United Kingdom Submission to the UN Secretary-General on a Programme of Action (PoA) to advance responsible State behaviour in the use of ICTs in the context of international security.

Pursuant to UNGA Resolution A/RES/77/37

INTRODUCTION

1. Over the past 30 years, UN Member States have developed a *Framework of responsible state behaviour in information and communications technologies in the context of international security* ("the Framework"), endorsed by the UN General Assembly in successive resolutions (70/237; 76/19 and others).

2. The 2019-2021 *Open-Ended Working Group (OEWG) on security of and in the use of information and communications technologies* (ICTs) concluded that future Regular Institutional Dialogue should take place through an 'action-oriented process with specific objectives, building on previous outcomes…[which is] inclusive, transparent, consensus-driven and results-based"[1].

3. In 2022, the General Assembly voted to welcome proposals for a Programme of Action (PoA) 'to advance responsible State behaviour in the use of information and communications technologies in the context of international security'[2]. The United Kingdom strongly supports the creation of the PoA as a permanent, inclusive, action-oriented mechanism for discussions on international peace and security in cyberspace.

4. This Programme of Action should also be developed with a particular focus on:

   I) **Inclusivity.** The PoA should be shaped by, and open to participation from, all UN Member States. Modalities should allow for meaningful participation by non-government stakeholders. Establishing the PoA as the single successor mechanism to the current OEWG will help States to efficiently allocate the resources to participate.

   II) **Legitimacy.** Member States have agreed a Framework of responsible state behaviour in ICTs in the context of international security. This should be our starting point. There is a clear role for the PoA in supporting states to implement this consensus Framework, and in further clarifying how existing international law applies to cyberspace.

   III) **Flexibility:** This focus on implementation of the agreed Framework would identify gaps for further elaboration. The structure of the PoA should therefore be flexible enough to allow it to respond to such gaps as they are

[1] 2019-2021 OEWG Final Report, Para 74

[2] UNGA Resolution A/RES/77/37

identified over time and to further develop the evolving Framework, including in response to emerging threats.

SCOPE AND OBJECTIVES

5. The overall purpose of the PoA should be to contribute to international peace and security through the preservation of a free, open, peaceful and secure cyberspace. It should do so by facilitating dialogue and cooperation between Member States on security of and in the use of information and communications technologies; and supporting the implementation and evolution of the Framework.

6. The PoA should be the single successor mechanism to the current Open-Ended Working Group, in its discussion of security of and in the use of information and communications technologies. In doing so, it would provide:

   - An opportunity for discussion of, and information-sharing on, cyber threats. (*E.g. through discussion at annual meetings and in focused workstreams; and consideration of new mechanisms on threats, such as the portal proposed by India.)*

   - A means of supporting States to identify the areas of capacity needed to improve their performance in the implementation of the Framework *(E.g. through voluntary reporting; stock-takes of existing capacity-building activities carried out by UN bodies; active participation of non-government stakeholders including regional organisations, civil society and the private sector; engagement with the World Bank Cybersecurity Trust Fund and others.)*

   - An inclusive process through which to elaborate the Framework. *(E.g. through a workstream to consider how international law applies to cyberspace.)*

   - A basis for the development of further Confidence Building Measures. (*E.g. by building on the Points of Contact directory, a permanent mechanism already under development in the current OEWG; discussion of further measures that would benefit from links to a permanent UN forum on international peace and security in cyberspace.)*

STRUCTURE AND CONTENT

Political Declaration

7. The PoA should be initiated through a Political Declaration agreed at the political level, through a High-Level Meeting or international conference. The Framework should form the basis of this Declaration, which should include: agreement on actions to advance the implementation of commitments to responsible state behaviour in cyberspace; clarification of the application of International Law in cyberspace; and the agreed scope and modalities for the PoA.

8. Political-level agreement would provide an opportunity for States to publicly and visibly reaffirm their commitments at this stage in the evolution of the Framework and could help States to secure political buy-in within their own systems.

9. Capacity-building is an important part of the Framework and its value should be highlighted through the Political Declaration. The Declaration should take account of the OEWG's principles on capacity building and also the work of other UN and non-UN bodies, including the capacity building principles set out in the GFCE's Delhi Communique.

Annual Meeting

10. The PoA should hold an annual, formal meeting, which would provide an opportunity to:
    - discuss and share information on new and emerging threats;
    - review the implementation of the Framework, including on the basis of voluntary reporting;
    - share capacity-building opportunities and ensure briefings by relevant stakeholders;
    - elaborate understandings of the Framework, including on the application of international law;
    - consider the recommendations of specific workstreams (which could be established through the annual meeting).

Review Conferences

11. The PoA should hold a review conference every four years. These conferences would allow the PoA to take stock and to adapt, given the dynamic and evolving nature of threats to international peace and security in cyberspace.

Voluntary Reporting

12. Implementation of the Framework and support to capacity-building have been identified as important priorities for the Programme of Action. Voluntary reporting would support this effort. Existing surveys (such as the UNIDIR National Survey of Implementation) and evolving mechanisms (such as Singapore's proposed norms checklist) provide possible bases for a consistent approach through the PoA.

Multistakeholder Participation

13. Member States should have the exclusive right to negotiate outcomes and make decisions within the PoA. However, non-government stakeholders provide valuable perspectives. They are often the first to be affected by cyber incidents and are essential to the response. They can also play an increased role in delivering capacity-building. Non-government stakeholders should therefore be able to participate meaningfully in all PoA meetings, including through written and oral contributions. Stakeholder participation should be inclusive and diverse, regional participation

should be encouraged. Stakeholder accreditation should be informed by transparency, with final decisions on accreditation being taken by all states, including through voting if consensus cannot be reached.

PREPARATORY WORK AND MODALITIES

14. The OEWG should play an important role in the further elaboration of the PoA. Mindful of the resource constraints experienced by delegations, dedicated time to discuss and further elaborate the POA should be given within the formal and informal meetings of the current OEWG. Given the significance of the task, dedicated intersessional meetings are likely to be needed.

15. Member States should also not be precluded from developing proposals in additional conferences and bringing them to the OEWG and the General Assembly for consideration.