ICT4Peace Statement to the UN Security Council Meeting
Cyber security and International Peace and Security
November 28, 2016, UN HQ, New York

Dr. Daniel Stauffacher, President, ICT4Peace Foundation

Mr. Chairman, Excellencies, Colleagues,

On behalf of the ICT4Peace Foundation, an NGO dedicated to the promotion of a peaceful cyberspace, I thank you for this opportunity to address this meeting.

The international community often addresses threats to international peace and security only once those threats have materialized and violent conflict has erupted.

Yet, all here would agree, I suspect, that conflict prevention is far superior to engaging in conflict or dealing with the messy aftermath of such conflict.

The relatively new environment of cyberspace (the very term was only coined 30 years ago) presents us with a golden opportunity to engage in conflict prevention. The internet alone represents an information and communication platform of extraordinary importance.
With over 3.5 billion users, our global society is highly dependent on the internet for its well-being and prosperity.

As we embark on Agenda 2030 for development, societies will increasingly need to apply ICTs to achieve their goals. Yet, despite its enormous socio-economic importance and its overwhelming use for civilian purposes, much remains to be done to ensure that cyberspace is used “for peaceful purposes” and “in the interests of all countries”.

In particular, we need to ensure that states commit to protecting critical civilian infrastructure from state-sponsored attack. The dictates of international law, including international humanitarian law, and the recognition of common security interests require, at a minimum, such restraint.

To this end, States should move rapidly to implement cyber security confidence-building measures aimed at protecting such critical infrastructure, including the computer emergency response teams (CERTs) that are the “first responders” of cyberspace.

More generally, at this early stage of considering what sort of governance should be applied to cyberspace, it is crucial that the advocates of peaceful uses of cyberspace are given priority.

The first destructive acts of offensive cyber operations have occurred, although it is telling that no state has yet to claim responsibility for these violations of the peaceful operations of cyberspace. If this reflects a residual shame in taking action to undermine the peaceful potential of cyberspace it could be a salutary sentiment on which to urge restraint.

We have heard the calls for the forging of a global consensus around norms of responsible behavior in cyberspace. For some, the necessary diplomacy to realize this goal has lagged behind the moves to militarize and indeed weaponize this vulnerable environment.

It is crucial that the outcome of positive discussions and recommendations of a series of UN Group of Governmental Experts studying ICT developments in the context of international security and relating to international law, norms of responsible state behaviour as well as confidence measures, are acted upon by all states. To that end we have to find appropriate ways to involve member states beyond the UN GGE format.

Focusing on those actions that can have a destabilizing effect – for instance, offensive cyber operations against civilian infrastructure, would be a good starting point. They would focus on state-conducted activities, the effects of which cause significant damage, including physical damage.

As has been the case in the past with measures to limit arms and/or destabilizing military activity, there is a need to base these on a common security interest in sustaining a stable and smoothly functioning cyberspace.

In parallel to diplomatic efforts, there should also be a greater focus on capacity building, not only to minimize vulnerability to malicious activity but also to maximize cooperation in the event of incidents.

Beyond state action, we also realize that there is growing concern about the potential use of cyberspace by terrorist groups to conduct attacks against critical infrastructure. While there is no evidence that existing groups under the Security Council radar possess these capabilities, increased cooperation between states can also help respond to these concerns.

The private sector and civil society are the principal owners and users of ICT. They have a vital stake in ensuring that cyberspace remains a non-threatening environment in which all can benefit from its capabilities in a peaceful manner.

The Security Council can play a leadership role in raising awareness of current ICT threats and the risks they pose for international peace and security, while also ensuring that key actors such as the private sector, civil society and academia are part of the discussion.

Thank you for your attention.