



<sup>1</sup>Excellencies, Ladies and Gentlemen, Dear Colleagues,

It's an honor to have been invited to speak at this session on the theme of "Cooperation in the field of prevention of military conflict and the peaceful settlement of disputes in the ICT environment".

While it was before my time at ICT4Peace, I have been told of our earlier cooperation with Russian experts in identifying norms for state conduct in cyber space.

---

<sup>1</sup> Statement by Ms. Anne-Marie Buzatu, Vice-President and COO, ICT4Peace Foundation, Geneva, on 27 September 2021 at the Conference of the [Russian National Association for International Information Security](#) in Moscow.

In particular our joint project and report entitled **METHODOLOGICAL ISSUES OF THE APPLICATION OF NORMS, RULES AND PRINCIPLES OF RESPONSIBLE BEHAVIOUR OF STATES**

Edited by Prof Anatoly A. Streltsov Dr. Eneken Tikk

This report has been published and widely disseminated. ICT4Peace is proud to have been part of this all too 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 Vice President of the civil society organization ICT4Peace I try to 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 and act for this goal.

A singular accomplishment 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). They formed the core of a report which was 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.

We regret that despite this promising start this hope that states possessing offensive cyber capabilities would respect the non-targeting of critical infrastructure norm that they signed up to has not been borne out. Almost daily there are credible reports of cyber penetrations, disruption of normal functionality and at times actual damage of critical infrastructure as a result of offensive cyber operations, many of which are state sponsored or conducted.

The fact that the health care sector was targeted extensively during the COVID 19 pandemic was a cause for justified outrage on the part of many around the world. But we must not reduce the general prohibition on targeting critical infrastructure to only those elements which have a medical logo.

.

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.

We are heartened by the fact that the UN Open Ended Working Group in its final report of March 2021 reiterated the norm of critical infrastructure protection in an undiluted form. 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. In 2019 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.

However, just because a norm is reaffirmed doesn't mean that it will be respected in practice. In order to incentivize states to fulfill their commitments some form of mechanism to **hold states to account** for their cyber operations affecting other states is needed. Such a mechanism would be a cooperative process that would be state-centric, but which would also provide for the input of other stakeholders who represent the vast majority of Internet users and owners.

Among existing models, the Human Rights Council's Universal Periodic Review (UPR) mechanism is 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 we consider is a readily doable form of ensuring accountability for state behaviour in cyberspace, as it builds on an existing, well-functioning mechanism of a UN body.

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 should be a near term goal of the international community.

The UN OEWG has just been extended for another five years, but we believe 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. Real world developments point to the necessity of quickening the pace of UN action to prevent worsening online conflicts.

The PoA envisages a permanent UN forum for cyber security issues. ICT4Peace has long called for such an institutional manifestation of the importance cyber activity represents for global security and well-being. We believe the time has come to create a standing Committee on Cyber Security under the UN General Assembly and ensure that this forum is supported by a UN Office of Cyber Affairs.

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 cyber security CBMs. As with norms, simply signing up to a set of CBMs is insufficient – one requires follow-up processes to monitor implementation. 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 agreed CBMs in policy and practice.

Tangible support for cyber security capacity building should also figure 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 confront the current yawning accountability gap. If cyber powers are to be pressed 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 a possible approach, 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 consider 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 many 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 for your attention.

\*\*\*\*\*