Working Paper by Pakistan

Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security

Introduction

1. Pakistan attaches immense importance to the Open-ended working group on developments in the field of information and telecommunications in the context of international security (OEWG), established pursuant to General Assembly resolution 73/27 of December 2018. The OEWG represents the first inclusive institutional process under the UN auspices, having universal membership on this topic of great significance.

2. Information and communications technologies (ICTs) have reshaped and transformed every aspect of national and global economies and societies. Progress in this field is a measure and driver of economic growth and prosperity. However, the benefits offered by ICTs and emerging technologies do not come without risks.

3. Threats to security and stability in cyberspace due to the malicious use of ICTs risk undermining the opportunities offered by ICTs. This represents a global challenge that requires a global response. There is an urgent need to identify and formulate rules for State behaviour, as well as to develop clarity regarding rules and responsibilities for States and other stakeholders, to increase stability and security in the global ICT environment.

4. In this context, the OEWG provides an extremely useful forum for achieving meaningful progress, building on the previous recommendations on this topic in order to strengthen rules for responsible State behavior in cyberspace, and to achieve meaningful international cooperation to minimize the threats posed to international security by the malicious uses of ICTs.

5. Pakistan hopes that the OEWG would be able to achieve meaningful outcomes on the following main fronts:

a) Elaborating detailed rules based on the recommendations of the previous Groups of Governmental Experts (GGEs) which have been endorsed by the General Assembly. There is a need for the United Nations to adopt **binding rules for responsible State behaviour in relation to the use of ICTs**. The 2015 GGE recommendations could provide a useful basis for such politically or legally binding rules.

b) Arriving at a preliminary **agreement on the establishment of an inclusive institutional platform** dedicated to international cooperation on ensuring the peaceful uses of ICTs and mitigating their associated risks. Such an institutional platform could enable an inclusive and transparent exchange of information on vulnerabilities and best-practices, foster international cooperation and capacity-building, issue recommendations on Confidence-Building Measures (CBMs), and contribute to addressing the threats to security and stability in the cyber domain.

c) Agreeing to meaningful **recommendations on capacity-building measures**, **especially for developing countries, and on international cooperation** in this field.

Existing and potential threats

6. ICTs provide vast opportunities for social and economic development and are increasingly growing in importance for the international community. However, there are disturbing trends in the global ICT environment, which include a dramatic increase in incidents involving the malicious use of ICTs by State and non-State actors. These trends create risks for all States. Misuse of ICTs carries the serious risk of harming international peace and security.

7. ICTs can be used for both legitimate and malicious purposes due to their dual-use nature. A number of States are developing ICT capabilities for military purposes, making their use in future inter-State conflicts more likely (UNGA Resolution 73/27). The pursuit by some States of military objectives in cyberspace, including though introduction and formulation of rules of engagement in this realm, are increasing the risks of conflicts in cyberspace, thus undermining international peace and security.

8. Cyber operations against a State's critical infrastructure and associated information systems constitute the most harmful attacks using ICTs which can undermine States' national security, economic development and people's livelihood. The risk of harmful ICT attacks against critical infrastructure is both real and serious, and is growing. Traditional military facilities constitute critical infrastructure, which if compromised, would have far reaching security ramifications.

9. The use of ICTs by malicious non-State actors for criminal and terrorist purposes, including recruitment, financing, training and incitement, as well as for attacks against ICTs or ICT-dependent infrastructure, carries grave risks for international peace and security, especially in light of the attribution related challenges.

10. The diversity of malicious non-State actors, including criminal groups and terrorists, their differing motives, the speed and anonymity associated with malicious ICT actions and the difficulty of attributing the source of an ICT incident, all increase risk. States are rightfully concerned about the danger of destabilizing misperceptions, the potential for conflict and the possibility of harm to their citizens, economy and national security.

11. The relative ease with which malicious technologies are available and accessible to a very large number of State and non-State actors, and their continued development, especially by technologically advanced States, increases their proliferation risks. Transfer, replication or reproduction of malicious technologies by terrorists and criminals poses a real threat.

