Germany's submission
to UNSG report mandated by UNGA Resolution 77/37

A) Underlying Principles of the Programme of Action

Germany supports the establishment of a Programme of Action (PoA) as an **action-oriented, permanent and inclusive forum** for regular institutional dialogue on **security of and in the use of information and communications technologies** within the UNGA's First Committee. The PoA shall be the **single follow-up mechanism of the current Open-Ended Working Group** (OEWG 2021-2025) and become **operational** to implement the results of the OEWG after completion of the latter's mandate.

Parallel processes or double structures need **to be avoided** as this would exceed the capacity of many States to participate meaningfully. To prepare for a **smooth transition**, discussions among States about the scope, structure and content of the PoA need to be continued inside the OEWG with the ambition of finding consensus on the PoA's substance and modalities, which should be endorsed by all UN member states at a dedicated conference to be held back to back with the last sesssion of the OEWG in 2025.

The overall purpose of the PoA is to contribute to **international peace and security** in cyberspace, by **facilitating dialogue and cooperation** among States to **implement the existing international framework** for responsible State behaviour in the use of ICTs. This requires:

- **Cyber capacity building,** according to the guidelines agreed in the OEWG 2021 final report and leveraging synergies with mechanisms in other fora
- **Confidence-building measures** (CBMs), including making effective use of the future global **Points-of-Contact (PoC) directory**
- **Exchange of best practices** at the international, inter-regional, regional levels
- Meaningful **participation of relevant stakeholders**

Moreover, the PoA shall constitute the permanent platform for **advancing recurring items,** by facilitating discussions on **existing and emerging threats,** as well as on **how international law**, including international humanitarian law and human rights, applies to the use of ICTs by states. **Further potential development** of the international framework of responsible state behaviour in cyberspace shall be possible within the PoA in order to adapt and respond to new threats as they evolve over time.

The PoA should provide the overarching institutional framework for other cybersecurity mechanisms currently under preparation in the OEWG such as a Cyber Portal as suggested by India and a Cyber Repository as suggested by Kenya.

The overarching **goal**, specific **objectives** and **underlying principles of the PoA** should be anchored in the form of a **political declaration** to be agreed by the UN General Assembly. The declaration should be complemented by a **First Committee resolution** describing the **tasks, structure and modalities** of the PoA. Both the political declaration and the First Committee

resolution should be based on the outcome of the dedicated conference to be held in 2025 as mentioned above.

B) Tasks, Structure and Modalities of the Programme of Action

Building on the lessons learned from previous and existing instruments, the **Cyber PoA's Tasks** should be designed in a way that ensures the **effective, inclusive and transparent participation of States** and allows for **measuring progress of the implementation** of the framework of responsible State behaviour, including through a **voluntary reporting mechanism such as the UNIDIR National Survey of Implementation**. **Capacity building** and **cooperation**, **among States** as well as with **regional organizations** and **non-state actors**, are key in order to address those areas where national implementation is lagging behind.

The **Structure and Modalities** of the PoA should include:

- **Annual conferences** to be held at **UN Headquarters in New York**
    1) To review and measure progress of the implementation of the framework and the defined tasks.
    2) To discuss the potential evolution of the framework including by further advancing the joint understanding of the application of international law in cyberspace.
    3) To adopt decisions on specific topics.
    4) To exchange information on current and emerging threats to international peace and security resulting from the use of ICTs,
    5) To further elaborate cyber capacity building measures,
    6) To consider the possible further evolution of the PoA in an incremental way, based on member states needs, taking into account changes in the threat landscape and following the understanding, that the PoA is a flexible instrument.

- **The implementation and further elaboration of CBMs based on the global PoC directory** to be established by the current OEWG 2021-25. Beyond being a **confidence-building measure in itself**, the PoC directory shall provide the basis for the **implementation of other CBMs** with the overall objective of reducing the risk of misunderstanding and conflict in cyberspace. By **facilitating the implementation of dedicated CBMs focusing inter alia on communication**, particularly in times of crises, **peer-to-peer exchange, sharing of best practices, transparency measures, cooperation with the private sector or joint table top exercises**, the **PoC directory** would constitute a **central pillar of the PoA** focussing on the implementation of the existing framework.

- **UNODA** acting as the PoA's Secretariat. In addition to **preparing the annual meetings and review conferences**, UNODA will also be in charge of administering the global **PoC directory and other CBMs**.

- **UNIDIR** providing States with relevant monitoring & review instruments (e.g. norms implementation checklists) and conduct **research activities** related to the implementation of the framework.
- The possibility of additional meetings of **technical workstreams** in the intersessional period. Dedicated technical workstreams could focus inter alia on advancing cyber capacity building, CBMs, the application of international law and current and evolving threats. Participation in the workstreams should be **voluntary, open to all States** and **regionally balanced**. The number and set-up of workstreams, including the participation of stakeholders, and the frequency of meetings should take into account the capacities of States to participate meaningfully and be **decided by consensus** at the annual meetings.

- **Review conferences** every four years to allow for potential adaptation of the PoA to the dynamic evolution of cyberspace and the associated risks for international peace and security**.**

- While States will retain the exclusive right to negotiate outcomes and make decisions within the PoA, exchange with **non-governmental stakeholders** (multilateral and regional organizations, civil society, private sector and academia) should be **enhanced**, by providing **inclusive and meaningful participation** similar to the modalities of the Ad Hoc Committee on Cybercrime (any veto of a member state against the participation of stakeholders should be justified publicly; exclusion of stakeholders would be decided by a vote). This includes the right to speak and submit written inputs at annual meetings, review conferences as well as at additional meetings of technical workstreams during the intersessional period. Furthermore, hybrid options of participation would increase inclusiveness of the deliberations.

- Particularly in the area of confidence-building measures and capacity-building, **existing initiatives and structures** at the (sub)-regional level or in other fora should be **leveraged** and synergies be built (i.a. regional organizations, World Bank Cybersecurity Trust Fund, Global Forum on Cyber Expertise).

- **Existing funding facilities** in other UN fora, such as **SALIENT or UNSCAR** in the area of arms control, could provide useful guidelines for establishing a mechanism to support cyber capacity-building efforts in the form of **training and sharing of best practices**. Furthermore a fellowship programme to facilitate broad capital representation from delegations of developing countries could be envisaged.

- A **voluntary, cross-regional "partnering system"** could be established, in which a State that has high capacities in implementation of the framework is paired with one or more States with lower capacities. Such a mechanism would **enhance cooperation** among States, facilitate dialogue and exchange of best practices, and **increase capacities** of States for norm implementation overall. The "Adopt a CBM" approach of the OSCE could be used as a reference model in that regard.