ICT for peace foundation

POLICY BRIEF

ICT4PEACE AND THE UNITED NATIONS OPEN-ENDED WORKING GROUP ON INTERNATIONAL CYBERSECURITY (UN OEWG) 2019-2021

By Paul Meyer (Author) and Daniel Stauffacher (Editor)

GENEVA 2021

ICT4Peace Foundation

ICT4Peace Publishing, Geneva. April 2021
Copies available from www.ict4peace.org

ICT4PEACE AND THE UNITED NATIONS OPEN-ENDED WORKING GROUP ON INTERNATIONAL CYBERSECURITY (UN OEWG) 2019-2021

By Paul Meyer (Author) and Daniel Stauffacher (Editor)

ICT for peace foundation

FOREWORD

Geneva, April 5, 2021

It's a pleasure for ICT4Peace to publish this compilation of its inputs to and comments on the negotiations of the United Nations open-ended working group on developments in the field of information and telecommunications in the context of international security (UN OEWG) (2019 – 2021).

With a view to promoting a peaceful cyberspace, ICT4Peace has been calling for and supporting global negotiations at the United Nations since 2007. In light of the rapidly emerging threats also from State Actors, ICT4Peace in 2011 issued a Call for a Code of Conduct for Cyber Conflicts[1]. In the same spirit it subsequently focused its work on supporting the development and implementation of Norms of Responsible State Behavior[2], Confidence Building Measures (CBMs)[3] and Capacity Building in the context of the UN as well as Regional Organizations such as the OSCE, OECD, OAS, ASEAN and the AU. ICT4Peace is particularly proud to have cooperated with the UN Office for Disarmament Affairs to prepare and publish a first ever Commentary on the Voluntary[4], Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communication Technology proposed by the 2015 UN Group of Governmental Experts (GGE)[5] and adopted by the UN General Assembly by

1 Getting down to business – Realistic Goals for the Promotion of Peace in Cyberspace. A Code of Conduct for Cyber Conflicts by Daniel Stauffacher, Riccardo Sibilia and Barbara Weekes, ICT4Peace Publishing, Geneva, December 2011.

2 https://ict4peace.org/wp-content/uploads/2019/08/ICT4Peace-2014-Baseline-Review-ICT-Processes.pdf by Eneken Tikk, Tim Maurer and Camino Kavanagh, ICT4Peace Publishing, Geneva 2014

3 https://ict4peace.org/wp-content/uploads/2019/08/ICT4Peace-2013-Confidence-Building-Measure-And_Intern-Cybersecurity.pdf by Camino Kavanagh and Daniel Stauffacher (Editor) ICT4Peace Publishing, Geneva 2013.

4 https://ict4peace.org/wp-content/uploads/2019/08/ICT4Peace-2017-Civil-Society-And-Disarmament.pdf by Eneken Tikk (Editor) with a Foreword by Daniel Stauffacher. United Nations Publications, New York 2017

5 https://www.un.org/ga/search/view_doc.asp?symbol=A/70/174

consensus[6]. An overview of the ICT4Peace activities in the context of the UN GGE and UN OEWG as well as the Regional Organizations can be found here[7] and the list of publications here[8].

In 2019, as an NGO with ECOSOC status and fully accredited to the UN, ICT4Peace participated in the UN OEWG from day one, including in the informal and multi-stakeholder meetings. Our submissions, proposals and comments in the plenary sessions and on the various draft reports during the negotiations are accessible on the official UN ODA website[9].

For easy reference this Volume compiles all ICT4Peace's submissions to and comments on the UN OEWG negotiating process. In the beginning you will find the ICT4Peace's comments on the OEWG Final Substantive Report[10] and a Chairman's Summary[11] with the title: "The OEWG final report: Some progress, much remains unresolved". In Annex I, the full texts of all ICT4Peace official submissions to the OEWG process can be found. Annex II contains a list of ICT4Peace publications, posts and commentaries on the UN OEWG and the UN GGE.

In addition, ICT4Peace supported the UN OEWG negotiation process in organizing - in cooperation with the OAS, UN ODA and Kenya - a series of cybersecurity policy and diplomacy training workshops for policy makers and diplomats from Latin America and Africa.

The ICT4peace engagement with and support to the UN OEWG would not have been possible without the tireless and exceptional work of Amb. (ret.) Paul Meyer, ICT4Peace Senior Advisor. Paul Meyer[12] is the author of practically all the commentaries, submissions and statements published in this Volume. ICT4Peace is deeply indebted to him. With this publication, ICT4Peace hopes to inform policy makers, diplomats,

6 Adopted by consensus in resolution 70/237. This resolution "calls upon Member States to be guided in their use of information and communications technologies by the 2015 report of the Group of Governmental Experts." (https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/457/57/PDF/N1545757.pdf?OpenElement)

7 https://ict4peace.org/activities/support-to-un-oewg-and-un-gge/?load=all

8 https://ict4peace.org/publications/

9 https://www.un.org/disarmament/open-ended-working-group/

10 https://ict4peace.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf

11 https://front.un-arm.org/wp-content/uploads/2021/03/Chairs-Summary-A-AC.290-2021-CRP.3-technical-reissue.pdf

12 https://ict4peace.org/about-us/team/paul-meyer/

academics, industry and civil society, who did not have the opportunity to follow the OEWG process, about the submissions and proposals of ICT4Peace to this important UN process. Many of the points and ideas ICT4Peace put forward remain valid for the next stage of international discussion of how cyberspace can be sustained for peaceful purposes.

Dr. Daniel Stauffacher
Founder and President, ICT4Peace Foundation

THE OEWG FINAL REPORT: SOME PROGRESS, MUCH REMAINS UNRESOLVED

March 21, 2021

On Friday March 12, 2021, after one and half years of proceedings the UN Open Ended Working Group (OEWG) on Information and Telecommunications (ICT) in the context of international security, adopted a report. Given the varied perspectives of the member states engaged in the OEWG it is not surprising that agreement was only achieved on a final report by dividing the text developed over several months into two parts: a consensus section and a Chairman's Summary. The latter document was described as containing "diverse perspectives" , "new ideas" and "important proposals"(para 80) which preserved them for future reference even though they lacked universal support. As the consensus text, however, is the only part of the final report that states will accept as binding (in a political sense), this will be the focus of the present analysis.

