To all Permanent Representatives and
Permanent Observers
to the United Nations
New York

and

Distinguished Participants of the Open-ended
Working Group informal intersessional
consultative meeting

New York, 26.11.2019

Excellencies,
Distinguished Participants,

It is our honour to address you in our capacities as Chair of the Open-ended Working Group on developments in the field of information and telecommunications in the context of international security (OEWG) and Chair of the forthcoming OEWG informal intersessional consultative meeting.

As announced in the letter of the Chair of the OEWG of 1 November 2019, the OEWG informal intersessional consultative meeting will take place from 2 to 4 December 2019 in Conference Room 1 at the United Nations Headquarters in New York.

We warmly welcome all Participants including Member States to this important event. This is the first time in the history of UN ICT discussions in the context of international security that such an inclusive and global multi-stakeholder meeting is held to discuss cyber threats and challenges and how to address them.

Please find attached the current list of registered participants. For ease of reference, the final list of participants will be published on the website of the OEWG. We look forward to interactive discussions between Member States and the approximately 110 Organizations attending, and to benefiting from the public and private sector, civil society and academic expertise in the room.

Our vision for the consultative meeting is that it will be as inclusive as possible. Instead of panels, we encourage participants to engage in an open and interactive dialogue. As a short kickoff introduction, expert scene-setters will provide a brief overview of the issue from the floor at the start of each session after which the floor will be open to all Participants. Please see the attached draft agenda with the proposed scene-setters.

Participants are invited, should they wish, to provide a video introduction to their organization which will be uploaded to the meeting website. We therefore look forward to discussions in the room that are substantive and interactive, for which some possible framing questions could be considered (attached).
In addition, it is our pleasure to extend an invitation to all Permanent Representatives, Deputy Permanent Representatives, Heads of Delegation and Participants to the OEWG to a welcome reception on Monday, 2 December, from 6.15 to 8 pm at the Permanent Mission of Singapore. The invitation is attached.

For more information, please visit the consultative meeting’s website at https://www.oewg-intersessional.org.

Please accept, Excellencies, Distinguished Participants, the assurances of our highest consideration.

Jürg Lauber  
Ambassador  
Permanent Representative  
Chair of the Open-ended Working Group

David Koh  
Chief Executive  
Cyber Security Agency of Singapore  
Chair of the Open-ended Working Group informal intersessional consultative meeting

Encl.
List of registered participating organizations at the informal intersessional consultative meeting of the Open-ended Working Group on developments in the field of information and telecommunications in the context of international security

