Critical Infrastructure and Offensive Cyber Operations: A Call to Governments

"A State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public".[i]

This norm is one of eleven such principles for the responsible behavior of states in cyberspace recommended in the consensus report of a UN Group of Governmental Experts (GGE) released in 2015. The next year, the UN General Assembly adopted a resolution which called upon member states "to be guided in their use of information and communications technologies (ICT) by the 2015 report" of the GGE.[ii] Although all these norms have a voluntary, non-binding character, it is fair to say that the norms expressed in the 2015 GGE report enjoy a status of near universal support within the international community. In conjunction with international law, they are the closest the UN has got to a set of "rules of the road" to guide state behavior in the unique and increasingly important realm of cyberspace.

While all of the norms proposed by the 2015 GGE have merit, ICT4Peace believes the norm on the prohibition of cyber operations that deliberately damage critical infrastructure upon which the public depends, has special importance. The welfare of global society is heavily dependent on the proper functioning of critical infrastructure across a wide spectrum of services, from water treatment to electricity generation, from transportation systems to financial networks.
This infrastructure is, in turn, increasingly controlled by computer systems vulnerable to disruptive cyber operations. If some or more of this infrastructure failed to perform, the impact on societies and individuals could be enormous.

Unfortunately, and despite the fact that the vast majority of this infrastructure is of a civilian nature, damaging cyber operations have already occurred against them, by states and non-state actors alike.[iii] The experience to date underlines the potential for massive negative effects on infrastructure essential for the safety and well-being of the public. While some states, possessing offensive cyber capabilities, have affirmed that their activity is compatible with their international legal obligations, there is more work to be done to clarify and consolidate international legal understanding in this area.

Given the uncertainties regarding how the international law applies to state operations, the importance of politically binding restraint measures, such as the prohibition on cyber operations against critical infrastructure is all the more acute. ICT4Peace believes that there is a pressing need to reinforce the nascent normative framework set out in the UN GGE report, by operationalizing these norms, and in particular, the norm concerned with the protection of critical infrastructure.
It is only by means of a demonstrable commitment by states to abide by this norm that it will be possible to begin to solidify in policy and practice the still fragile restraint measure represented by the prohibition against cyber interference with foreign critical infrastructure.

ICT4Peace calls upon governments, especially those possessing offensive cyber capabilities, to publicly confirm that they will respect the norm prohibiting cyber operations directed at critical infrastructure. This will provide a proactive means of assuring the international community that these states are committed to acting in a responsible manner in cyberspace.

[i] *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security,* UN General Assembly, A/70/174, 22 July 2015

[ii] *Developments in the field of Information and Telecommunications in the Context of International Security,* UN General Assembly Resolution, A/71/28, 5 December 2016

[iii] For a valuable resource detailing the scope and implications of attacks on critical infrastructure, see *The Potential Human Cost of Cyber Operations,* The International Committee of the Red Cross, 20 June 2019, https://www.icrc.org/en/publication/potential-human-cost-cyber-operations. The section providing a listing of major cyber-attacks and describing the impact on specific civilian sectors (pp 54-67) is particularly useful.

For further information please contact: danielstauffacher@ict4peace.org