To judge the merits of the report one has to situate it in the context of what has preceded it in the UN's work on international cyber security policy and what is to follow on in future. Since 1998 the UN General Assembly has had on its agenda an item on "Developments in the field of Information and Telecommunications in the context of International Security". Since 2003 the UN has created a series of Groups of Governmental Experts (GGEs) to consider this issue and in the years 2010, 2013 and 2015 these groups produced consensus reports on the task of identifying "norms of

responsible state behaviour" in cyberspace. The zenith of these efforts came with the 2015 GGE report and its enumeration of eleven voluntary norms for states to observe in their cyber conduct. These norms covered such important elements of restraint as the non-targeting of critical infrastructure on which the public depends, the non-targeting of so- called Computer Emergency Response Teams (CERTS) which act as the "first responders" to cyber incidents and the prohibition on states employing proxies. Significantly, the UN General Assembly in 2015 adopted by consensus a resolution (70/237) which stipulated that states should be guided in their use of ICTs by the agreed norms of the 2015 GGE.

Unfortunately, rising tensions between leading cyber powers resulted in the 2016-17 GGE failing to agree on a report. The next year witnessed a bifurcation of the UN efforts with the establishment of the OEWG (open to all member states) and the authorization of a further GGE (with a restricted membership of 25 representatives).

A primordial question for many was whether the OEWG, despite the deteriorating atmosphere of emerging "great power rivalry" and the growth of "offensive cyber operations", would be able to build on the 2015 outcome and make real progress. Now that the results are in concerned observers are better placed to render an assessment on this key question. This analysis will be structured along the six themes the report is built around plus considering the fate of two of the most "action-oriented" proposals submitted to the OEWG (namely the National Surveys of Implementation and a Programme of Action) and providing some conclusions on multi- stakeholder involvement and the future course of action.

Section A Introduction:

The introduction provided a summary of the UN action that preceded the initiation of the OEWG and tried to capture some of the positive spirit that has informed it. In this light the report notes in para 6 "the international community's shared aspiration and collective interest in a peaceful and secure ICT environment for all and their resolve to cooperate to achieve it".

Section B Conclusions and Recommendations:

Existing and Potential Threats:

The report tries to characterize the current threat landscape, but the language here generally has been muted as several states opposed the more direct calls by some to condemn the growing "militarization" of cyberspace and the increasing trend of states to acquire "offensive cyber capabilities". The argument was made that it wasn't the existence of such capabilities that should be of concern, but only how they were employed. Thus in para 15 , it is blandly noted that "Harmful ICT incidents are increasing in frequency and sophistication" and in para 16 states "recall" that "several states are developing ICT capabilities for military purposes" and that the "use of ICTs in future conflicts between states is becoming more likely" without relating these two phenomena to each other. Para 18 echoes the 2015 prohibition norm regarding critical infrastructure in concluding that "there are potentially devastating security, economic, social and humanitarian consequences of malicious ICT activities" on such infrastructure. This section concludes (in para 22) that "In light of the increasingly concerning digital threat landscape…States underscored the urgency of implementing and further developing cooperative measures to address such threats". While expressing a sense of urgency is appropriate this section doesn't reflect it and stipulates no new measures of restraint on state cyber operations beyond their borders.

Rules, Norms and Principles of Responsible State Behaviour:

This core section is largely a reaffirmation of what states have already pledged to do some six years earlier. There are references back to past resolutions, but little in the way of any advance on the past agreed norms. Characteristic of the 'treading water' nature of this section is the para 27 statement "States affirmed the importance of supporting and furthering efforts to implement norms by which states have committed to be guided at the global, regional and national level". Similarly, para 32 of the recommendations is a verbatim reiteration of the 2015 agreed norm against targeting critical infrastructure. Is sheer repetition of a norm likely to make it any more respected in practice, especially when the last few years have been marked by a disturbing rise in reports of state conducted offensive cyber operations doing just that?

International Law:

Although the GGE reports established the principle that international law applies to cyberspace and the conduct of states within, how exactly the law applies to the activities of states remains an open question. Indeed, disagreements over this issue was the principal reason for the failure of the 2016-17 GGE and has continued to cast its shadow over the OEWG proceedings. The final report represents a simple reiteration of the status quo and its recommendation in para 40 consists of suggesting that "States continue to study and undertake discussions within future UN processes as how international law applies to the use of ICTs by States as a key step to clarify and further develop common understandings on this issue". This kicking the problem down the road was disappointing, if foreseeable given the views of influential states. The fact that IHL is only operable in a state of armed conflict has led some states to take the view that such a condition should not be allowed to occur in cyberspace. Even the ICRC's plea to insert text to affirm the applicability of international humanitarian law to the cyber realm, while asserting that this did not represent condoning the militarization of cyberspace or legitimizing cyber warfare, was rejected.

Confidence Building Measures:

Confidence Building Measures (CBMs) have been a mainstay of past GGE reports and the OEWG sings their praises without providing much in the way of new material or direction. A paean to the various benefits of CBMs is given in para 41, such as the statement "CBMs can also support implementation of norms of responsible behaviour, in that they foster trust and ensure greater clarity, predictability and stability in the use of ICTs by States". No new CBMs however are put forward unless one counts a recommendation in para 51 that "States, which have not yet done so, consider nominating a Point of Contact, inter alia at technical, policy and diplomatic levels" and that "States are also encouraged to continue to consider the modalities of establishing a directory of such Points of Contact at the global level". Continuing to consider rather than taking action, regrettably marks this section as it does several others in the OEWG report.

Capacity Building:

This subject which had already featured in earlier GGE outputs received further elaboration in the OEWG report, which flagged that capacity building was an important aspect of the international cooperation required to achieve the "open, secure, stable, accessible and peaceful ICT environment" that has been the established goal of the UN process. In para 56 a set of principles for guiding capacity building efforts is provided which could prove a useful reference in future. This section also contains an apparent endorsement of the "National Survey of the Implementation of UNGA Resolution 70/237", an Australian-Mexican proposal submitted to the OEWG for regular reporting on the national implementation of agreed norms. Although still appearing with the "on a voluntary basis" caveat, and uniquely in the context of sharing information on capacity building efforts, the report's suggestion that states may wish to employ this model for exchanging information, represents the only endorsement of a substantive proposal previously presented to the OEWG in its final report.

Regular Institutional Dialogue:

Although earlier GGEs had called for the continuation of a "regular, institutional dialogue under UN auspices" there were high hopes that the OEWG would provide actionable guidance on what form such a dialogue would take. Matters were complicated however when the UN General Assembly adopted a resolution (75/240) in December 2020, well before the conclusion of the current OEWG, that created a new OEWG to operate from 2021 to 2025 with essentially the same mandate. To many observers this action seemed to be pre-judging the outcome of the current OEWG.

This issue of follow-on became all the more acute in light of the presentation by some 50 states of a proposal for a "Programme of Work" lightly modeled after the 2001 UN Programme of Work on Small Arms and Light Weapons. This Programme had as one of its principal features the consolidation of the UN's work on international cyber security into a single permanent forum which would hold regular meetings as well as review and ad hoc thematic sessions and which would be provided with secretariat support. This proposal was the most practical and results- oriented option submitted to the OEWG. It was in line with ICT4Peace's long-standing call to institutionalize the UN's work on cyber security by establishing under the General Assembly a "Committee on Cyber Security" and provide that committee with dedicated secretariat support via a UN "Office of Cyber Affairs".

