Pakistan's Views Concerning the Capacities required by the Member States to Effectively Participate in UN Points of Contact (PoCs) Directory

Pakistan believes that the Points of Contact (POCs), designed by the Member States, shall requires the following capacities to effectively participate in the Directory:

i. **Technical Expertise**: To understand and address the complex cyber threats, vulnerabilities, impact at national, regional level and mitigation strategies under collaborative framework.

ii. **Analytical Skills**: To assess cybersecurity risks, critically evaluate reported technical information, incidents, interpret consequences and make assessment report to seek informed decisions for further collaboration.

iii. **Policy & Regulatory Knowledge:** Ability to seek guidance on Policy and Regulatory (National, Regional, International) frameworks through domestic consultation, prior to any exchange of information. This includes data governance & protection laws, cybersecurity /cybercrimes frameworks, industry standards, diplomatic norms (avoid attribution) and responsible state behavior.

iv. **Communication Skills**: To collaborate with PoCs from other Member States as well as to communicate technical concepts and findings clearly and concisely to non-technical audiences, including executives, policymakers, and end-users.

v. **Continuous Learning and Adaptability**. Staying updated on the latest cybersecurity trends, best practices, and technologies and be able to adjust their approaches and strategies in response to changing cyber threats and international needs.

vi. **Cross-Cultural Competence**: Ability to effectively navigate cultural differences, communication styles, and working norms and respect for diverse perspectives and practices.

vii. **Ethical and Professional Conduct**: In their interactions with stakeholders, handling sensitive cybersecurity information, and making decisions that impact cybersecurity policies, practices, and outcomes.

2. Pakistan further believes that some specific capacity-building requirements of Technical-POCs to effectively participate in the Directory, may include the following:

i. **Hands-on Workshops and Simulations**: Providing practical experience in responding to real-world cybersecurity incidents and threats. These interactive sessions can help reinforce technical skills, enhance problem-solving abilities, and promote teamwork and collaboration.

ii. **Community Events**: Sharing insights, best practices, and practical advice for navigating the cybersecurity landscape while participating in peer learning sessions, technical forums, and community events.

iii. **Cross-functional Exercises**: Organizing interdisciplinary teams or working groups composed of IT professionals, cybersecurity specialists, legal experts, policy makers and business stakeholders, collaborate with each other and respond to various scenarios evolving due to cyber incidents and international cooperation.

iv. **Online Training**: Providing access to online training resources, webinars, technical blogs, and industry conferences.

v. **Skill Development**: Provide opportunities to attend specialized training courses, workshops, and seminars that address their specific technical needs and cyber diplomacy.

vi. **Cyber Drills & Competitions**: Conduct and support participation of interdisciplinary teams in cybersecurity competitions, hackathons, and '*Capture The Flag*' (CTF) events to foster innovation and problem-solving skills.

*****