-led mutual examination while providing as well for private sector and civil society input and participation.

ICT4Peace in its submission to the UN Open Ended Working Group has therefore proposed a "Cyber Peer Review Mechanism", that is one way of ensuring accountability for state behaviour in cyberspace.

This basic framework would respect the principle of a transparent, state-led review mechanism incorporating input from civil society and the private sector.

It would also enable those growing number of states possessing the capability for offensive cyber operations to reassure the international community that these capabilities were being employed in a manner consistent with international law and agreed UN norms of responsible state behaviour.

The establishment of such a cyber peer review mechanism would be a worthy recommendation emerging from the UN OEWG. The OEWG has just been extended for another five years, but we are of the view that states could begin now to initiate multilateral negotiations that would yield concrete results. Several states participating in the OEWG have proposed a "Programme of Action" on cyber security. The negotiation of such a PoA should begin sooner rather than later. Our peer review mechanism proposal alongside other elements reinforcing or supplementing the original set of norms could be introduced into this process.

Further refinements of confidence-building measures to impart transparency and predictability could figure in an eventual PoA. Confidence-building measures have long contributed to the reduction of mistrust amongst states in an adversarial relationship. The UN GGE process has already yielded a number of CBMs and regional organizations such as the OSCE, the OAS and ASEAN have also generated several cyber security CBMs.

Getting states to agree on a set of CBMs is not the same as getting them to actually implement them in practice. That is why ICT4Peace has emphasized the importance of accountability mechanisms and institutional support to incentivize states to follow through with their political commitments to ensure the realization of the CBMs in policy and practice.

Tangible support for cyber security capacity building would also merit inclusion in any eventual PoA. In this regard, ICT4Peace has advocated for the OECD Development Assistance Committee (DAC) to make expenditure on capacity building eligible for Official Development Aid (ODA) credit.

If we are serious about bridging digital divides and enabling developing countries to participate on an equal footing in multilateral cyber security forums, international organizations need to take steps to facilitate funding from donors.

Any eventual PoA for international cyber security will have to face up to the current yawning accountability gap. If cyber powers are to be incentivized to behave responsibly when they engage in cyber operations outside their borders, the international community will need to embrace a comprehensive mechanism for reviewing state action, and via a transparent, multi-stakeholder process for ensuring accountability.

Accountability and Attribution of cyber-attacks go together - we can't achieve the former without the latter.

It is understandable that sovereign states wish to retain attribution as a national prerogative, but given inherent bias, a purely national approach will lack credibility.

We need to devise an independent mechanism to generate evidence-based attribution findings. As is already evident in the numerous cyber threat reports being prepared by cyber security firms, there is great scope for accessing private sector capabilities in this regard.

Early on in the OEWG's work, ICT4Peace submitted a proposal sketching out possible approaches, that takes into account the technical and political challenges related to effective attribution, and presented a simple proposal for improvement, namely the setting up of an independent network of organizations engaging in attribution peer-review. We need to think through how such a autonomous attribution network can be connected to official, multilateral processes to decide on incidents on the basis of empirical evidence.

When we look upon the contemporary cyber landscape, deformed as it is by ever increasing cyber enabled abuses of human security and violations of agreed norms, it is clear that global society has more than enough "current problems" to contend with. At the same time, there is an expanding group of actors in and outside of governments that are developing creative solutions for these problems. If we are to reclaim cyberspace for peace and sustainable development we will require a concerted effort by all stakeholders.

Thank you

Daniel Stauffacher

President ICT4Peace

7 December 2020

****