The Programme, however, did not enjoy universal support which meant in the end it could only be acknowledged as one proposal among others. This lead to the final report's statement in para 77-"States note a variety of proposals for advancing norms of responsible state behaviour in ICTs, which inter alia support the capacities of States in implementing commitments in their use of ICTs, in particular the Programme of Action…In this regard the Programme of Action should be further elaborated including at the OEWG process established pursuant to General Assembly resolution 75/240"

In so far as the OEWG offers any guidance as to the nature of the body which would carry out the regular, institutional dialogue, it is contained in para 74: "States concluded that any future mechanism for regular institutional dialogue under the auspices of the UN should be an action- oriented process with specific objectives, and building on previous outcomes, and be inclusive, transparent, consensus-driven and results-based". Of course, the real challenge is devising a mechanism that meets these general criteria and which can finally demonstrate an on-going and substantive capacity at the UN to deal with the many issues relating to international cyber security.

Multi-stakeholder Participation:

The OEWG Final Report, as its proceedings throughout, suggest a mixed message with regard to participation of non-governmental stakeholders. Ambassador Lauber demonstrated a commitment to engaging such stakeholders and created the important enduring legacy of the dedicated OEWG website in which submissions from all categories of participants were treated in an equitable fashion. Regrettably however, many non-ECOSOC accredited civil society and private sector entities that sought accreditation to the OEWG were refused. While a successful session was held in December 2019 providing for a substantive exchange of views with non- governmental stakeholders and official delegations, this had to be conducted as an "informal" meeting separate from the OEWG and presided over by a chairperson from outside of the OEWG. In the final session of the OEWG, non-governmental stakeholders were excluded completely even though a few states took it upon themselves to organize informal virtual consultations on the report which probably strengthened the Chair's hand in issuing his summary. Lip service is paid at several points in the final report to the complementary role of non-governmental stakeholders, but no redeemable guarantees are issued regarding their rights to be meaningfully involved in any future process. The most on offer is an acknowledgment in para 71 that states affirm the importance "of identifying appropriate mechanism for engagement with other stakeholders in future processes".

Conclusions:

The OEWG in its work from September 2019 to March 2021 provided an important forum for discussing issues relating to international cyber security affairs and the role of the UN in dealing with this subject matter. On the basis of the Final Report, an observer can conclude that modest progress has been made with respect to this work and the group's mandate. Many in the stakeholder community would have wished for more concrete results emerging from the OEWG, along the lines of the "Programme of Action" proposal. The fate of this proposal will now be largely up to its sponsors and friends. Will they be content to continue its "elaboration" over the next five years of the new OEWG, or will they want to press for more rapid action, perhaps through a UN General Assembly resolution to initiate a dedicated process to develop its text and modalities. To be successful in such an endeavour would however require expanding the support base well beyond the original sponsors.

A fundamental deficiency in the OEWG Final Report is the total absence of the concept (and even the very word) of "accountability". ICT4Peace and many in civil society felt that agreement on norms of responsible state behaviour would have little real impact if they were not accompanied by some form of mechanism to hold states to account for their cyber security actions. This concern underpinned ICT4Peace's proposal for establishing a "Cyber Peer Review" mechanism which would have provided for a state-led review process coupled with input from the wider stakeholder community. The absence of the "accountability" theme in the Final Report of the accountability imperative was especially disappointing as throughout the period of the OEWG's existence media reports were filled with alarming accounts of state offensive cyber operations, several of which were in direct contravention of the agreed 2015 norms.

After twenty plus years of UN discussions of ICT in the context of international security, we still seem some way off from creating an inter-governmental forum to be the "go to" institution for dealing with this subject matter on a regular basis. No one believes the challenges of international cyber security policy and practice are going away any time soon and these challenges are likely to take on ever greater significance for global security and well-being. The OEWG has provided a modest impetus to this endeavour, but much more is required of states and stakeholders alike if the goal of a "peaceful ICT environment" is ever to be attained.

Paul Meyer
Senior Advisor, ICT4Peace Foundation Geneva

ANNEX I

ICT4Peace Engagement in the UN OEWG:

As an NGO officially accredited to the United Nations, ICT4Peace was an active participant in the UN OEWG process from the start. The following is a compilation of official submissions by ICT4Peace to the OEWG:

ICT4Peace Submission to the UN Open Ended Working Group (OEWG) on ICT and International Security

August 4, 2019

We commend the OEWG's openness to input from civil society, academia and the private sector and ICT4Peace will look forward to contributing to its work through a sustained dialogue.

The 2015 report of the UN Group of Governmental Experts (GGE) noted that even as ICTs have grown in importance for the international community, "there are disturbing trends that create risks to international peace and security. Effective cooperation amongst states is essential to reduce these risks".

More recently, the Secretary General, in connection with his Agenda for Disarmament, has warned that malicious activity in cyberspace has already been directed at critical infrastructure with serious consequences for international peace and security. It is incumbent on the international community to work to counter such threats and to ensure the "secure and peaceful ICT environment" that your authorizing resolution (A/RES/73/27) stipulates. The OEWG represents the latest installment of the 20-year UN endeavour to address developments in ICTs in the context of international security. This effort has yielded some important results, notably the consensus GGE reports of 2010, 2013, 2015. Yet these positive findings have not been adequately reflected in the actual conduct of states in pursuit of a "militarization" of cyberspace. With increasing reports of state-conducted offensive cyber operations including the targeting of critical infrastructure in other countries, promoting adherence in practice

to UN identified norms of responsible state behaviour is vital. If the international community is to foster digital human security alongside cybersecurity for states it will need to keep pace with these developments and ideally steer them towards cooperative ends.