12. Stockpiling of "vulnerabilities" in ICT systems and the potential threat posed by "autonomous cyber operations" that are capable of actively impersonating networks and people further undermines security in the ICT environment.

13. There exist real threats associated with manipulation and theft of digital identity, private data as well as targeted propaganda campaigns in ways that could undermine national economies and imperil national security, besides jeopardizing personal security of individuals.

14. Threats in the global ICT environment also undermine full realization of the opportunities offered by emerging technologies like artificial intelligence (AI), cloud computing, big data, the Internet of Things (IoT), e-government services, blockchain technology and digital finance.

15. Harmful hidden functions embedded in ICTs pose a threat to ICT supply chain, erode public trust in digital commerce and undermine national security and global development. Malicious use of ICTs thus impedes social and economic development and hampers progress towards the achievement of sustainable development goals.

16. The absence of common understandings on acceptable State behaviour with regard to the use of ICTs further aggravates the threat landscape.

17. In an increasingly interconnected world, varying levels of capacity for ICT security among States can immensely increase and amplify vulnerability. Thus, the widening "digital divide" among countries and regions poses a serious threat in the global ICT environment.

International Law

18. Previous GGEs have concluded that international law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, stable, accessible and peaceful ICT environment.

19. The principles of international law and Charter obligations provide a fundamental framework guiding States' use of ICTs. The principles of sovereignty; sovereign equality; the settlement of international disputes by peaceful means; refraining from the threat or use of force against the territorial integrity or political independence of any State, or in any other manner inconsistent with the purposes of the United Nations; respect for human rights and fundamental freedoms; and non-intervention in the internal affairs of other States, are cross-cutting in nature and must be adhered to in all domains, including cyber-space. Respect for and compliance of these principles must be the international community's first port of call in maintaining security and stability in the ICT environment.

20. The issue of the applicability of the law of armed conflict (jus ad bellum) and States' "right to self-defense" under article 51, as well as the applicability of the rules of engagement in military conflicts in the ICT context raises legitimate concerns of States.

21. Given the unique differences between the physical and cyber spheres, including speed, stealth and anonymity associated with the use of ICTs, as well as the difficulty in attributing the source of an ICT incident; this issue requires careful consideration. There is a need to adapt international law according to the unique characteristics of the ICT environment.

22. Every effort must be made to prevent cyberspace from turning into an arena of conflict. Pending a universal and internationally agreed understanding on this issue, States should refrain from interpreting the applicable international law in the ICT environment, which could exacerbate the security and stability risks in this domain. States should instead focus on cooperating to prevent conflicts in cyberspace from erupting in the first place.

23. Differences on this issue among Member States should however not prevent the OEWG from focusing its attention and efforts on translating the existing norms and recommendations into more elaborate, operational, and binding measures that guide States in their use of ICTs in the context of international security.

24. Pakistan also recognizes the need for legally binding international instruments, specifically tailored the unique attributes of ICTs, which can provide a regulatory course to ensure stability and security in the ICT environment. Such a framework should address the concerns and interests of all States, be based on consensus, and pursued within the UN with equal participation of all stakeholders.

Rules, norms and principles

25. Voluntary, non-binding norms of responsible State use of ICTs can contribute to reducing risks to international peace and security. However, given the unprecedented threats in the ICT environment and the rapid pace of technological developments, there is a need to strengthen international efforts to develop binding rules that can help in maintaining peace and stability and promote an open, secure, stable, accessible and peaceful ICT environment.

26. Such rules should guide States in their use of ICTs in order to prevent conflict in the ICT environment, as well as the legitimization of the use of force and weaponization of this domain.

27. At the same time, they should avoid any undue restrictions on the peaceful uses of ICTs, international cooperation in this field or technology transfer, which could undermine economic and social

development and hamper the efforts, particularly of developing countries, in realizing their sustainable development goals.

