Our submission to Open-Ended Working Group on ICTs
First substantive session (13-17 December 2021)

About Global Partners Digital
The advent of the internet – and the wider digital environment – has enabled new forms of free expression, organisation and association, provided unprecedented access to information and ideas, and catalysed rapid economic and social development. It has also facilitated new forms of repression and violation of human rights, and intensified existing inequalities. Global Partners Digital (GPD) is a social purpose company dedicated to fostering a digital environment underpinned by human rights and democratic values. We do this by making policy spaces and processes more open, inclusive and transparent, and by facilitating strategic, informed and coordinated engagement in these processes by public interest actors.

Input on priorities for the second OEWG on ICTs

It is important for the Open-Ended Working Group on ICTs to build on the existing achievements of the OEWG and Group of Government Experts (GGE). In this way it must do the following:

1) **Continue to provide greater clarity** on how threats are perceived and their differential impact (as recognised in previous OEWG and GGE reports)

2) **Support states to implement** the existing framework in a human-centric and inclusive manner. For example by:
   - Sharing information on the status of norms implementation both in substantive sessions and through the provision of inputs to the UNODA webpage which provide an overview of norm implementation, as some countries have already done (e.g. the United Kingdom and Australia). The OEWG should also encourage both state and non-state actors to share information on the implementation of norms, including by using the survey template developed under the previous OEWG. Similar efforts could be conducted on the status and means of CBM implementation.
   - Deepening understanding of how international law applies in cyberspace, by reaffirming all bodies of international law apply but also to deep understanding in key areas such as on the application of the principle of due diligence
   - Ensure complementarity between discussions at the OEWG and other relevant processes, including for example by taking into account the OHCHR’s report on cyber mercenaries and the UN Third Committee Ad Hoc Committee on Cybercrime.

3) **Provide greater accountability**: Human rights are directly impacted by state behaviour in cyberspace. For example, from attacks on critical infrastructure including through the use of ransomware, the use of spyware, shutdowns and the implementation of regulatory frameworks such as cybersecurity and cybercrime legislation which criminalise speech or expand surveillance powers, and introduce security vulnerabilities. Therefore the OEWG should:
• Encourage states and other actors to refer to norms and international law when they undermine, violate agreed norms or international law
• Share information on efforts, measures and frameworks to address these violations
• Encourage the discussion of the criteria used/required for independent and impartial attribution of cyber incidents to foster better and common understanding.

All of the above should be done in a way that is inclusive of stakeholders, including civil society and explore virtual/hybrid formats (see the joint letter to the Chair sent by a range of stakeholders on 07 December 2021). States should engage stakeholders in evaluating and implementing norms (see text box below), identifying capacity building needs and implementing capacity building efforts, and in supporting the development of their views on how international law applies in cyberspace. Therefore, states should conduct national consultations and utilise existing relevant forums nationally, regionally and globally to gather input on these areas of the OEWG’s mandate.

**Examples of existing efforts from the multistakeholder community relevant to norm implementation**
- GPD series on the implementation of the responsible state behaviour framework
- GFCE paper on norm implementation in practice
- Best Practice Forum on Cybersecurity of the IGF: research on norms