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

Honorable Chair,

We, the undersigned organizations, are writing to express deep regret with the recent decision of a few member states to exclude over 30 members of industry and civil society from the workings of the United Nations Open-Ended Working Group (UN OEWG) on cybersecurity. This exclusion applies to many in the technology industry, including the 150 technology companies represented by the Cybersecurity Tech Accord, the incident responders and security professionals represented by the Forum of Incident Response and Security Teams (FIRST), as well as many more relevant organizations in civil society and academia.

Unfortunately, the decision to exclude these key communities seemingly reflects political considerations that undermine the potential of the OEWG at a time when its mission is more important than ever. We believe that the use of the veto in this instance was not "judicious", as outlined in the agreed modalities which encourage member states to utilize the non-objection mechanism carefully, bearing in mind the spirit of inclusivity.

There is broad agreement among the UN member states that to address matters of peace and security in cyberspace, to implement international expectations, will require increased cooperation and collaboration of a diverse range of stakeholders at the UN. As stated in the Final Substantive Report of the previous OEWG on this topic in 2021,

> *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. The OEWG discussions were an affirmation of the importance of recurrent and structured discussions under UN auspices on the use of ICTs. (Paragraph 69)*

This is especially true for organizations with unique insights and/or expertise related to cyberspace, a synthetic and new domain of human activity. It is hard to imagine, for example, that future OEWG deliberations on safeguarding CERT/CSIRT teams from targeting or on securing critical infrastructure would not benefit greatly from the meaningful inclusion of the technology industry and incident response communities.

More must be done to build the systems, structures and trust necessary to cooperate across stakeholder groups. We recognize the ongoing geopolitical challenges and that have and will continue to create obstacles for international cooperation on cybersecurity, and applaud the efforts of the OEWG and its Chair thus far to facilitate an inclusive dialogue despite these challenges. However, as conflict and instability online continues to escalate, continued leadership and courage from the OEWG will be essential if it is to fulfil its mandate and live up to member state expectations.

We, the undersigned, represent organizations with varied and diverse perspectives, some of which will not align. But we all believe in the importance of diplomacy in this space, and in ensuring that member states benefit from relevant perspectives in their deliberations. We urge the Chair to seek conversation with relevant parties in the OEWG to reverse the recent decision that prevents the contribution of many members of the multistakeholder community to the OEWG process.

Access Partnership
Anglo American
Association for Progressive Communications (APC)
Australian Strategic Policy Institute
The Azure Forum for Contemporary Security Strategy
Chatham House
CyberPeace Institute
Cyber Policy Institute
Cyberspace Cooperation Initiative at ORF America
Cybersecurity Tech Accord
DXC Technology
Géopolitique de la datasphere
GFCE Foundation
Global Partners Digital
Fair Tech Institute
Forum of Incident Response and Security Teams
Hitachi
ICT4Peace Foundation
Igarape Institute
Independent Diplomat
ICC United Kingdom
Jokkolabs Banjul
Jonction
Kaspersky
Kenya ICT Network
KnowBe4
Media Rights Agenda
Microsoft
Oxford Institute for Ethics, Law and Armed Conflict
Research ICT Africa
Safe PC Solutions/Safe PC Cloud
Temple University
United States Council for International Business