It is our hope and expectation that the OEWG will deliver results that tangibly contribute to conflict prevention and preserve cyberspace as a realm for peaceful purposes. In doing so it will need to build on the accomplishments of the past, while "further developing" these and promoting their implementation. ICT4Peace believes the following norms merit priority attention:

1. Non-targeting of critical infrastructure including devising common understandings as to what constitutes such infrastructure.
2. Non-targeting of Emergency Response Teams (e.g. Computer Emergency Response Teams and Cybersecurity Incident Response Teams).
3. Non-involvement of these Emergency Response Teams in offensive cyber operations.
4. Non use of proxies by states in conducting offensive cyber operations.
5. Responsibility of states to prevent or prosecute malicious cyber activity originating from their territory.
6. Commitment to a responsible disclosure of vulnerabilities to help preserve the integrity of cyberspace and transparent policies for handling such vulnerabilities.
7. Transparency of policy and doctrine governing state offensive cyber operations. In addition to developing these norms, which have already been generated by the UN GGE processes, we suggest that the OEWG also develop proposals for dealing with four other pressing problems:

Attribution: The necessity for substantiation of "accusations of organizing and implementing wrongful acts brought against States" is acknowledged in Resolution 73/27, but if this norm is to be implemented it will require a reliable attribution mechanism. ICT4Peace sees merit in developing a neutral, international cyber attribution agency which could take the form of a public-private partnership drawing upon capabilities in the private sector. ICT4Peace has published a paper on this theme: https://ict4peace.org/wpcontent/uploads/2018/12/ICT4Peace-2019-Trust-and-Attribution-in-Cyberspace.pdf

Disinformation, Hate Speech and political Interference: These actions affect every means of expression at both national and international levels, but ICTs, including social media, substantially increase their impact. Any norm in this regard to be observed in practice will require definitional and operational elaboration. As these issues are somewhat distinct from the international security context of the OEWG and could complicate its efforts, ICT4Peace suggests that separate fora may be tasked with this work.

Export Controls: There has been increasingly concern expressed about sophisticated cyber surveillance equipment being misused by some states to monitor individuals and impinge on their civil and privacy rights. ICT4Peace would like to see the OEWG develop a recommendation that would require states to include such equipment and software in their national export control regimes.

AI and Cyber Security: The potential of Artificial Intelligence to amplify some of the problematic aspects of current state conducted cyber operations will require extension of the normative framework for responsible state behaviour in cyberspace to this potent new technology. The OEWG could draw upon the earlier work of the CCW's GGE on Lethal Autonomous Weapons (LAWS) in formulating initial guidance in this regard.

Finally, we would like to stress that the cumulative economic and financial cost of cyber incidents to national economies and in particular developing and emerging economies have become enormous. Therefore, it has become evident, that national cybersecurity building has become a necessary state function. However, many developing countries lack the necessary resources to build and maintain the required national cybersecurity institutions and technical and human capacities. Cybersecurity therefore must become a priority in national development strategies and cooperation agreements. The need for cybersecurity capacity building in developing countries has already been highlighted in the UN GGE 2015 report and should also be reflected in the OEWG outcomes.

Daniel Stauffacher
President, ICT4Peace
danielstauffacher@ict4peace.org

Critical Infrastructure and Offensive Cyber Operations A Call to Governments

October 21, 2019

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[13].

"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".

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 same 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[14]. 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,

13 *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

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

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 civilian nature, damaging cyber operations have already occurred against them, by states and non-state actors alike[15]. 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.

15 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 cyberattacks and describing the impact on specific civilian sectors (pp 54-67) is particularly useful.

Statement by ICT4Peace to the OEWG on Cybersecurity, UN HQ, Sept 10, 2019,

September 10, 2019

Mr. Chairman, Excellencies, distinguished representatives, colleagues,

On behalf of ICT4Peace I am pleased to have this opportunity to address the inaugural session of the Open-Ended Working Group (OEWG) on "Developments in the field of information and telecommunications in the context of International Security".

After almost two decades of UN work on developing "norms for responsible state behaviour" in cyberspace, a new, inclusive process for advancing this goal has been established. We believe the need for such norms has become all the more pressing, as some state conduct in cyberspace threatens to transform this unique, human created environment into just another "warfighting domain" in the eyes of some.

Fortunately, earlier UN processes have generated a significant body of norms which would serve the goal, as expressed in your authorizing resolution, of preserving a "secure and peaceful ICT environment". We urge states participating in this OEWG to lead by example in implementing the norms already identified in the 2010, 2013, 2015 GGEs. As indicated in our submission to the OEWG, we believe of the eleven, these seven norms merit priority attention:

1. Non-targeting of critical infrastructure including devising common understandings as to what constitutes such infrastructure
2. Non-targeting Computer Emergency Response Teams (CERTs)
3. Non involvement of these Computer Emergency Response Teams (CERTs) in offensive cyber operations
4. Non use of proxies by states in conducting offensive cyber operations
5. Responsibility of states to prevent or prosecute malicious cyber activity originating from their territory
6. Commitment to a responsible disclosure of vulnerabilities to help preserve the integrity of cyberspace
7. Transparency of policy and doctrine governing state offensive cyber operations.

We would like to see the OEWG further develop these existing measures with a view to operationalizing them as soon as possible. In the absence of an energetic assertion of these norms we risk leaving cyberspace vulnerable to whatever some cyber 'warrior' decides is advantageous.

ICT4Peace has already spoken out against the deployment of malware by states into foreign electricity grids threating the disruption of infrastructure critical for public use. If states are not going to abide by a key principle of conduct that their representatives have agreed to in the UN context, we will all suffer. International experts convened at a meeting last year by the International Committee of the Red Cross have voiced their concern regarding the upswing in major cyber-attacks including those affecting the functioning of electricity networks, medical facilities and nuclear power plants. These findings are a stark reminder of the vulnerability of essential civilian infrastructure to cyber-attacks and of the significant humanitarian consequences that may ensue.

Be it in a state of armed conflict or not, ICT4Peace believes that the prohibition on targeting critical infrastructure by cyber operations should be publicly acknowledged by states and put into practice.

This should be a priority task for the OEWG to accomplish in line with its mandate to "further develop the rules, norms and principles of responsible behaviour of States". As the Secretary General noted in his Agenda for Disarmament, he foresees a personal role in the prevention and peaceful settlement of cyber conflict and in "fostering a culture of accountability and adherence to emerging norms, rules and principles on responsible behaviour in cyberspace". It is the current lacking of accountability for "irresponsible state behaviour" that has frustrated many of us in civil society who wish to preserve this hugely important cyberspace as a zone of peace.

In this exercise of accountability, we think the "attribution" issue requires considerable work with a view to devising mechanisms of impartial attribution of internationally wrongful acts. ICT4Peace has put forward one possible model which could lay the basis for such an attribution capacity and I refer you to our submission for further details.

The challenges posed by offensive cyber operations are not solely the concern of states and companies. Individuals and communities have been harmed through mass campaigns of disinformation and the propagation of hate speech. Ethnic cleansing and sectarian violence have been promoted through nefarious cyber operations. These abuses must be countered with determination. A human-centered security approach should also be considered by the OEWG.

Effectively addressing the myriad of challenges posed by offensive cyber operations will require the engagement of the private sector and civil society as well. We have been encouraged by the provisions the OEWG have made for receiving input from these non-governmental stakeholders. However, we hope that all NGOs, that wish to participate in OEWG process will be allowed to do so.

