Comments by the CyberPeace Institute on the Initial “Pre-draft” of the report of the OEWG on developments in the field of information and telecommunications in the context of international security

April 2020

The CyberPeace Institute has reviewed the ‘Initial “Pre-draft” of the report of the Open-Ended Working Group (OEWG) on developments in the field of information and telecommunications in the context of international security’ with great interest. We commend the OEWG’s inclusive approach towards civil society, academia and the private sector and the Chair, his Excellency Ambassador Lauber, and his team for the high quality of this initial pre-draft.

The CyberPeace Institute would like to submit to you and to the attention of all interested stakeholders the following comments, organized by section of the report. As requested, we have focused our feedback where we see room to strengthen areas of agreement and on the norms and recommendations sections of the report.

**Section A: Introduction**

- **Paragraph 12:**

The CyberPeace Institute urges the Chair and all Member States and observers to note how the current global pandemic starkly illustrates the critical importance of a human-centric focus. For extended periods during late 2019 and 2020, governments around the world have implemented social distancing and other restrictions in order to stem the spread of disease in the physical world. As a result, during this time many more humans have suddenly, out of necessity, moved online. Many of these new participants are likely to lack some of the “basic instincts” and familiarity common to those who are more accustomed to regular online activity. Regardless, for new online entrants and veterans alike, the massive increase of remote work means that individuals are now accessing business networks and data outside of generally more controlled enterprise environments. These shifts offer only a glimpse of the impact that online security during the COVID-19 pandemic has had on civilian life, but they are powerful examples of both the impact of cyber risk on civilians as well as the role that civilians play in defining, and changing, risk profiles.

This emphasis on the need for a more human-centric lens was raised by both Member States and observers during previous OEWG meetings and, we note, has been flagged by both Member States and observers in comments already submitted to the Chair on this pre-draft. Moreover, the COVID-19 pandemic is by no means the first and surely will not be the last time that global shifts in the ICT landscape significantly impact civilian lives. Accordingly, while we support the statement in Paragraph 12 regarding the need for a human-centric lens we urge that, now more than ever, there is a need for the work of the OEWG and any resulting reports to focus less on ICTs and cyber operations themselves or related costs to infrastructure or business disruption, and more on their effects on civilian populations. Accordingly, we would welcome greater emphasis and articulation of these effects – including their scale and scope, with particular emphasis on the potential loss of basic human rights and human life. Such an approach will not only better reflect and fulfill the OEWG mandate; we believe this is an area of common agreement and its emphasis can help to pave the way for productive exchanges in areas until now characterized by more divergent views.

**Section B: Existing and Potential Threats**

- **Paragraph 19:**

While the CyberPeace Institute recognizes that diverse national priorities make it difficult to create an all-inclusive definition for “critical infrastructure,” we believe the current global crisis demonstrates the overriding importance of recognizing a universal set of core critical civilian infrastructure sectors that
enable delivery of essential services to the population and which may be threatened by the use of ICTs. In particular, we echo the submitted comments from the International Committee for the Red Cross (ICRC) recommending that the Chair consider explicitly mentioning in this section of the report electrical, water, and sanitation facilities. We would also add consideration of food production and distribution to this list.

Inclusion of these essential services is in keeping with the OEWG’s stated recognition (Paragraph 12) that the elements comprising its mandate are to be considered through a human-centric lens. Also consistent with this commitment to a human-centric approach is our recognition that other sectors may be deemed essential depending on evolving national priorities and shifting threat landscapes. Accordingly, rather than attempting to create an exhaustive list of sectors, we recommend consideration of adding the above-mentioned sectors complemented by a list of common criteria for determining the qualification of additional sectors as “critical infrastructure” under various circumstances.

Whether resolved by establishing a core list of sectors and/or a common criteria, or not at all, this persistent ambiguity around the definition and treatment of the term “critical infrastructure” further highlights the need for additional clarity regarding stakeholder interpretation and implementation of the laws, rules and norms relevant in the context of ICTs. With respect to the definition of “critical infrastructure” specifically, we recognize prior and existing efforts to gather, document, and analyze various state perspectives on this topic. But, like many discrete issues that are critical to ongoing discussions, we note that a centralized, dynamic tool for understanding how these viewpoints interact with other relevant issues is lacking. As set forth below, we believe that support for a robust and neutral mechanism for documenting and analyzing stakeholder perspectives on laws, rules and norms, particularly those that are central to the protection of civilians, would further reflect a real commitment by OEWG participants to take a human-centric approach.

