It is more than a question of health – the need to protect critical infrastructure

By Amb. Paul Meyer, Senior Advisor, ICT4Peace Foundation

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)[1] 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. Within the context of the on-going UN work on norms of responsible state behaviour in cyberspace (i.e. the current GGE and the Open-Ended Working Group), condemnation of such attacks was a refrain amongst official statements.

At the same time, few of these statements were referring back to the agreed norm forbidding attacks against all critical infrastructure. While the health care sector is a crucial element of critical infrastructure, there is a risk in only citing it as a public service meriting protection. This could lead to a diminishment of the commitment to safeguard *all* critical infrastructure. One

[1] https://undocs.org/A/70/174

does not need deep technical knowledge to appreciate how devastating for society cyber attacks against infrastructure such as energy grids, water treatment plants, transportation hubs and nuclear facilities could be. It is not in the public interest if those possessing offensive cyber capabilities, believe that they are free to "cherry-pick" which critical infrastructure in foreign countries they will refrain from attacking and which they will target.
This vital norm of restraint on state conduct in cyberspace needs to be upheld in its totality and not allowed to decay down to only those elements with a medical logo on them.

ICT4Peace has long advocated for the need to resist the "militarization" of cyberspace and the necessity to protect critical civilian infrastructure. Recognizing the desirability of pro-active confirmation by states of their commitment to respect the norm of non-targeting of critical infrastructure, ICT4Peace has initiated a "Call to Governments" [2]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.

Geneva November 16, 2020

[2] This Call has been published by ICT4Peace on the occasion of the launch of the negotiations of the Open-ended Working Group on developments in the field of information and telecommunications in the context of international security ("OEWG") on 21 October 2019 https://www.un.org/disarmament/open-ended-working-group/