Federal Foreign Office

Statements delivered by Germany during the inter-sessional meeting of the OEWG, held in New York from 05 to 09 December 2022

05 December:

Introductory Statement on the PoC presentation by the Confidence Builders Group

- In the name of the open cross-regional group to advance CBMs in the OEWG, Germany wishes to thank the chair for calling this inter-sessional meeting and for allocating dedicated space to the topic of CBMs and very specifically also the establishment of PoC directory at UN level, as agreed in the Annual Progress Report of this Group.

- Thank you, Mr. Chair, for your openness in encouraging UN member states to present their concepts and plans for the future work. Particular thanks go to UNODA and UNIDIR for their excellent presentations this morning.

- The results of these surveys have highlighted many of the practical questions that need to be solved before we can establish a PoC directory. In that way survey results present us with a very valuable roadmap for our work on this topic.

- The responses to both surveys have also highlighted the high level of support for this undertaking with many states making succinct recommendations on how the PoC directory can contribute to security and stability in cyberspace.

- Our informal group has circulated two joint working papers addressing the establishment of a PoC network.

- Members of our group are going to present a summary of the most important points here today, focusing on the interplay with already existing regional PoCs, possible uses of such a PoC directory, administrative issues and the way forward towards the establishment of such a first, universal network.

- **Why are we placing this focus on the PoC directory? Because we see the PoC directory as the essential starting point for anchoring a whole set of confidence building cyber measures at the UN level.**

- **This is the basis for exploring CBMs, that make a direct contribution to security and stability in cyberspace by offering a platform for communication, transparency measures or sharing of best-practices.**

- The following presentation is made on behalf of all the members of this group, namely **Australia, Brazil, Canada, Chile, Fiji, Germany, Israel, the Republic of Korea, Mexico, the Netherlands, Singapore and Uruguay**.

- Let me add, that **we regard this as an open group and we are happy to take on board any new members interested in taking CBMs further**. If you allow I would now pass the floor to Canada, to start off our presentation with some thoughts on the interplay with regional PoCs.

- Canada is particularly well placed to take us through this topic as Canada is member of two regional organisations with experience in implementing confidence building cyber measures, namely the OAS and the OSCE.

- Canada will then give the floor to Singapore, to be followed by Israel and the Netherlands to conclude our joint presentation in the name of our group.

06 December

Statement on CBMs and Capacity Building as part of the sequenced intervention of the Confidence Builders Group

1) Israel – Introduction
2) Chile on Regional Experiences

3) Singapore on Regional Experiences
4) Canada on Stakeholder Involvement
5) Germany on CBMs and capacity building
6) Australia on Transparency Measures
7) Mexico on Joint Exercises and Training
8) Netherlands – general points and closing

- Would like to focus on: how CBMs can contribute to capacity building. Would like to highlight three avenues.

- 1. **Establishment of PoCs can be of capacity building nature**
  - for UN member states that so far don't have PoCs
  - Even if only limited capacity is required, establishing a PoC for the first time is an **act of institutional capacity building**.

- 2. The PoC directory **will open channels for communication between PoCs**. This can also be used to **communicate information, that contributes to capacity building**:
  - **Sharing of best – practices to incident response**
  - **Sharing of national strategies via a CBM on transparency**
  - **Sharing of information on effective national legislation**
  - **This illustrates: being part of the PoC-Directory gives access to a community of learning. This is capacity building**

- 3. **OEWG could agree on a CBM dedicated to CCB**. This CBM could have the explicit purpose to build cyber capacity
  - By serving as a **platform to hold trainings**
  - By **sharing information on cyber capacity building measures** made available by UN member states, multilateral organizations
  - By **linking UN member states to capacity building opportunities** offered by the multi-stakeholder community including industry and academia.

- Let me mention in closing two practical examples. CBMs with a direct capacity building effect:
  - OSCE CBM 5: „use OSCE as a platform for dialogue, exchange of best practices, awareness raising, and info on capacity building
  - OSCE CBM 12: „activities to identify co-operative activities to reduce risks via workshops, seminars, round-tables

06 December

Statement in response to Chair's question on expectations for the OEWG session coming up in April 2023

Germany's expectations are as follows:

1. **Agree on modalities of PoC directory**
2. **Agree to establish in principle a first set of CBMs at UN level covering issues that have been raised in today's discussion.**

   Listening to today's discussion, such a first set of CBMs could cover

   1) Conduct of communication checks
   2) Information exchange
   3) Transparency measures
   4) Sharing of best-practices on incident response
   5) Sharing information on capacity building measures offered by UN member states and multilateral organisations

07 December

International Law

- Welcome the ideas put forward by Canada, Switzerland to deepen our discussions on applicability of international law with a special focus on Charter of the UN, peaceful settlement of conflicts, IHL, state responsibility.

- **Focus on state responsibility important**:

- Russia's brutal war against Ukraine also fought by cyber means.

- This is in reaction to the statement made by Cuba, which seemed to call into question whether **international military conflicts are fought in cyberspace. This is the reality we are already seeing in Europe today**.

- **Russia's cyber-attacks against Ukraine involve blatant violations of international law**: are being waged against critical infrastructure, key civilian institutions of Ukraine.

- **This reality makes it more relevant than ever to defend principles of international law.**

- Germany and our EU partners have adopted a joint practice of attributing cyber incidents.

- Recent attribution includes spill-over effects from Russia's cyber-attacks against Ukraine on critical infrastructure in Germany.

- **These spill-over effects can be clearly traced to Russia's cyber-attacks against Ukrainian targets. This is substantiated by detailed technical intelligence.**

- These attacks comitted in the context of Russia's war of aggression also **underscore the importance of expanding the discussion about state responsibility to one including the principles of state accountability**.

- Given the international security situation we operate in, Germany would like to **highlight the importance of putting renewed focus on applicability of international law in this group.**

- Germany looks forward to further advancing discussions on this important topic inside the OEWG in the years to come.

09 December

Regular institutional dialogue

- The overwhelming support of 157 positive votes for the PoA resolution in this year's First Committee has shown: The **PoA is now a common aspiration of a vast majority of states from all regions**.
- The inclusive and transparent consultations led by France and supported by the European Union have resulted in a sound resolution paving the

way for the **PoA as <u>the</u> permanent and action-oriented forum for global discussions on security of and in the use of ICTs**.

- **The PoA will take up its work after 2025 when the current OEWG will have completed its work.**
- In order to facilitate a smooth transition and an effective implementation of the OEWG's results, we **have to start working <u>now</u> on the modalities of the future PoA**.
- Germany is **looking forward to fruitful discussions about the structure and substance of the PoA based on input from all regional groups**.
- From our point of view, the PoA is a unique chance to **make a quantum leap from dialogue to implementation of cyber norms**, CBMs and capacity building.
- For effective implementation, strengthening the role of non-state actors will be crucial. We therefore **encourage to involve all stakeholders in the exchange about the future set-up of the PoA**.
- We would welcome if upcoming sessions of the OEWG dedicated appropriate opportunities for these discussions.
- Let's jointly take this opportunity to design the PoA as an inclusive and transparent UN mechanism that provides for responsible state behavior in cyberspace.