Section C: International Law

- Paragraphs 26, 27, 30, 31, 33:

Multiple paragraphs in this section (see, e.g., Paragraphs 26, 27, 30, 31, 33) highlight continued disagreement among stakeholders about how international law applies. However, at the same time these paragraphs also highlight, albeit in a less pointed manner, stakeholders’ agreement on three key points:

i) the need for additional clarity regarding how international law applies to the use of ICTs;

ii) the fact that achieving greater clarity requires thoughtful attention, consideration, and robust participation by all relevant stakeholders; and

iii) the relative merits of a variety of existing and proposed mechanisms for the exchange of views and development of common understandings.

We believe these are important bases of common agreement which should also be explicitly acknowledged, and which can serve as important foundational elements for prioritizing the next steps towards a viable path forward.

While recognizing the need for further discussion and clarity regarding these issues, the CyberPeace Institute also strongly urges that unilateral pledges made by stakeholders – either in the context of OEWG proceedings or elsewhere – regarding their interpretations of and obligations under international law, rules, norms and principles related to the use of ICTs be documented. We also strongly urge stakeholders who have not made such statements to do so. At a minimum, we support the calls by OEWG Member States that states should pledge not to use ICTs and ICT networks to carry out activities which run counter to the task of maintaining international peace and security. Documenting such pledges will serve as an important element of an evidence-led accountability framework and will also help to more clearly identify specific areas of stakeholder agreement or discord.
Paragraph 32:

Significantly, this paragraph touches on a point of agreement that could be strengthened: the development and enforcement of laws and norms must be supported by a more robust, evidence-led framework for achieving greater accountability, including for attribution of malicious cyber activities. The CyberPeace Institute has underscored this issue in its previous statements and position paper, “Closing the accountability gap: A proposal for an evidence-led accountability framework” (https://cyberpeaceinstitute.org/assets/news-articles/cyberpeace-institute-position-paper.pdf).

Discussion and written statements by a variety of stakeholders demonstrate growing agreement around this need, including the need for attacks to be linked with consequences. We urge that more fully recognizing this point of agreement could serve as a critical stepping-stone to the next stage of determining the specific contours of such a framework for accountability.

In addition, we echo previous comments regarding the importance of a human-centric approach and recommend that the human-centric element be incorporated into this paragraph. In particular, we believe it is critical to clarify that accountability and attribution in this context are not political concepts but rather they are necessary bases for the protection of civilian rights and life. The end goal of closing the accountability gap is for human beings around the world to exercise their basic human rights in their use of ICTs free of fear or harm.

To this end, we believe it is also important to note in this section that approaches that were proposed during the OEWG sessions included those by neutral parties emphasizing the importance of an evidence-led framework.

Section D: Rules, Norms and Principles for Responsible State Behaviour

• Paragraphs 37, 38 and 40:

The CyberPeace Institute notes that this section (including Paragraphs 37, 38, 40) highlights both i) emerging broad agreement around the importance of strengthening the implementation of agreed norms as well as ii) a number of diverging views on whether and which new norms are currently needed or should be developed. These two threads serve as critical guideposts for the international community’s priorities and next steps.

In order to close the accountability gap, the CyberPeace Institute believes near-term next steps must include the operationalization of existing norms. For this, we strongly support the recommendation to create a neutral, inclusive and easily accessible mechanism or repository for collecting, sharing, comparing and analyzing current views, implementation practices and guidance regarding applicable norms. Such a centralized mechanism could bring together in one repository various inputs that are essential to informing this operationalization. For example, state perspectives on the definition of “critical infrastructure” could be housed and analyzed in this repository. The approach put forward by Canada regarding guidance on norm implementation offers a concrete example of the kind of specific content and outputs that could be developed with the support of such a mechanism. Similarly, the work and recommendations of other multi-stakeholder initiatives (i.e., the Global Commission for the Stability of Cyberspace and the Paris Call for Trust and Security in Cyberspace) should also serve as important inputs and guidelines.

Recalling the need for an evidence-led accountability framework that links attacks with consequences, we also believe that new norms, if needed, are welcome. For example, the COVID-19 global pandemic highlights the need for an agile approach to ensure that the international community can effectively address grave threats to the well-being of humans, such as attacks on the health or food supply chains, especially as they manifest during times of crisis. If current processes do not enable rapid alignment regarding the application of existing norms (for example, those related to the protection of “critical infrastructure”) when needed, we should consider the creation of new norms as a more workable alternative.
Accordingly, we recommend that the ongoing work to operationalize existing norms, which is essential, be supplemented in parallel by the addition of new norms when warranted. To this end, the CyberPeace Institute supports the ICRC’s proposal for the following new norm: “Norm prohibiting states from conducting or knowingly supporting ICT activity that would harm medical services or medical facilities, and would oblige them to take measures to protect medical services from harm.” Targeted attacks against hospitals, testing centers and health agencies during the COVID-19 pandemic demonstrate the need for a clear prohibition of this activity in order to protect human lives and build an effective evidence-led accountability framework.