28. The elaboration of binding norms would help in strengthening cooperation and trust between governments, as well as between governments and the private sector. Such norms and rules must also set standards for stakeholders and entities from the private sector.

Confidence Building Measures

29. Previous GGE reports have recognized that CBMs strengthen international peace and security and that they can increase interstate cooperation, transparency, predictability and stability.

30. Reports of previous GGEs include valuable recommendations that can enhance confidence among States in the ICT environment. These include: identification of points of contact to address serious ICT incidents; development of mechanisms and processes for bilateral, regional, subregional and multilateral consultations to reduce the risk of misperception, escalation and conflict from ICT incidents; and encouraging transparency on a voluntary basis to increase confidence.

31. Voluntary sharing of information regarding infrastructure that they consider critical and national efforts to protect them, including national laws and policies for the protection of data and ICT-enabled infrastructure, also represents a useful measure.

32. Establishment of computer emergency response team at the national level and promoting cooperation among such bodies represents a useful measure. Such cooperation could include, where appropriate, addressing requests from other States to investigate ICT-related incidents or to mitigate malicious ICT activity emanating from their territory, while taking into account the possible limitations on the technical capacities of developing countries to address such requests.

Capacity-building

33. States bear primary responsibility for national security and the safety of their citizens, including in the ICT environment. However, some States may lack sufficient capacity to protect their ICT networks.

34. In a highly interconnected world, lack of capacity for ICT security among States may present a serious threat to security and stability in the global ICT environment. Towards this end, international cooperation and assistance to enhance States' capacity can play an essential role in enabling them to secure ICTs, ensure their peaceful use and strengthen international security.

35. Previous GGE reports have recommended a number of measures to develop capacity of States. These include assistance in strengthening cooperative mechanisms with national computer emergency response teams; providing assistance and training to developing countries to improve security in the use of ICTs, including critical infrastructure, and exchanging best practices; providing access to technologies deemed essential for ICT security.

36. The 2015 GGE report has emphasized that capacity-building involves more than a transfer of knowledge and skills from developed to developing States, as all States can learn from each other about the threats that they face and effective responses to those threats.

37. Varying levels of capacity among States underscores their 'common but differentiated responsibility' in making the global ICT network safe and secure. Developed countries have a special responsibility in bridging the digital divide, securing the global ICT environment and achieving the development goals though international cooperation and assistance.

38. Capacity-building must be seen as a trust-building measure, requiring steps to ensure that capacity-building remains politically neutral, with the objective of bridging inequalities caused by the "digital divide".

39. Developing countries could benefit from technical and financial assistance in improving their emergency response capabilities and filling gaps in the protection of critical infrastructure, which exist due to the lack of financial investment and much needed technical capacity in developing Critical Infrastructure Protection frameworks.

Regular Institutional Dialogue

40. The United Nations has a central role in promoting dialogue on the security of ICTs in their use by States and developing norms, rules and principles for responsible State behaviour in this field.

41. An inclusive, multilaterally-agreed, and consensus-based process within the UN System represents the best way to ensure that the agreed arrangements in this field take into account the concerns of all States and are equitable, comprehensive and are effectively implemented.

42. Dialogue on this subject should take place within an inclusive institutional platform and should focus on advancing discussions on this subject, including on ways to enhance implementation of the agreed rules and developing and elaborating further norms in this field.

43. States have the primary responsibility for maintaining a secure and peaceful ICT environment. However, private sector entities, academic experts, and civil society organizations should also be allowed to share their experiences and express their views during discussions within such a UN-led process.

44. Establishment of a specialized institutional forum on this subject under the UN auspices could represent a major contribution towards strengthening international efforts to ensure a more reliable and secure global ICT environment.

45. The Conference on Disarmament also represents an appropriate venue for multilateral discussions which can focus on elaborating elements of an international instrument on this subject. Such an instrument should delineate the limits of acceptable State behavior in ICT environment in the context of international peace and security and provide for international assistance and cooperation.

___