Submission to Australia's Consultations on International Cyber Security Policy

Paul Meyer, Adjunct Professor of International Studies and Fellow in International Security, Simon Fraser University, Vancouver, Canada and Senior Advisor, ICT4 Peace.

Australia is to be commended for the leadership it has shown on international cyber security policy. Its willingness to articulate a specific *International Cyber Engagement Strategy* and to provide a comprehensive and transparent account of its own policies and practices has been exemplary. The initiation of the present public consultation also is testament to the Australian Government's desire to engage non-governmental stakeholders in the formulation of its future course of action on the international scene. The following represents my personal input into thinking as to what aims Australia should pursue in the current UN OEWG and GGE processes.

The main goal: Australia has already expressed in its *Strategy* the goal of a "peaceful ICT environment". While the 2015 GGE described the goal of an "open, secure, stable, accessible and peaceful ICT environment", primacy should be accorded the "peaceful" goal as the other desirable features flow from this. "Stability" in cyberspace is not an adequate goal or substitute for cyber peace, in the same way that the "strategic stability" of the nuclear armed East-West confrontation was never viewed as an acceptable end state for the international community. Efforts should be geared to retaining as much of the "peaceful" character of cyberspace as possible in keeping with the wishes of the vast majority of its users.

Unconditional respect for key norms: Australia has (alongside several of its allies) has taken to condition its respect for the agreed UN norms as being only applicable in peacetime. For the most important of these norms (e.g. non-targeting of critical infrastructure or computer emergency response teams-CERTs) a blanket prohibition is preferable. ICT4Peace has issued a "Call on Governments" to publicly commit to respecting the ban on targeting critical infrastructure *at all times.* Such a complete prohibition is desirable given the frequency of offensive cyber activity below the threshold of armed conflict in which international humanitarian law (IHL) applies as well as the potential dilution of protection because of the inherently subjective judgments about the collateral damage-military advantage trade-off stipulated under IHL. There are several existing prohibitions on weapon systems under international law that apply both in peacetime and wartime and global society deserve the reassurance that an unconditional ban on cyber operations that damage or disrupt critical infrastructure on which publics depend.

Extending the non-targeting norm to nuclear weapon complexes: Attention has recently been given to the vulnerability of nuclear facilities to potential cyber attacks. While civilian nuclear facilities would be covered under the prohibition on targeting critical infrastructure, facilities involved with nuclear weapons (e.g. nuclear forces, early warning systems and nuclear weapon production and storage facilities) should also be subject to a comprehensive ban on offensive cyber activity (even intelligence-gathering activity given the inability to discriminate between such probes and intrusions of a more destructive intent). Several experts have called for nuclear weapon-possessing states to agree on such a ban, but in the interim including this new norm

into the existing UN inventory would be a prudent step and one that would facilitate subsequent action by concerned states.

A division of labour between the OEWG and the GGE: Although the bifurcated processes for UN consideration of cyber security emerging from the 2018 UNGA session was regrettable for the cohesion and efficiency of UN action, we are stuck with it for the immediate future. Australia should, in concert with others, try to restore the consensus approach that had marked earlier stages in the UN's work on cyber security policy. In that regard, it would be helpful to devise a logical division of labour between the two processes given the great overlap in their mandates.
A possible approach would have the GGE devote itself to considering the outstanding question of previous GGEs, namely, *how* international law applies to state-conducted cyber operations in specific circumstances. The OEWG might best concentrate on the *operationalizing* of the agreed norms as well as considering if additional tweaking of these norms would facilitate their implementation by states.

Accountability requires Attribution: Australia among others have called for holding to account states or non-state actors engaged in malicious international cyber activity. Such accountability however requires reliable and credible attribution of those responsible for such actions. Australia should take a lead in devising an international mechanism that could provide such attribution in a manner that would support robust accountability. In my view, such a mechanism could take the form of a public-private partnership in which private sector cyber security expertise could provide an evidentiary base for a "peer review" process amongst states that would subject their actions to peer and public scrutiny and ideally prompt more responsible state conduct. The experience of the UN Human Rights Council and its Universal Periodic Review is relevant to any effort to develop a comparable mechanism for cyber activity.

Institutional Support: The UN effort to date has largely been consumed with norm development, but the time has come to consider what institutional support and follow-up can be added to the normative framework to encourage its fullest implementation. At a minimum this would require some form of dedicated working group or forum at which issues connected with the implementation of the UN norms could be regularly discussed. Putting into place a process of regular (perhaps annual) reports by states on their implementation of the UN norms and to outline other relevant policy or practical steps would be a vital near-term objective. Australia should work with like-minded states and other stakeholders to equip the UN with some basic institutional support for its cyber security understandings in order to give them practical effect. A more ambitious step, but one consistent with Australia's leadership to date, would be to offer to host an international organization to provide this institutional support for UN member states.

January 18, 2020