Section F: Capacity-building:

- Paragraph 52:

Paragraph 52 describes Member States’ emphasis on the use of widely accepted principles to guide capacity-building efforts. The CyberPeace Institute recommends that these principles reflect the need for capacity-building to adapt to the rapid evolution of relevant ecosystems and communities. The COVID-19 pandemic again provides a powerful example: during a very short period of time, communities around the world quickly recognized the need to build capacity in supply chains (e.g., medical equipment and supplies, food distribution) that may not have been considered as high-priority in the past.

- Paragraph 54:

The CyberPeace Institute welcomes the emphasis in Paragraph 54 on the importance of engaging with local organizations in order to enhance sustainability of capacity-building efforts. For vulnerable communities to receive actionable assistance, they require a certain baseline level of capacity. We note that partnering with grass-roots practitioners at the local level, including those whose focus is not specific to cyberspace but who have field networks and trusted relationships with local communities, plays a vital role in building such a baseline and making longer-term efforts sustainable.

- Paragraph 55:

Finally, in consideration of the points highlighted in Paragraph 55 regarding greater coordination, we wish to emphasize that capacity-building efforts must consider and account for effective and responsible onboarding of the rapidly increasing multitude of volunteer initiatives, whether individual or corporate, (and, again, with the COVID-19 crisis as a prime example) while mitigating the risk for crisis predators.

Section H: Conclusions and Recommendations

- Paragraph 67:

The CyberPeace Institute welcomes the emphasis made in Paragraph 67 that the current global normative framework for cooperative measures to address existing and potential threats in the sphere of ICTs is the result of important linkages and synergies between related elements. We believe it is also important that the report emphasizes the particularly close linkages in this respect between voluntary non-binding norms and obligations under international law.

We also welcome the recognition in this section that regular institutional dialogue regarding this global normative framework at the UN level is critical. At the same time, we note that, as described in numerous sections of the pre-draft report and highlighted in our comments above, there is broad agreement that additional information is needed to inform these dialogues. In particular, Member States and other stakeholders have flagged throughout their interventions and comments that there is a lack of information and understanding regarding stakeholder interpretation and implementation of relevant
norms and international law. We believe this strongly supports prioritizing a neutral and global mechanism for the collection, analysis, and sharing of such information as the next near-term action.

- **Paragraph 68:**

The CyberPeace Institute welcomes the recommendations set forth in Paragraph 68, sections (a) and (b), regarding the continued development and sharing of stakeholder views and practice related to both voluntary norms and international law. In order to maximize transparency and effectiveness of such efforts, and noting the close linkages between these two elements acknowledged in Paragraph 67, we also propose that the collection, sharing and analysis of these elements be undertaken as a combined effort on an integrated platform.

As noted by stakeholders and in the current pre-draft report, a number of existing efforts touch on various aspects of stakeholder policy and practice. However, these efforts generally focus on sharing stakeholder documents and/or providing analysis on specialized policy issues. In addition, many are focused solely on government perspectives and, therefore, do not reflect the input or expertise of communities that directly manage ICTs or that have experience advocating for peace and security across a range of contexts and issues. Lastly, none of the existing platforms are aimed at providing a neutral, accessible, inclusive, comprehensive and transparent repository of easily searchable stakeholder views and practice organized according to the specific areas of international law and voluntary norms that are the subject of institutional dialogue at the UN level.

The CyberPeace Institute proposes that a new, integrated platform could not only combine the work of existing efforts in one repository but it could also fill another gap that must be addressed in order to meet the call for an evidence-led accountability framework: the possibility of comparing analytics and evidence of attacks with the views, practices and pledges of the international community. Adding this missing element and joining up the very important work of existing efforts would ultimately provide a great benefit to the wider public in terms of both greater access to information and more responsible, accountable stakeholder behaviour. In light of its mission and neutrality, we believe the CyberPeace Institute is well-equipped and -positioned to serve as the custodian of such a platform.

We believe that taking this next step addresses concerns, raised by many other stakeholders throughout the OEWG proceedings, that a truly multi-stakeholder perspective is needed in understanding the normative landscape and that the international community is neither mature enough in its national views and practices for a comprehensive evaluation nor has sufficient data to begin forming the basis of new legal instruments.

Moreover, consistent with previously submitted recommendations of other stakeholders related to this section of the pre-draft report, we believe this approach is both pragmatic and practical, helping to avoid duplication and fragmentation of effort and providing important input into discussions about applicability and implementation of laws and norms, including specific modalities of applicability (e.g., who, how and in which circumstances they apply). Rather than diluting existing efforts or indiscriminately broadcasting sensitive information, the creation of such a repository would concentrate, complement and streamline existing efforts while also giving stakeholders control over what they disclose. It is our hope that, consistent with their statements during the OEWG process, many stakeholders would be eager to proactively contribute their views and practices to such a repository in order to enhance mutual trust, understanding and confidence.