Italian contribution to the UNSG for a report mandated by UNGA Resolution 77/37 on a Programme of Action (PoA) to advance responsible State behaviour in the use of ICTs in the context of international security

A) Introduction, Motivations, Scope and Objectives

Italy is a staunch supporter of **multilateralism** and a strong advocate of UN processes and of regular institutional dialogue on security of and in the use of information and communications technologies within the UNGA's First Committee.

The work of the 2010, 2013, 2015, and 2021 Groups of Governmental Experts (GGEs), as well as that of the 2021 Open-ended Working Group (OEWG) on Developments in the Field of Information and Telecommunications in the Context of International Security have **established the international framework** that Italy has pledged to respect when adopting its posture in cyberspace. It has contributed to shaping Italy's national cyber architecture too. Italy is committed to continue promoting it both at national and international level.

As part of this vision, Italy actively participates in the current OEWG, due to conclude its work in 2025, and supports the establishment of **a Program of Action**, as the best means to ensure effective Regular Institutional Dialogue (RID), thus **contributing to implement both the framework further, and the results of the current OEWG**.

The PoA should be a **single permanent structure / platform / mechanism / forum** for tackling cybersecurity issues at the global level, notably in the UN context. Lack of capacities at national, regional and global level is a challenge and the PoA should support national efforts to implement the normative framework and provide **capacity building** to help bridge the digital divide.

As digitalisation increases so does the potential for instability in cyberspace. Looking towards the end of the mandate of the OEWG, it is high time to start discussions on the establishment of the PoA, to ensure that discussions continue beyond 2025 in a more **structured and predictable** manner.

B) Process

Duplication of efforts should be avoided, therefore discussions on goals, objectives, principles, structure, tasks, modalities and content of the PoA should take place in the context of Regular Institutional Dialogue within the current OEWG. References to the PoA should be inserted it in the upcoming Annual Progress Report and discussions on a 2024 and 2025 Programme of Work should begin at the earliest.

The UNSG Report will be crucial for this process and – if needed – more time should be allowed for States to contribute, should the need arise. One could also consider the possibility of yearly technical Resolutions to mark annual progress, until 2025, when a political declaration to be agreed by the UN General Assembly should also be passed. A specific conference could be convened in 2025, after the conclusion of the current OEWG, to advance the set-up of the PoA and prepare the grounds for the political declaration.

C) Principles, Structure and Content

For such an endeavour to succeed and taking into account the speed at which ICTs are evolving, the PoA needs to be have sufficient **flexibility** in order to make it future-proof. Such characteristic should be reflected in the frequency at which its mechanisms are reviewed, as well as in the number of intersessional technical workstreams that could be established and/or terminated.

The OEWG has successfully brought the use of ICTs to the attention of the whole UN membership. **Inclusivity** should therefore be the cornerstone of the PoA's activities, both in terms of taking into account the capacities of all States, as well as in terms of participation of non-governmental entities to the debate. On the first aspect, **cross-regional pairings, groupings and participation** to the various workstreams should be encouraged and become one of the defining features of the PoA. While the intergovernmental nature of the decision making-process of the PoA is not questionable, civil society and the private sector are essential players in cyberspace and a key ingredient of any successful RDI. Current OEWG arrangements are sub-optimal, ways to improve the depth and frequency of **multi-stakeholder consultations** should be thoroughly explored, also by taking into account lessons learned from other processes.

Building upon the successes of past and present mechanisms and processes will be key to make the PoA fit for purpose. The excellent work of **UNODA** should continue as the Secretariat of the PoA. Similar words of appreciation are applicable to **UNIDIR,** which should continue providing input in the context of the PoA not only in its capacity as a Research Institute but also when applying its methodologies for analytical, monitoring and review capacities.

The work in the field of cybersecurity carried out by **regional organisations** is fundamental. This is becoming increasingly apparent in current efforts to establish a global Points of Contact directory, as a first enabling step to increase cooperation among States. Collaboration between the PoA and regional and sub-regional organisations should be carefully considered to accelerate discussions on some topics thus allowing for more time to dive deeper on other pressing issues. Mechanisms to avoid repeating discussions and decisions which have already been taken at regional level, should be thoroughly explored in order to make the PoA as action-oriented as possible.

Regularity and predictability of consultations amongst States and stakeholders are also key elements of a successful PoA. One way of ensuring it could be to hold: (i) Annual conferences in New York to discuss the implementation and possible evolution of the framework, as wells the work of technical workstreams; (ii) Review Conference focused on the assessment of the performance of the PoA and its possible review every 4 yrs (Geneva could be a possible location); (iii) set-up of technical / topic-specific workstreams, which meet on a more regular/frequent manner, to be decided by consensus. In such formats discussions could also take place in different geographical locations and/or in hybrid format as long as recommendations stemming from such activities are validated at least on a yearly basis during plenary meetings. Technical workstreams should primarily focus on the implementation of the acquis.

A Biennial **Programme of Work** should provide visibility on activities and topics to be tackled. This should be presented and approved at Annual conferences, together with a Chair's Report of activities carried out the previous year. The **Chair of the PoA** should be appointed for a triennial term of office with the possibility for a one-year extension. A six-month overlap in office with the incoming Chair would be advisable to ensure continuity of work and smooth transition arrangements.

The current **lines of activity** identified in the OEWG (Existing and Potential Threats; International Law; Rules, Norms and Principles of Responsible State Behaviour; Confidence-Building Measures; Capacity Building) should be continued within the PoA which should initially focus on implementing what has been consensually agreed in the past. Given the pace of tech developments and their implications, particular focus is needed on threats. An additional workstream dedicated to a voluntary, Peer Review mechanism on the National Implementation of the framework could be envisaged. Current reporting mechanisms/obligations could also be maintained, with a view to developing more efficient and less time-consuming systems in the medium/long-term. Finally, discussions on how international law applies in cyberspace are of crucial importance to further the understanding of States, influence their behaviour in cyberspace and increase the possibilities of mutual cooperation.

Regarding **Cyber Capacity Building** (CCB) support, which should constitute one of the most prominent features of the PoA, this should be provided upon request and on the basis of the principles outlined in Document A/76/135. The PoA could absorb any initiative currently being developed provided it helps to facilitate the analysis of CCB offers, does not duplicate existing efforts and contributes to de-confliction and prevents "forum-shopping". A dedicated funding mechanism should be explored, looking at existing instruments provided by regional organisations such as the EU and/or specialised bodies such as the World Bank Cybersecurity Multi-Donor Trust Fund or the Global Forum on Cyber Expertise (GFCE).

Regarding participation to different workstreams and activities, mechanisms to ensure **geographical balance and cross-regional collaboration** should be promoted. One such mechanism could be the pre-condition to join any workstream "in tandem" ie. provided that the request to participate from a member State is submitted jointly with another member State from a different geographical area. In addition and conversely, a mediation support mechanism to assist member States on diametrically opposed positions should be explored – this could be provided by the UN or by constituting a pool/roster of willing and able member States. The initiative could constitute a spin-off of the CBM workstream.