Sustainable Peace: From Conflict to Cooperation
Seoul, 14 September, 2018

Panel IV: "Cyber Security: Enhancing Mutual Cooperation"
Ambassador Daniel Stauffacher
ICT for Peace Foundation

Executive summary
Advancing from the climate of (cyber) conflict to the climate of cooperation requires changes in state behaviour. Sustainable peace depends on our ability to develop change-enhancing mechanisms.

ICT for Peace Foundation calls upon all states, the private sector and the civil society to: strengthen the public international order in a cooperative manner; enhance regional cooperation; and support sustainable development goals in their unilateral and mutual cyber security endeavours.

The 1970 UNGA "*Declaration on Principles of International Law* concerning Friendly Relations and Co-operation among States in accordance with the United Nations Charter" stresses that states have a duty to cooperate "in the maintenance of international peace and security" and in the promotion of universal human rights. It has been well established that cooperation is essential to achieve cyber security. In this context, the 48 years old principles are still of utmost importance, and most relevant and applicable in cyberspace.

Cooperation in the field of cyber security often focuses on solving contingent issues, such as incident handling and capability development, but also on prevention of conflicts and conflict escalation through confidence building measures. These forms of cooperation are essential but not necessarily sufficient to achieve sustainable peace in cyberspace. To echo renowned peace researcher Johan Galtung, they rather speak of negative than of positive peace.

To achieve positive peace, our cooperation must address the underlying causes of (cyber) conflict and promote change in thinking and behaviour. Sometimes the weekly patches are not sufficient, and we need to upgrade or even change the operating system.

Allow me to offer three possible approaches to sustainable peace and how to move from conflict to cooperation:

Firstly, alongside international security, we need to **strengthen the public international order.**

The public international order is eroding as countries deliberately stress an interpretation of international law allowing cyber operations. It is eroding when states use ICTs to attack and undermine other countries. It erodes when states refuse assistance to each other in case of a cyber attack.

Globally, the *UN Group of Governmental Experts on Developments in the field of information and telecommunications in the context of international security* has offered a norm of cooperation. They invite states to follow this recommendation and exchange their experience about ways to work together.

Secondly, we **need to promote and deepen regional cooperation**. Although cyberspace is global and borderless, neighbouring countries often face similar challenges and are in a rather similar stage of technological development. The overwhelming majority of contemporary and foreseeable cyber security issues, threats can and need to be solved at the national level.

Many governments, however, do not have sufficient human, technical and financial resources or competences. Here, ASEAN is paving a path. The "ASEAN Leaders' Statement on Cybersecurity Cooperation" promoted ASEAN Member States coordination in cybersecurity policy, diplomacy, technical and capacity building, "so that ASEAN's efforts are focused, effective, and coordinated holistically."

Moreover, Cambodia, Laos, Myanmar and Vietnam, CLMV, offer an excellent example of working together and sharing their experiences and concerns in the subgroup.

Such forms of cooperation help reduce insecurity, increase national and functional resilience and regional stability. Enhanced regional, sub-regional or even cross regional cooperation also helps to reduce the digital divide.

Thirdly, it is essential that the measures to strengthen the public international order and enhance regional cooperation support and align with **sustainable development goals**. Poor levels of cyber security severely hinders nations ability to achieve basic social and economic development objectives and erodes their long-term development potential. The following SDG impact areas are easily identified as those that will benefit from enhanced cooperation in promoting and protecting the use of ICTs: i) sustainable livelihood; ii) health and well-being; iii) equitable and sustainable economic growth; and iv) stability, governance and justice.

To conclude,

- Norms and laws cannot replace capacity and lack of resources in the least developed countries where hardware and software updates are an issue;
- Norms cannot change the fact that fundamental disagreement exists between major cyber powers about the role and utility of ICTs in the world;
- Creative and considerate cooperation allows us to overcome some of the burning issues like the lack of resources for training and education, distrust, misunderstandings.

Where cooperation exists, political differences and self-interest are put aside – look at the ways the CERT community works together. In a dialogue that is dominated by these features, we must seek for ways to cooperate and assist each other.

Recalling the sprit and the letter of the 1970 UNGA "Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States", ICT for Peace Foundation calls upon all states, the private sector and civil societies in cooperative manner to strengthen the public international order; to enhance structured regional cooperation; and to support sustainable development goals in their unilateral and mutual cyber security endeavours.

We are ready to promote and support such coordination with our expertise, network and good will.