ICT4Peace will continue to contribute, via its programs, to the OEWG goals of confidence building and capacity building, crucial components of a sustainable cyber peace. With regards to capacity building, ICT4Peace has implemented since 2014 numerous Cybersecurity Policy and Diplomacy Courses in close cooperation with the OAS, ASEAN, AU, OSCE and the UN.

It's great that a large number of delegations are underlining the importance of cybersecurity capacity building. But I am not sure that the need for cybersecurity capacity building has sunk in as a true development priority in the international development debate as yet. ICT4Peace has tried in the past, to raise the awareness and recognition of the emerging cyber security divide, but we are not sure this priority has been accepted by the Development Cooperation Agencies and Finance and Development Ministers of this world.

More work of convincing is needed.

UN OEWG Intersessional and UN GGE Informal Meetings in New York – ICT4Peace Statements

December 7, 2019

https://ict4peace.org/wp-content/uploads/2019/12/Cyber-OEWG-ISM-InterventionsDec2019.pdf

After having participated in the First substantive session of the OEWG – New York, 9-13 September 2019, where ICT4Peace delivered the following statement , along with a written submission of its views, ICT4Peace participated also in the OEWG Intersessional Meeting and as well as the UN GGE Informal Meeting (2 to 6 December 2019).

Amb. (ret) Paul Meyer and Dr. Elaine Korzak, representing ICT4Peace, made inter alia the following three main points:

1. **A Call to Governments: Critical Infrastructure and Offensive Cyber Operations**
2. **Trust and Attribution in Cyberspace: An ICT4Peace proposal for an independent network of organisations engaging in attribution peer-review**
3. **ICT4Peace Matrix on on National and International Goals and Measures of Cybersecurity" of 2018**

The transcripts of the Interventions by Amb. (ret) Paul Meyer on behalf of ICT4Peace can be found here:

December 2 (morning session)

"In the spirit of promoting an interactive discussion I refer to the earlier interventions of colleagues from FIRST and the Cyber Peace Institute to ask if there is a trend with respect to the degree of discrimination occurring in state -conducted cyber operations. The world was shocked by the damage inflicted by the "Not Petya" attack in 2017 that had effects far removed from the original target in Ukraine to cause multi-million dollar damage to a global shipping company, disrupted hospitals in the UK and destroyed data at many small and medium enterprises across the globe.

Whether these indiscriminate effects were accidental or intended is not clear, but it

underlines how state cyber operations seem have paid scant attention to protecting the rights of citizens.

In order that the civilian owners and users of cyberspace do not end up as mere "collateral damage" we need to act to reinforce the norm of a "secure and peaceful ICT environment".

To this end, ICT4Peace has issued a Call to Governments: Critical Infrastructure and Offensive Cyber Operations (the text of which is available on our website) that seeks to have states proactively confirm that they will abide by the agreed prohibition on targeting critical infrastructure in policy and practice.

December 2 (afternoon session)

In the context of the OEWG, we are building on the acquis of earlier multilateral diplomacy, notably the consensus results of the three UN GGEs. While all eleven of the norms agreed by the 2015 GGE are worthy of implementation, ICT4Peace puts special emphasis on the prohibition on damaging cyber operations targeting critical infrastructure. Given the increasing dependence on such infrastructure and the dependence of that infrastructure on the proper functioning of computer systems, attacks that damage or disable the normal operations of this infrastructure could have an enormous impact on human security and societal well-being.

Despite the fact that the norms on protecting critical infrastructure were agreed four years ago, there still have been disturbing reports on state-conducted operations that have targeted such infrastructure, electricity grids in particular. In this light, ICT4Peace has in October issued a Call to Governments: Critical Infrastructure and Offensive Cyber Operations urging states, especially those possessing offensive cyber capabilities, to publicly confirm that will respect the norm prohibiting cyber operations directed at critical infrastructure at all times. Not only will this action help reinforce the standing of the norm but will provide a proactive means of assuring the international community that these states are committed to acting in a responsible manner in cyberspace.

We believe that this prohibition should be respected at all times, given the continued debate over the threshold of an "armed conflict" in the cyber realm (triggering IHL) and the fact that damaging cyber operations are being carried out in peacetime. The 2015 GGE also did not condition their recommended prohibition on cyber operations against critical infrastructure in this way.

ICT4Peace agrees that the focus of the OEWG should be on operationalizing the existing norms agreed through the UN GGE process, rather than engaging in a proliferation of norms. There is one additional prohibition however that may merit consideration – a ban on cyber operations directed at nuclear facilities. While the critical infrastructure prohibition would cover operations against civilian nuclear facilities, nuclear weapon complexes should also be protected. As think tanks such as Chatham House and the Nuclear Threat Initiative have produced papers addressing this threat and eminent experts are now calling for a specific prohibition on any cyber operation targeting a nuclear weapon complexes, it would be appropriate for this further norm to be considered by this First Committee body.

December 3 (morning session)

We recognize the Paris Call on Trust and Stability in Cyberspace as an impressive effort to provide a broad-based endorsement of core principles to govern behaviour in cyberspace. Although there are a large number of supporters from international and civil society organizations (over 300) and from the private sector (over 600), to date the Paris Call has only been endorsed by 74 states. This is less than half of the UN membership and notably several leading states are conspicuous by their absence: US, Russia, China, India, Brazil, South Africa, Indonesia and Iran to name a few. If our aim is to ensure responsible state behaviour in cyberspace, it is evident that we will need to bring these states on board.

The resolution establishing this OEWG flagged the necessity for substantiation of "accusations of organizing and implementing wrongful acts brought against States". If this objective is to be realized, it will require a reliable attribution mechanism. The Secretary General in his Agenda for Disarmament has also stressed the need to foster a culture of accountability for cyber activity. ICT4Peace sees merit in developing a neutral, international cyber attribution mechanism, which could take the form of a public-private partnership drawing upon expertise in the technical security community, ICT firms, academia and civil society.

Last year ICT4Peace published a paper on this subject Trust and Attribution in Cyberspace. It foresees a network of contributors providing a "fact finding function" and a type of "peer review" that could consider attribution judgments and provide a forum for accountability. Reference was made yesterday to the "Universal Peer Review" mechanism established by the Human Rights Council and this could provide a possible model for a cyber security equivalent.

The ICT4Peace paper is designed to stimulate more detailed consideration of how to develop such an accountability/attribution mechanism under UN auspices. Devising a mechanism could even be a "deliverable" for this OEWG process.

We have made major collective progress in identifying key norms via the UN GGE reports and through other inputs such as those proposed by the Global Commission on Stability in Cyberspace. At the same time, we must recognize that a list of norms for responsible state behaviour without some complementary accountability mechanism could end up as a "to do" list that is never really acted upon.

