10 December 2021

His Excellency Ambassador Burhan Gafoor
Chair of the Open-Ended Working Group
on security of and in the use of information
and communications technologies 2021-2025
C/O The Secretariat of the OEWG
Office of Disarmament Affairs
prizeman@un.org
New York

Dear Chair

The undersigned Member-States, regional organizations, and non-governmental stakeholders would like to thank you for your proposal for the modalities for the United Nation's second Open-Ended Working Group ("OEWG") on security of and in the use of information and communications technologies (ICTs) in your letter of 15 November. We appreciate receiving this information sufficiently in advance of the convening of the first session in December for us to consider it in detail and provide our views to you.

As the final report of the first OEWG on ICTs stated, "*...the broad engagement of non-governmental stakeholders has demonstrated that a wider community of actors is ready to leverage its expertise to support States in their objective to ensure an open, secure, stable, accessible and peaceful ICT environment*"[1]. We are committed to your vision to build on the work already achieved by the first OEWG and to leverage their expertise by engaging stakeholders in a 'systematic, sustained and substantive' manner.

Rather than make proposals of specific measures we propose a set of principles that the modalities should embody which we see as fully in line with your vision and commitment to engaging with stakeholders:

1. **The participation modalities should ensure that more non-governmental stakeholders are able to meaningfully participate in formal OEWG meetings than was the case for the previous working group**. In particular there should be participants *in addition* to those already eligible due to their existing consultative status with the UN;
2. **There should be a transparent process in place regarding any objection from a Member State to the accreditation request of a non-governmental stakeholder to participate in the formal substantive meetings,** especially those who are already officially recognized by the UN in other contexts;
3. **In the event that interested non-governmental stakeholders are denied accreditation to formal OEWG sessions there should be channels for such stakeholders to regularly express their views and for those views to be available to all accredited delegations.** These channels can be convened through the good offices of the OEWG Chair as informal measures, and a facility that allows the official delegates to have access to them is essential;
4. **Sufficient time should be made available to non-governmental stakeholders to meaningfully raise their views in both formal and informal meetings** and for delegations to have sufficient time to meaningfully discuss those views.
5. **A hybrid format should be utilized for formal and informal meetings to a sufficient extent to facilitate the participation of delegates and other stakeholders who cannot travel to New York in person.** This is especially important during a global pandemic whilst so many countries do not have sufficient access to vaccines to facilitate travel and while vaccine regimes differ and given the potential for new variants to cut off travel for entire countries.

We are committed to a successful OEWG process and believe that it is likely to have a far-reaching impact on many stakeholders, including direct impacts on communities and individuals. We also hope for an open, transparent and

[1] https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf

inclusive dialogue that would provide the basis for stakeholders to play a role in implementing the decisions and which would take into consideration their means and ability to participate and contribute to the outcome. Given the subject matter of the OEWG, this is doubly true: many of the measures agreed cannot be implemented effectively without the active participation, alongside governments, of non-governmental actors. Correspondingly, addressing threats emanating from cyberspace will require leveraging the experience, expertise and resources of all relevant stakeholders.

With this in mind, our proposal reflects what we believe is required to realize a minimum level of the systematic, sustained, and substantive participation by non-state actors in the work of the OEWG. We present this, therefore, as a compromise in the interest of consensus.

Finally, Excellency, we would like to emphasize our commitment to a successful outcome of the OEWG and to actively participate in our respective capacities, and the assurances of our highest consideration.

State and regional organizations signatories

1. Australia
2. Austria
3. Belgium
4. Bulgaria
5. Canada
6. Chile
7. Colombia
8. Costa Rica
9. Croatia
10. Cyprus
11. Czech Republic
12. Denmark
13. Dominican Republic
14. Estonia
15. European Union
16. Finland
17. France
18. Germany
19. Greece
20. Hungary
21. Iceland
22. Ireland
23. Israel
24. Italy
25. Japan
26. Latvia
27. Lithuania
28. Luxembourg
29. Malta
30. Mexico
31. Netherlands
32. New Zealand
33. Norway
34. Poland
35. Portugal
36. Republic of Korea
37. Romania
38. Slovakia
39. Slovenia
40. Spain
41. Sweden
42. Switzerland
43. United Kingdom of Great Britain and Northern Ireland
44. United States

Non-governmental signatories

45. 7amleh - The Arab Center for the Advancement of Social Media
46. Africa Freedom of Information Centre (AFIC)
47. Aims360
48. APNIC
49. Archive360
50. Association for Progressive Communications
51. Australian Strategic Policy Institute