2 to 4 December 2019, Conference Room 1

1. Access Now
2. AfricaCERT
3. Amnesty International Kenya
4. Article 19
5. Asabe Shehu Ya’adua Foundation
6. Asia Blockchain Industry Institute
7. Asia Pacific Network Information Centre
8. Association for Progressive Communications (APC)
9. Australian Strategic Policy Institute, International Cyber Policy Centre
10. Azure Forum for Contemporary Security Strategy
11. Beijing Dentons Law Offices, LLP
12. Boston Consulting Group
13. BRAC University School of Law
14. Brazilian Center for International Relations (CEBRI)
15. CAPA 8 Foundation
16. Center for Technology and Society, Fundacao Getulio Vargas Law School
17. Center for Youth Development Services
18. Central European University
19. Centre for Humanitarian Dialogue
20. Centre for Information Technology Law Studies, University of Chile School of Law
21. Centre for Intellectual Property and Information Technology Law, Strathmore Law School
22. Centre for Internet and Global Politic, Cardiff University
23. Centre for Strategic and International Studies (CSIS) Indonesia
24. Centre of Excellence for National Security, Nanyang Technological University
25. Chatham House
26. China Academy of Information and Communications Technology
27. Citizen Lab
29. Commonwealth Centre for eGovernment
30. Commonwealth Telecommunications Organisation (CTO)
31. Consultancy Support Services (CS2) Limited
32. Cyber Policy Institute
33. Cyber Security Experts Association of Nigeria (CSEAN)
34. CyberGreen Institute
35. CyberPeace Institute
36. Cybersecurity Tech Accord
37. Derechos Digitales
38. DXC Technology Company
39. EastWest Institute
40. EU Cyber Direct
41. European Union Institute for Security Studies
42. Forum of Incident Response and Security Teams (FIRST)
43. Freedom House
44. Fujitsu Limited
45. Fundación Karisma
46. German Marshall Fund
47. Global Cyber Alliance
48. Global Forum on Cyber Expertise
49. Global Partners Digital
50. Hague Centre for Strategic Studies
51. HealthTech & Society
52. Hiperderecho
53. Hitachi America, Ltd.
54. Https Card - Internet Identity Card
55. Huawei Technologies USA
56. Human Rights Watch
57. ICT Association of Malawi
58. ICT4Peace Foundation
59. Igarape Institute
60. IGF Best Practices Forum on Cybersecurity
61. Innov'COM Sup'COM
62. Institute for Security and Safety
63. Institute of Computing Innovation, Zhejiang University
64. Institute of Strategic and International Studies Malaysia
65. International Cable Protection Committee
66. Internet Society Tanzania Chapter
67. IPANDETEC
68. JP Morgan Chase & Co.
69. Kenya ICT Action Network (KICTANet)
70. Knowledge House
71. Konrad Adenauer Foundation
72. Luftbrücke Irak
73. MAFINDO (Indonesian Anti-Hoax Society)
74. Media Foundation for West Africa
75. MediaNama
76. Microsoft Corporation
77. Mzumbe University
78. National Law University Delhi
79. NEC Corporation
80. Norwegian Institute of International Affairs
81. National Security Research Institute (NSR)
82. OISTE Foundation
83. Oxford Institute for Law, Ethics and Armed Conflict (ELAC)
84. Paradigm Initiative
85. Perry World House
86. R Street Institute
87. Red en Defensa de los Derechos Digitales (R3D)
88. Rapid7
89. Renaissance Foundation for Social Innovation
90. Research ICT Africa
91. Rwanda Internet Community and Technology Alliance
92. Samsung
93. Shanghai Institutes for International Studies
94. Soka Gakai International
95. Stimson Center
96. StrikeForce Technologies, Inc.
97. Tech & Law
98. Techloy
99. TEDIC
100. Telenor Group
101. Temple University School of Law
102. Trend Micro
103. Tuwindi
104. U.S. Chamber of Commerce
105. U.S. Council for International Business
106. Ubik Group
107. Universidad de Montevideo
108. Universidad Nacional Autónoma de México
109. University of Hong Kong
110. University of Waterloo
111. Women's International League for Peace and Freedom
112. World Economic Forum
113. World Wide Web Foundation
Open-ended Working Group on developments in the field of information and telecommunications in the context of international security

*informal intersessional consultative meeting – New York, 2-4 December 2019*

<table>
<thead>
<tr>
<th>UN Headquarters, Conference Room 1</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Monday, 2 December</strong></td>
</tr>
<tr>
<td><strong>10 AM – 1 PM</strong></td>
</tr>
<tr>
<td><em>Possible scene-setters:</em></td>
</tr>
<tr>
<td>Cyber threat landscape: Existing and emerging cyber threats: A view from Industry and Academia</td>
</tr>
<tr>
<td><em>Possible scene-setters:</em></td>
</tr>
<tr>
<td>Forum of Incident Response and Security Teams (FIRST)</td>
</tr>
<tr>
<td>Cyber Security Experts Association of Nigeria (CSEAN)</td>
</tr>
<tr>
<td><strong>3 PM – 6 PM</strong></td>
</tr>
<tr>
<td><em>Possible scene-setters:</em></td>
</tr>
<tr>
<td>Rules, laws and norms: Creating a cyber space based on rules, laws and norms: How can stakeholders support Governments</td>
</tr>
<tr>
<td><em>Possible scene-setters:</em></td>
</tr>
<tr>
<td>Temple University</td>
</tr>
<tr>
<td>Center for Technology and Society at Fundacao Getulio Vargas Law School in Rio de Janeiro</td>
</tr>
<tr>
<td>International Committee of the Red Cross (ICRC)</td>
</tr>
</tbody>
</table>
Multi-stakeholder meeting of the Open-ended Working Group
Guiding Questions