ICT4Peace Proposed[16] "States Cyber Peer Review Mechanism" for state-conducted foreign cyber operations

March 1, 2020

It has been generally acknowledged that some form of mechanism to hold states to account for their cyber operations affecting other states would be desirable. Such a mechanism would be premised as a cooperative process that would be state-centric, but which would also provide for the input of other stakeholders. Among existing models, the Human Rights Council's Universal Periodic Review (UPR) mechanism[17] is especially relevant to the cyber security context in its combination of state-led mutual examination and NGO input and participation. The Universal Periodic Review applies to all 193 UN member states with a periodicity of approximately once every 4.5 years. While this timing and scope is appropriate for the scrutiny of human rights implementation, something more selective and frequent for foreign cyber activity would be preferable.

It is suggested that the initial scope of the cyber peer review (CPR) would be those states which have declared a capability for offensive cyber operations by their militaries or foreign intelligence agencies. These states (estimated at some 30) merit being the focus of scrutiny due to their practical capacity to engage in projecting cyber force beyond their borders and their declared commitment to abide by international

16 ICT4Peace has launched this proposal at the second substantive Meeting of the UN Open Ended Working Group (UN OEWG) from 10 to 14 February 2020 at the United Nations New York, (See ICT4Peace Statement).

17 [2] Human Rights Council's Universal Periodic Review (UPR) mechanism.

law in their cyber operations. The smaller subset would also permit the CPR to have a more regular periodicity, perhaps on an annual basis. On this basis the CPR would consist of the following six stages:

1. State under Review (SuR) would submit a report on its foreign cyber activity and its implementation of agreed UN norms of responsible state behaviour in cyberspace.

2. Other stakeholders could submit their own input regarding the conduct of the SuR.

3. Secretariat would compile these reports and post them to publicly accessible website.

4. A working group of three states not part of the CPR pool would hold a halfday session with the SuR after which it would prepare a report with findings/ recommendations.

5. The SuR would have the opportunity to submit a written response to the WG report.

6. The WG report plus SuR response would be forwarded to an oversight body which would hold each year one-hour long sessions per state for consideration of these inputs with provision for oral statements by the SuR, other states and other stakeholders. The oversight body could be the First Committee, a subsidiary body of the First Committee or some other intergovernmental forum assigned this task. The CPR session would be webcasted and documents posted to the CPR website. Costs could be limited by incorporating the CPR into the work program of an existing body. The private sector might be encouraged to contribute to a CPR fund given its interest in accountability.

This basic framework would respect the principle of a transparent, state-led review mechanism incorporating input from civil society and the private sector. It would enable those states possessing the capability for offensive cyber operations to reassure the international community that these capabilities were being employed in a manner consistent with international law and agreed UN norms of responsible state behavior. The establishment of such a CPR mechanism would be a worthy recommendation from the OEWG and would represent a proactive response to the threat to international peace and security posed by unrestricted state-conducted foreign cyber operations.

The proposed CPR would be in support of the proposal by the **Mexican delegation** to establish a review or reporting mechanism to monitor the implementation of norms and to identify and share best practices in this area[18].

Paul Meyer
Senior Advisor ICT4Peace

Statement by ICT4Peace to Second OEWG Session February 10-14, 2020, UN HQ

February 10, 2020

Dear Chairman, members of the Secretariat and distinguished delegates,

We are grateful to address again this important Open Ended Working Group. The Chairman through his working paper has provided us with a helpful framework for focusing the work of this second substantive session.

In describing the existing and potential threats posed by irresponsible state behaviour in cyberspace, we consider that the threat to international peace and security should be preeminent. In the context ofits First Committee origins, the OEWG's efforts should focus on stepsto maintain the "cyber peace" at a time of rising geopolitical tensions and an expansion of offensive cyber capabilities on the part of several states.

When it comes to offensive cyber operations, thereis considerable debate as to how existing international law applies to specific state uses of ICTs. While we would welcome the negotiation of legally binding prohibitions on some offensive cyber actions, we recognize that in the near term, adherenceto politically binding measures, such as those generated by the 2015 GGE, is probably a more feasible goal.

The Chair has posed the question as to whether member states should "..unilaterally declare to refrain from militarization/offensive use of ICTs?".

We answerin the affirmative and remind delegates of ICT4Peace's "Call on Governments" to publicly confirm that they will refrain from offensive cyber operations targeting critical infrastructure. This would be a proactive meansfor states

18 The proposed CPR would also complement the ICT4Peace proposal for an independent network of organizations engaging in attribution peer-review, see link here

to demonstrate their commitmentin policy and practice to this agreed UN GGE norm.

We also believeit is time for sophisticated cyber/Al surveillance systems to be brought morefully into export controls as a means of preventing human rights abuses.

The Chair has flagged "attribution" as one of the issues which might require additional norms for responsible State behaviour. We believe attribution is a critical precondition for achieving accountability for state conductin cyberspace. Capacity for objective, welldocumentedattribution for malicious cyber activity should be developed as a matter of urgency.

ICT4Peace has circulated a paper and launched pilot "peer-review" process, describing one mechanism for collecting this information, drawing upon the expertise residing in the private and civil sectors. We consider that such a solid information base would complement an eventual "Peer Review Mechanism" that could serve as an inter-governmental forum for holding states to account over their cyber actions. The Human Rights Council and its Universal Periodic Review remains a relevant modelin this regard.

We support the goal of the Mexican proposal to encourage reporting by states on their implementation of norms, but believe this should be but one input to a "peer review mechanism" that would provide for interactive discussion of state conduct.

In addition, in our view, the current and future importance of cyberspace for international peace and prosperity warrants a dedicated forum under UN auspices to enable on-going consideration of international cyber security-related issues. Suitable secretariat support would be required for such a forum.

Perhaps the time has come for the UN to establish an "Office of Cyber Affairs" as a manifestation of the importance the UN Secretary General has assigned to these issues through the HLP on Digital Cooperation and the preparations for the upcoming 75" Anniversary of the founding of the United Nations.

In conclusion, ICT4Peace has high expectations for this WG's output which it believes can only be enriched by the continued input from industry, academia and civil society as evidencedin the productive inter-session meeting of last December. ICT4Peace stands ready to support this group through its capacity building and other work as it has done over the past 15 Years.

Comments 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

March 27, 2020

Dear Ambassador Lauber,

Many thanks for the kind opportunity to comment on your Initial "Pre-draft" of the report of the OEWG on developments in the field of information and telecommunications in the context of international security.

First, and while recognizing the challenges of integrating views from a diversity of stakeholders, we would like to see the report display a higher level of ambition overall.