52. Avast
53. Big Cloud Consultants
54. Bitdefender
55. Capa 8 Foundation
56. Carnegie Europe
57. Carnegie Endowment for International Peace (CEIP)
58. Cornerstone IT
59. Cyber Trust Alliance
60. CyberPeace Foundation
61. CyberPeace Institute
62. Cybersecurity Tech Accord
63. Cyberspace Cooperation Initiative at ORF America
64. Digital Tanzania Initiative
65. Deloitte Consulting & Advisory
66. Derechos Digitales
67. Digital Peace Now
68. Dragos
69. DXC Technology
70. ESET
71. European Cyber Security Organisation
72. FIRST
73. F-Secure
74. G DATA CyberDefense
75. Gefona Digital Foundation
76. Global Forum on Cyber Expertise Foundation
77. Global Partners Digital
78. ICT4Peace
79. IMPENDO Inc.
80. Indonesia Cyber Security Forum
81. Integrity Partners
82. International Chamber of Commerce
83. Internet Australia, The Internet Society of Australia a Chapter of ISOC
84. Internet Society
85. Jonction
86. KICTANet
87. Madison Computer Works
88. Media Foundation for West Africa
89. Microsoft
90. NetApp
91. Northwave
92. onShore Security
93. Pax8
94. Professional Options LLC
95. Raiffeisen
96. Ranking Digital Rights
97. Red en Defensa de los Derechos Digitales
98. Resecurity, Inc
99. SafePC Cloud
100. SecureSoft Corporation
101. Siemens
102. Silent Breach
103. Tech Policy Design Centre, Australian National University
104. Telefonica
105. The Azure Forum for Contemporary Security Strategy
106. The Hague Centre for Strategic Studies (HCSS), Secretariat of the Global Commission on the Stability of Cyberspace (GCSC)
107. Trend Micro
108. U.S. Council for International Business (USCIB)
109. US Licensing Group
110. Validy Net Inc
111. WCA Technologies
112. Wipfli
113. Wisekey
114. Women4Cyber Foundation
115. Women's International League for Peace and Freedom
116. World Wide Web Foundation

Individual supporters

117. Rinalia Abdul Rahim, Senior Vice President of Strategy, Communications, and Engagement, Internet Society

118. Dapo Akande, Professor of Public International Law, Blavatnik School of Government, University of Oxford

119. Anahiby Becerril, Graduate program tutor visiting professor, UNAM

120. Joe Burton, Senior Lecturer, University of Waikato

121. Enrico Calandro, Research ICT Africa

122. Mark Carvell, Independent Internet Governance Consultant and EuroDIG Member

123. Abhik Chaudhuri, Chevening Fellow in Cyber Policy

124. Vint Cerf, Internet Pioneer

125. Ying Chu Chen, Taiwan Network Information Center

126. Dr Talita Dias, Shaw Foundation Junior Research Fellow in Law, University of Oxford

127. Ababacar Diop, President, Jonction

128. Dr. Kabir Hamisu Kura, Community Development Initiative

129. Dr. Mischa Hansel, Head of 'International Cybersecurity' Research Focus, Institute for Peace Research and Security Policy at the University of Hamburg (IFSH)

130. Niamh Healy, University College London

131. Duncan B. Hollis, Laura H. Carnell Professor of Law, Temple University Beasley School of Law

132. Prof. em. Wolfgang Kleinwächter, University of Aarhus

133. Andreas Kuehn, Senior Fellow, ORF America

134. Neal Kushwaha, CEO and Adviser on National Security, IMPENDO Inc

135. James A. Lewis, Senior Vice President and Director, Strategic Technology Program, Center for Strategic and International Studies

136. Paul Meyer, Senior Advisor, ICT4Peace

137. Katie Moussouris, Founder & CEO of Luta Security, NIST Information Security and Privacy Advisory Board Member

138. Kazuo Noguchi, Hitachi America

139. Elina Noor, Asia Society Policy Institute

140. Pavlina Pavlova, Independent Expert

141. Patryk Pawlak, Project Director, EU Cyber Diplomacy Initiative - EU Cyber Direct

142. Tawhidur Rahman,Chief Data Security Officer, Digital Security Agency-NCIRT, Bangladesh"

143. Mariana Salazar Albornoz, OAS InterAmerican Juridical Committee, Rapporteur on International Law applicable to cyberspace

144. Hina Sarfaraz, Chief Consultant, Third Eye Legal, Inc.

145. Michael Schmitt, Director, Tallinn Manual 3.0 on the International Law Applicable to Cyber Operations project

146. Ben Scott, Australian Academic in the field of Internet Security Engineering and 2020 Internet Society (ISOC) Mutually Agreed Norms on Routing Security (MANRS) Research Fellow

147. Rayna Stamboliyska, PhD, RS Strategy

148. Dr. Douglas Torres, University Professor, Independent Consultant

149. Tsvetelina van Benthem, Blavatnik School of Government, University of Oxford

150. Liis Vihul, CEO, Cyber Law International

151. Dr. Bruce W. Watson, Advisor on National Security, IMPENDO Inc., and Chair of AI Research, Stellenbosch University

152. Heidi Winter, Founder, Kids SecuriDay

This letter remains open for further signatories; all parties are invited to support these principles for multi-stakeholder engagement.