Pakistan maintains a consistent position on developments in the field of Information and Communication Technologies (ICTs) having impact on international security. Pakistan recognizes the crucial role of ICTs and the internet in driving socio-economic growth and believes that the new and emerging technologies, particularly cyber and Artificial Intelligence (AI), are powerful tools for economic advancement, with their broad-ranging applications in communication, information access, commerce, healthcare, and industry. Additionally, ICTs are essential for governments to provide efficient governance and deliver essential services to citizens.

However, at the same time, the ubiquitous use of ICTs, especially cyberspace, poses new challenges having implications for global and regional security. The employment of cyber technologies and internet by cybercriminals for destructive purposes and its militarization is an undeniable reality. Pakistan considers that the possession of offensive cyber capabilities by certain states and the rising incidents of cyber attacks against the critical infrastructure are gradually turning cyberspace into an arena of conflict. Both state and non-state actors are employing cyber tools to degrade, disrupt, destroy and damage the critical infrastructure (CI) i.e. health, energy, transportation, industry, banking, and financial system responsible for the delivery of basic necessary services to the civilian population.

Pakistan participated in the 2014-2015 GGE and the 2019-2021 OEWG, and it is an active member of the UN Open-Ended Working Group (OEWG) (2021-2025) on the security of and in the use of Information and Communications Technologies (ICTs). Pakistan takes part in the discussions under all six agenda items of the OEWG, which include the study of existing and potential threats in the sphere of information security, the application of International Law in cyberspace and the use of ICTs, the development of norms, rules, and principles of responsible behavior of States in cyberspace, confidence-building measures (CBMs), capacity building, and regular institutional dialogue.

Pakistan’s Position on the Identification of Existing and Potential Threats Emanating from the Cyberspace

Like any other country, Pakistan is also grappling with threats emanating from the ungoverned cyberspace. The rise in cyber-attacks against critical infrastructure, the use of trojanized versions of mobile apps and websites to ex-filtrate the critical data of the citizens, Distributed Denial of Service (DDoS) attacks, fake news, and targeted misinformation and disinformation campaigns through social media and other digital platforms represent just a few facets of the cybersecurity challenges facing by the country. Therefore, Pakistan strongly advocates the formulation of a legally binding instrument to effectively counter these threats.

Pakistan asserts that state-sponsored disinformation campaigns constitute a violation of the UN Charter and amount to interference in the internal affairs of a state. Therefore, Pakistan calls for global coordinated efforts and the formulation of guidelines to effectively combat the spread of fake news, misinformation, disinformation, false narratives and hate speech in all their forms and manifestations.
6. Pakistan is also concerned about the employment of Artificial Intelligence (AI) for the design, development and deployment of more advanced and sophisticated cyber tools, by both state and non-state actors, and calls for the formulation of a code of conduct to ensure the responsible applications of AI.

7. Furthermore, Pakistan observes that the threat identification during OEWG and GGE meetings is highly skewed towards attacks on critical infrastructure and ignores the important issues, inter alia, i) further democratization of the bodies regulating internet globally, ii) growing digital divide among countries, iii) software piracy and intellectual property theft, iv) cross-border data security, v) timely disclosure of vulnerabilities, vi) supply chain security, etc.

**Pakistan’s Position on the Militarization of Cyberspace**

8. On the militarization of cyberspace, Pakistan's position is consistent. We consider the internet as a "Common heritage of mankind" like the ocean and outer space and believe that the use of cyberspace for military purposes risks converting it into another arena of military confrontation.

**Pakistan’s Position on the Application of International Law in Cyberspace and the Use of Information and Communication Technologies (ICTs)**

9. Pakistan's position on the application of international law in cyberspace has remained quite clear. Pakistan believes that the principles of non-use of force, sovereign equality of all nations, non-interventionism, and peaceful settlement of disputes, as enshrined in the UN Charter, equally apply to cyberspace as in the physical world. Pakistan is a proponent of “rules-based” cyberspace, open for all, to reaping maximum economic benefits.