Although in para 7 of the "Pre-draft" the OEWG acknowledges that it has benefited from exchanges with non-governmental stakeholders, there seems little reflection of their views in the text as it stands.

Several principal themes expressed at the 2-4 December 2019 multi-stakeholder session (and captured in the Chair's summary report of that session) fail to appear in the "Pre-Draft". In particular we would flag the absence of the "human centric" approach that was well-expressed in the report's reference in para 14 to the requirement for "a human-centric, rights-based approach that also emphasizes shared responsibility and accountability."

Indeed, the crucial concept of accountability does not figure in the text, despite the fact that the report of the December discussions devoted a whole section to it (paras 57-60). References to the idea of a "Peer Review Mechanism" raised by several representatives in December and which would be one manner of addressing accountability are also absent. ICT4Peace has already submitted a specific suggestion for a Cyber Peer Review Mechanism which builds on an earlier Mexican proposal to require state reporting on implementation of norms.

Beyond having the Secretary General compile future inputs from states or regional organizations, it will be important for the OEWG report to provide more guidance as to how agreed norms of responsible state behaviour can best be operationalized and promoted. In this regard, the norm of non-targeting critical infrastructure is of prime

importance. ICT4Peace's proposal for states possessing offensive cyber operations to proactively confirm that they will respect this constraint at all times is one concrete way of demonstrating that commitment (para 41 of the December report refers).

At this juncture in global cyber security activity, we consider simply extending the two existing processes is an inadequate response to the challenge of ensuring a regular and rationalized institutional dialogue on this subject matter in the UN context. The time has come to signal that a dedicated inter-governmental forum with secretariat support is required by the UN.

ICT4Peace believes that the OEWG exercise could benefit from reflecting in its outcome document more of the input of civil society and private sector stakeholders, which would impart greater credibility to its eventual recommendations."

Sincerely,
Dr. Daniel Stauffacher
Former Ambassador of Switzerland
President, ICT4Peace Foundation

Comments by ICT4Peace on Chair's Revised Pre-draft Report – OEWG

December 18, 2020

This revision represents further progress in the effort to define an outcome of the OEWG in line with the importance of its subject matter. In our view, the OEWG's report must go beyond providing a "snapshot" of the current challenges facing global cyber security policy and chart a clear course for the UN to follow in managing these challenges going forward. In this regard we believe the following aspects of the revised pre-draft report need to be reinforced: i) restraint on offensive cyber operations; ii) accountability; iii) institutional support and iv) the role of non-governmental stakeholders. This submission will cover each of these themes in turn.

Restraint on Offensive Cyber Operations

The OEWG has recognized the pernicious effects of the "malicious use of ICTs carried out by State actors, including use of proxies" and that such use can have "significant and far-reaching negative impacts". The revised pre-draft report observes that "the use of ICTs in future conflict between States may become more likely", "absent a culture of restraint". It is correct that the report recognizes the crucial role of restraint on the offensive action of states in cyberspace, but "culture" is too amorphous a term to describe the degree of restraint required. To be effective and demonstrable, actual "measures" of restraint are needed. In other words, a framework of agreed measures and rules of restraint should be put in place to operationalize the existing norms that restrict the scope of state cyber operations that project power beyond their own borders.

Amongst the existing norms, ICT4Peace has long emphasized the primacy that should be shown the norm for the protection of critical infrastructure against cyber attacks. It is appropriate that the revised pre-draft report draws attention to "The potentially devastating human cost of attacks on critical infrastructure..."and proceeds to cite a few sectors, namely, "medical facilities, energy, water and sanitation". In our view the report should either enumerate a more comprehensive list of "critical infrastructure" or simply utilize that established term as there is a risk, in the context of protection, in specifying only a few sectors as it could leave the impression that those not named are legitimate targets. Given the importance of critical infrastructure to public well-

being, ICT4Peace has advocated for governments to go beyond the tacit agreement of this norm and publicly confirm that it will be fully respected in state policy and practice (cf "Call to Governments" proposal).

Accountability

The concept of accountability for state action largely remains absent from the revised pre-draft report. Against the acknowledged backdrop of increasing "harmful ICT incidents" it could well prove futile to call for responsible state behaviour without a mechanism to hold states to account for their cyber conduct. The interests of the wide non-governmental stakeholder community demand no less. Such a mechanism is all the more important as states continue to engage in stealth offensive cyber operations, refusing to acknowledge their responsibility for interference with foreign computer systems. ICT4Peace favours a "peer review mechanism" as have been developed in other areas of UN activity, notably the Human Rights Council's Universal Periodic Review mechanism, which allow states to take the lead in an equitable and collective process of a review of conduct while providing for inputs from concerned nongovernmental entities. An endorsement of this or some similar accountability process should figure in the OEWG's outcome.

Institutional Support

The UN and specifically the First Committee of the General Assembly has been engaged with the subject of international cyber security policy for over twenty years. Frankly the time is overdue for this consideration to progress beyond ad hoc discussions and find an institutional home for on-going management of subject matter that has grown immensely in importance for global security and prosperity over the last two decades. As ICT4Peace noted in its March 2020 submission: "The time has come to signal that a dedicated inter-governmental forum with secretariat support is required by the UN".

We are encouraged that the "Programme of Action" proposal currently before the OEWG has recognized the need for a permanent body that would be the venue for annual meetings, quadrennial review conferences and occasional thematic sessions. ICT4Peace believes that it is time for the UN to establish a standalone "Committee on Cyber Security" under the authority of the General Assembly. Such a committee should also be supported by a dedicated secretariat fashioned as a UN "Office of

Cyber Affairs". The existence of a permanent forum would also incentivize states to prepare the type of reports on implementation being advocated in the joint proposal before the OEWG as it would ensure such reports were subject to consideration at a diplomatic forum. The "Programme of Action" reflects the type of concrete result we would like to see the OEWG produce.

Role of Non-Governmental Stakeholders

To ensure the credibility of any eventual OEWG outcome it will need to integrate participation by other stakeholders in the future inter-governmental work. Enabling real-time participation by stakeholders in an observer capacity should be part of any institutionalized follow-up. Civil society and the private sector can bring much of benefit to the UN's future work on cyber security as well as being partners to governments in implementing programs that contribute to a productive and peaceful ICT environment.

Comments by ICT4Peace on the "Zero Draft" report of the UN Open Ended Working Group

February 2, 2021

We appreciate the evident efforts made in this "Zero Draft" to produce a cogent and accessible report prior to the OEWG's final session this March. It is generally a well-balanced account of the discussions that have taken place in the OEWG across its major themes. ICT4Peace would like to see a greater focus in the report on the future course of action recommended for this subject matter within the UN context, rather than a record of discussions. We offer the following comments on the present text with the view to enhancing the report's ultimate utility to the international community including concerned non-governmental stakeholders.

