Theme: *"Building Confidence and Security in the use of ICTs"*

At the outset, we commend the Co-Facilitators—the Permanent Representatives of Albania and Kenya—for their inclusive and transparent approach to the WSIS+20 Review, and also the Secretariat for diligently assisting in the preparation of the Elements Paper and facilitating meaningful engagement.

The Government of India has submitted its consolidated response to the Elements Paper, reaffirming our commitment to the WSIS vision of a people-centric, inclusive, and development-oriented Information Society. The views I share today are anchored in that submission and reflect India's broader approach to building a secure and trusted digital future.

The digital landscape of 2025 is unrecognizable from that of 2003. While connectivity has empowered billions, the proliferation of sophisticated cyber threats—from DNS abuse and ransomware to the potential misuse of generative AI—has undermined digital trust, often with real-world consequences for individual safety, public order, and national security. The WSIS+20 process, in this context, must move beyond abstract affirmations and provide a concrete roadmap for strengthening accountability, promoting cooperation, and future-proofing the integrity of our digital systems.

India believes that digital trust can no longer be viewed in isolation from cybersecurity. They are two sides of the same coin. A digitally empowered society cannot flourish unless its foundational systems inspire confidence—among users, governments, and industry alike.

User verification and accountability:

Strengthening cooperation between states and the multistakeholder community—particularly ICANN and domain name service providers—is essential to improving the accuracy of domain name registration data, enabling lawful access in exigent circumstances, and curbing the impunity of malicious online actors. Accountability and user verification must evolve hand in hand with privacy safeguards and anonymity must not become a shield for malicious actors engaging in unlawful online conduct.

We recommend that the WSIS +20 outcome document must promote cooperation between member states and the multistakeholder community within ICANN on verifying user identities, as also commonly accepted digital identifiers such as email addresses and mobile numbers, while safeguarding individual privacy to curb misuse and ensure responsible digital behaviour. Engagement with internet ecosystem actors is essential to improve domain name data accuracy

and facilitate lawful access by authorities. The IGF 2024 Riyadh Messages also highlight the need for secure, trusted digital identity systems using emerging technologies like Blockchain, AI and Biometrics.

Timely exchange of Information

In parallel, the WSIS+20 review process must also underline the importance of mechanisms that facilitate enhanced cooperation between member states and the multistakeholder community within ICANN for timely disclosure of information in cases involving national security, child sexual abuse material (CSAM), and public order concerns. This includes ensuring that domain name registries, registrars and service providers share verified identity details with law enforcement agencies in a timely manner preferably within 24 hours without compromising on legitimate privacy safeguards.

Security and Resilience of Critical Internet Infrastructure

The confidence we seek to build cannot rest only on procedural reforms; it must also be embedded in the resilience of our core internet infrastructure. India strongly supports the inclusion of the term *"critical Internet infrastructure"* within the relevant provisions of the Zero Draft on the theme Internet Governance to reflect the modern realities of digital interdependence. Submarine cables, DNS root servers, cloud infrastructure, and Internet Exchange Points (IXPs) are no longer technical footnotes; they are essential lifelines for commerce, communication, and crisis response. Their protection must therefore be elevated to a multistakeholder priority—both in technical terms and as a matter of public policy. The Zero Draft should also incorporate updated language that recognizes both legacy and emerging dependencies—such as cloud computing, DNS, routing systems, and undersea infrastructure—and promote a multistakeholder approach to their protection, resilience, and transparent governance.

Finally, confidence-building is not merely about systems—it is about people. **Capacity building,** especially in cybersecurity, must be placed at the centre of the WSIS+20 implementation framework. Technical capacity across the Global South remains uneven, which in turn exacerbates vulnerabilities and weakens deterrence. India underscores the importance of scaling up existing regional and global initiatives, encouraging inclusive knowledge exchange, and supporting targeted capacity-building efforts through a balanced

multistakeholder approach. Initiatives supported by the United Nations, in close coordination with governments, industry, civil society, and the technical community, can play a valuable role in Building Confidence and Security in the use of ICTs

Thank you.