10. However, Pakistan acknowledges the fact that considering the unique attributes of cyberspace and the transnational nature of cyber technologies, international law has certain gaps which must be addressed beforehand. For example, the application of concepts of sovereignty, self-defense, use of force, and attribution in cyberspace demands further clarity and in-depth discussion within United Nations.

11. Pakistan believes that the territorial sovereignty and national jurisdiction of states should be extended over ICT infrastructure residing within the territory of the State. Pakistan also proposes to get definitional clarities of the terms “cyber-attack”, “cyber-terrorism”, “Critical Infrastructure (CI)” and “Critical information infrastructure (CII)”, etc and to conduct further discussions on the application of International Humanitarian Law (IHL).

12. Pakistan believes that, in view of the unique attributes of cyberspace, there is a need for further neutral and objective debate to build a common understanding on the topics of the application of international law including the International Humanitarian Law (IHL) in cyberspace. Pakistan supports the formulation of a legally-binding instrument to ensure the responsible uses of ICTs and cyberspace.

13. In this regard, Pakistan also submitted a paper which, in detail, takes stock of Pakistan’s position on the application of international law in cyberspace including the need for the formulation of a legally-binding instrument to ensure the responsible employment of ICTs. The paper may be accessed at [https://docs-library.unoda.org/Open-Ended Working Group on Information and Communication Technologies-(2021)/UNODA.pdf](https://docs-library.unoda.org/Open-Ended Working Group on Information and Communication Technologies-(2021)/UNODA.pdf)
Pakistan’s Position on Non-Binding Cyber-Norms Building

14. Pakistan considers that the non-binding norms cannot be an alternative to a legally-binding instrument as an effective enforcement mechanism to ensure the responsible behavior of states in cyberspace. Furthermore, Pakistan also believes that the norms may work in peacetime but will lose utility in time of crisis, including wars. The main difference between non-binding norms and a legally-binding instrument is that the latter imposes certain obligations and their violation triggers the law of State responsibility. Moreover, norms are effective during peacetimes only and will lose efficacy in an event of war.

Pakistan’s Position on Confidence Building Measures (CBMs) and Global Points of Contact (PoC) Directory

15. Pakistan expresses deep concern about the rising trend of cyber attacks on the critical infrastructure, which is getting more complex and sophisticated. In such circumstances, Pakistan has always supported the idea of CBMs to avert confusion and escalation. Therefore, Pakistan unequivocally supported the establishment of the UN Points of Contact (POC) Directory and has nominated its PoCs Diplomatic and Technical.

16. Pakistan believes that PoC Directory shall be instrumental in averting confusion though the prompt exchange of information in an event of cyber-attack.

Pakistan’s Position on Capacity Building

17. Pakistan holds the view that capacity building of all states on equal footing is indispensable for a safe, secure and stable cyberspace. Pakistan also believes that the global capacity building initiatives should be demand-driven and designed taking into account the specific needs of the states. Furthermore, all states must be given fair, equitable and non-discriminatory access to cyber technologies along with the due right to participate and to make consensus-based decisions in the bodies responsible for regulating the global internet.

Pakistan’s Position on Regular Institutional Dialogue

18. Pakistan’s position on the topic of regular institutional dialogue, including the Programme of Action (PoA), is quite clear. Pakistan maintains that the key principles that should be considered in the formulation of future platforms for discussions on ICTs must include inclusivity, transparency, consensus-driven decision-making, multi-stakeholder participation, global collaboration, and sustainability. Pakistan believes that the future institutional dialogue must also include in its mandate the topics of capacity building, norms building, and the application of international law in cyberspace including discussion on the formulation of a legally-binding instrument to regulate the behaviors of states in cyberspace. Furthermore, Pakistan holds the view that such dialogue should take place under the auspices of the UN.

************