(A) Cyber threat landscape: Existing and emerging cyber threats: A view from Industry and Academia

- What are currently the most significant cyber threats, and how are these expected to change in the future?
- What are the main threats to critical infrastructure and critical information infrastructure?
- How does the malicious use of ICTs affect socio-economic development and, in particular, the digital economy?
- How do new technological developments, such as artificial intelligence and blockchain, alter the threats to the global ICT environment?

(B) Rules, laws and norms: Creating a cyber space based on rules, laws and norms: How can stakeholders support Governments

- How can stakeholders, such as industry, civil society and academia contribute to the implementation of the voluntary non-binding norms of responsible State behaviour contained in the report of the 2015 Group of Governmental Experts¹?
- How can all stakeholders including governments support each other in the responsible reporting of vulnerabilities and/or sharing of information on available remedies to protect ICT-dependent infrastructure²?
- As both multi-stakeholder initiatives and intergovernmental norms emphasize the need to ensure the integrity of the supply chain of ICT products, how can multi-stakeholder cooperation on the operationalization of these norms be enhanced?
- States have agreed that international law, and the UN Charter in particular, applies to the use of ICTs. Building on these recommendations, what additional perspectives can other stakeholders offer to the OEWG?

(C) Rules, laws and norms: Stakeholders’ commitments to rules, norms and principles: Tech Accord, Charter of Trust, Global Transparency Initiative, Paris Call and beyond

- What are the commonalities between the different multi-stakeholder initiatives on cybersecurity, such as the Tech Accord, the Charter of Trust, the Global Transparency Initiative, the Paris Call and other initiatives, and the norms developed at the intergovernmental level?
- What synergies should be encouraged between intergovernmental and multi-stakeholder initiatives to prevent us going on separate paths?

¹ The 2015 GGE report is available through https://undocs.org/A/70/174
² Norm (j), contained in paragraph 13 of the 2015 GGE report states that “States should encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies to such vulnerabilities to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure”
(D) Confidence-building measures and capacity-building: Confidence-building between States and between States and the Private Sector

- How can all stakeholders contribute to the implementation of confidence-building measures?
- How can confidence-building measures be further developed at a technical level through cooperation?
- What confidence-building measures should be co-developed between the Public and Private Sector?

(E) Confidence-building measures and capacity-building. Engaging all stakeholders to enhance capacity-building efforts

- How can all stakeholders including States cooperate to promote capacity-building including awareness and education?
- How can the needs and resources for capacity-building be best aligned, with a view to promoting complementarities and avoiding duplication?
- What roles can the different stakeholders including States play in the development of national ICT-security strategies?

(F) Conclusion: Ways forward on a multi-stakeholder approach

- What are the main benefits of regular multi-stakeholder dialogue on international ICT-security?
- What modalities for continued multi-stakeholder dialogue are most useful to the different stakeholders?
- What can be done do to ensure the views of relevant stakeholders from all regions are represented in future multi-stakeholder dialogue?
INVITATION

TO A

WELCOME RECEPTION

For Delegates to the Open-ended Working Group on developments in the field of information and communications technology in the context of international security (OEWG) informal intersessional consultative meeting

Co-hosted by

H.E. Mr. Burhan Gafoor
Permanent Representative of Singapore

&

H.E. Mr. Jürg Lauber
Chair of the OEWG and
Permanent Representative of Switzerland

For Permanent Representatives, Deputy Permanent Representatives, and Heads of Delegation and participants at the OEWG

Date: Monday, 2 December 2019
Time: 6.15 pm to 8.00 pm
Venue: Permanent Mission of Singapore to the United Nations, 318 E 48th Street (Between 1st and 2nd Avenues)

To confirm your participation, please RSVP at http://bit.ly/recep2dec