Our principal concern remains with the absence of the concept of "accountability" in the report. Experience has shown that a set of norms without any accompanying accountability mechanisms regarding their implementation is unlikely to be respected in practice. Regrettably the only time in the current text that the word "accountability" even appears (para 36) is part of a six-line, opaque sentence in which better understanding of "sources of ICT incidents" is somehow to produce "greater accountability and transparency". We would suggest substituting here a

concise sentence along the lines of "States agreed that greater transparency and accountability for their cyber operations would constitute a confidence-building and conflict prevention measure."

In terms of what form the desired accountability mechanism should take, we refer to our earlier proposal for a "Cyber Peer Review Mechanism". In the context of international cyber security, a state-led process of review that also provided for inputs from non-governmental stakeholders and publicly accessible results appears best suited to ensure a credible and effective procedure. The Universal Periodic Review mechanism of the UN Human Rights Council already provides a model and precedent for such a peer review process undertaken by states. We note that the call for accountability figured in several of the informal dialogues held in December and believe the OEWG report should acknowledge its importance for promoting responsible state behaviour in cyberspace.

We commend the priority accorded the protection of critical infrastructure in the report and its warning of the "potentially devastating humanitarian consequences" of any attack on this infrastructure. The report needs to demonstrate serious concern with the harm inflicted upon humans by irresponsible state cyber actions. While we appreciate that the singling out of "medical and healthcare facilities" (par 50) in this context is not meant to exclude other critical infrastructures, the report should include a specific statement to that effect along the lines suggested by Australia and five other states in the non-paper. ICT4Peace has earlier proposed the desirability of states possessing offensive cyber capabilities to publicly commit to respecting the prohibition on the targeting of critical infrastructure. We appreciate in this regard the report's encouragement (para 74) for states to "publicly reaffirm their commitment to be guided in their use of ICTs by the 2015 report of the GGE".

As a forward-looking report the language on how UN work on cyber security should proceed in future is of prime importance. The support expressed for "frequent and structured discussions under UN auspices of the use of ICTs" (para 96) is good but needs to be expressed in a more prescriptive manner. ICT4Peace welcomes the "Programme of Action" proposal (para 99) as providing the type of "institutionalized" follow-up that the UN urgently requires to adequately address the challenges posed by state sponsored cyber operations. ICT4Peace agrees that the "regular institutional dialogue" recommended by successive GGEs must be given practical, institutional expression. A permanent forum, with dedicated secretariat support and provision for regular and review meetings aligns with our call for the establishment of a "Cyber Security Committee" under the General Assembly to be supported by a UN "Office

of Cyber Affairs". We would like to see the OEWG report provide practical guidance regarding the form on-going UN work should take and would hope that the sponsors of the "Programme of Action" proposals can move rapidly to obtain the General Assembly's mandate to initiate its negotiation as soon as possible.

The need to involve other stakeholders in the future inter-governmental dialogue on international cyber security, both as concerned entities and eventual partners from the private sector and civil society is acknowledged at several points in this report. We note in particular the concluding reference to the "importance of identifying appropriate mechanisms for engagement with other stakeholder groups in future processes" (para 106). It would be preferable however if the OEWG report could provide more guidance as to the nature of these "appropriate mechanisms for engagement". There are models of such stakeholder engagement in other areas of the UN and given the high stake non-governmental entities have in promoting responsible state behaviour in cyberspace, we would favour a more substantive recommendation in this regard. Affirming the need for inclusive, transparent processes with non-governmental stakeholders granted equitable terms of participation, such as real-time rights to intervene in discussion, would constitute more appropriate language on this crucial aspect of future arrangements.

The OEWG's sessions have permitted frank discussion of the challenges posed to the maintenance of international peace and security of malicious cyber operations. After more than two decades of UN discussion of the cyber security issue, there are high expectations riding on the outcome of the OEWG. If the labours of the OEWG are to yield results that will truly help sustain a "peaceful ICT environment", its final report should provide an actionable blueprint as to how future UN work on this subject matter should be conducted.

ANNEX II

The following are commentaries on work of the UN OEWG and UN GGE:

Time to create a single negotiating cyber forum under the UN General Assembly First Committee

ICT4Peace in article of NZZ on recent conclusions the UN OEWG negotiations on Cybersecurity

UN OEWG & UN GGE – "REGULAR INSTITUTIONAL DIALOGUE" – FROM CONCEPT TO COMMITTEE

An International Response to Offensive Cyber Operations is long overdue

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

Disconnects in State Cyber Behaviour: Accountability for Attacks on Critical Infrastructure

UN OEWG: Accountability – The missing ingredient in the comments by states on the Chair's draft report

UN OEWG and UN GGE – Paul Meyer's Statement at Australia's UN CYBER PROCESS PUBLIC CONSULTATIONS

UN OEWG | A New Process for an Old Problem: Governing State Behaviour in Cyberspace

UN OEWG – UN Negotiations on Cybersecurity: Blog Post on the First Session of the Open-Ended Working Group at the UN in New York

An overview of the ICT4Peace activities since 2011 calling for and supporting the UN GGE and UN OEWG processes you find here.

About ICT4Peace Foundation

ICT4Peace is a policy and action-oriented international Foundation. The purpose is to save lives and protect human dignity through Information and Communication Technology. Since 2003 ICT4Peace explores and champions the use of ICTs and new media for peaceful purposes, including for peace-building, crisis management and humanitarian operations. Since 2007 ICT4Peace promotes cybersecurity and a peaceful cyberspace through inter alia international negotiations with governments, international organizations, companies and non-state actors.

The ICT4Peace project was launched with the support of the Swiss Government in 2003 with a book, published by the UN ICT Task Force in 2005 on the theory and practice of ICT in the conflict cycle and peace building[19] and the approval of para 36 of the Tunis Commitment of the UN World Summit on the Information Society (WSIS) in 2005.[20]

ICT4Peace on Twitter - www.twitter.com/ict4peace

ICT4Peace on Facebook - www.facebook.com/ict4peace

ICT4Peace official website: www.ict4peace.org

ICT4Peace additional publications: www.ict4peace.org/publications

ICT for peace foundation

19 https://ict4peace.org/wp-content/uploads/2019/08/ICT4Peace-2005-Information-and-Communication-Technology-for-Peace.pdf

20 Para *36. We value the potential of ICTs to promote peace and to prevent conflict which, inter alia, negatively affects achieving development goals. ICTs can be used for identifying conflict situations through early-warning systems preventing conflicts, promoting their peaceful resolution, supporting humanitarian action, including protection of civilians in armed conflicts, facilitating peacekeeping missions, and assisting post conflict peace-building and reconstruction.*