Establishing a UN Programme of Action on Cybersecurity – Aotearoa New Zealand submission

1. Cybersecurity has been a topic of discussion among states, under the auspices of the United Nations, for more than 20 years. Successive working groups – groups of governmental experts and open-ended working groups - has allowed for regular exchanges on issues relating to cybersecurity in the context of international security.

2. These working groups have delivered important foundational outcomes that collectively contribute to international security and stability, through establishment of a framework for responsible State behaviour in cyberspace - endorsed by the UN General Assembly, and based on four pillars:

- International law – all UN Member States agree that international law applies to states' conduct in cyberspace
- Norms of responsible state behaviour online in peacetime
- Confidence-building measures to support transparency, predictability and stability
- Capacity-building measures aimed at ensuring all States can lower the risks of increased connectivity, while still benefiting from it.

3. Aotearoa New Zealand believes that it is now time to build on this foundation and establish a permanent, regular, institutional cybersecurity dialogue at the UN. As co-sponsor of UNGA Resolution 77/37 (2022), we support ongoing discussions on the establishment of a UN Programme of Action on cybersecurity (PoA) and further elaboration of its scope, structure, content, preparatory work and modalities, including during the Regular Institutional Dialogue agenda item at the UN *Open-ended Working Group on security of and in the use of information and communications technologies 2021-2025* ("OEWG").

4. We envisage a POA being the 'permanent home' of cybersecurity discussions at the UN at the conclusion of the current 2021-2025 OEWG, building on the proposal adopted in UN Resolution 77/37. In line with that proposal, we support establishment of a POA that is:

    4.1. **The permanent mechanism for UN cybersecurity discussions after 2025**, ensuring predictability and institutional stability. Negotiating agreed modalities for a permanent mechanism would also deliver long-term efficiencies. Revisiting and agreeing modalities for successive working groups has required lengthy, recurring negotiations, taking time away from important substantive discussions.

    4.2. **Anchored in the agreed framework for responsible State behaviour in cyberspace, including international law,** ensuring the PoA builds on, and enhances, the foundational work of successive Group of Government Expert groups and OEWGs to advance responsible state behaviour online.

4.3. **Inclusive** – multi-stakeholder participation involving governments (who bear responsibility for international peace and security in cyberspace), companies, civil society, technical experts, academics and other organisations who contribute to a free, open, secure and interoperable internet. Aoteraoa New Zealand supports modalities that include participation (including statements and submission of written reports) by non-government stakeholders in discussions, including any formal and informal meetings and review conferences.

4.4. **Action-oriented**, including a focus on implementation of the framework for responsible State behaviour and promoting capacity-building measures that support states to implement the framework, and mechanisms for accountability and monitoring.

4.5. **Flexible and adaptable**, to respond to emerging technologies and threats.

12 April 2023