ROYAL NORWEGIAN
MINISTRY OF FOREIGN AFFAIRS

Norway's views pursuant to General Assembly resolution 77/37 Programme of action to advance

responsible state behaviour in the use of information and communications technologies in the context of international security

Norway supports the establishment of a Programme of action to advance responsible state behaviour in the use of information and communications technologies in the context of international security (PoA). The proposal of the establishment was welcomed by the General Assembly in its resolution 77/37, which Norway co-sponsored.

Norway considers that establishing a PoA is the best way to move forward in the UN discussions and efforts on cybersecurity and responsible state behaviour in cyberspace. We believe the PoA should be a permanent structure for dealing with cyber security issues in the UN. This will allow for a stable structure where we can focus on action-oriented activities and concrete progress, as well as continue the normative discussion. The PoA should reaffirm and build on the UN consensus-based framework of responsible state behaviour achieved through years of discussions in the 2010, 2013, 2015, and 2021 Groups of Governmental Experts (GGEs), as well as the 2021 Open-ended Working Group (OEWG). The PoA should be inclusive, transparent, consensus based, action oriented, and results based.

We should have one structure in the UN for both regular dialogue and implementation of the normative framework for responsible behaviour in the use of information and communications technologies. The PoA should be established by the time the OEWG concludes its mandate in 2025.

The achieved consensus on the normative framework should now be accompanied by action-oriented implementation and capacity building. The PoA can promote capacity building activities to support states in implementing the normative framework. In the PoA UN members and relevant stakeholders can have focused discussions, round tables, briefings, voluntary reporting by states on implementation efforts, mapping of needs, exchange of knowledge, best practices, and expertise. The PoA can provide a better opportunity for tailored assistance to states in their efforts to maintain a free, open, and secure cyberspace. The PoA should consider existing initiatives and cooperation on cybersecurity within relevant organisations like the OSCE and other regional organisations.

The PoA should be organised in a way that allows for flexibility in terms of focus areas and practical efforts. This can allow states to address new threats and emerging technologies. The PoA should focus both on the implementation of norms and continue the discussion on the further development of the normative framework. The framework of the PoA's structure should regularly be subject to review as necessary and appropriate, through the regular meetings or review conferences.

The PoA must be inclusive. All member states must be able to participate. In addition, we need a broad participation of non-governmental actors and other stakeholders, as they have important roles in maintaining a free, open, and secure cyberspace. Regular consultations with private sector, academia and NGOs will secure necessary expertise and resources to both discussions and practical efforts. Including stakeholders does not challenge the role of states in international security.

Norway believes there should be allocated enough time within the OEWG format for detailed discussions on the mandate, modalities, and realisation of a future PoA. The OEWG should have a dedicated session to discuss the PoA.