ISSUE BRIEF

INSTITUTE OF STRATEGIC STUDIES ISLAMABAD
Web: www.issi.org.pk
Phone: +92-51-9204423, 24
Fax: +92-51-9204658

PAKISTAN'S POSITION ON SECOND ANNUAL PROGRESS REPORT OF THE UN OEWG ON SECURITY AND USE OF ICTS IN THE CONTEXT OF INTERNATIONAL SECURITY 2021-2025

By
Aamna Rafiq
Research Associate
Arms Control & Disarmament Centre, ISSI

Edited by
Malik Qasim Mustafa

October 11, 2023

The Open-ended Working Group (OEWG) on the security of and in the use of Information and Communications Technologies (ICTs) 2021-2025 reached a consensus on its Second Annual Progress Report. The consensus report came at a crucial time as the UN is celebrating 25 years of discussions on the topic of ICTs in the context of international security.

Militarization of ICTs: Existing and Potential Threats

In this report, UN member states expressed their concerns vis-à-vis potentially malicious and irresponsible use of ICT capabilities by state and non-state actors. The increasing militarization of dual-use ICT capabilities in the wake of an unstable geopolitical landscape and rapid commercialization has resulted in the rapid proliferation of ICT capabilities and the formation of the international black market. The report also highlights wide-ranging existential and potential threats like data theft, misinformation, ransomware, malware, and phishing to the critical infrastructure (CI) and critical information infrastructure (CII), which provide services in essential sectors like healthcare, supply chains, aviation, and maritime. Highlighting the gender dimension of these threats and the digital divide across the globe makes this report more inclusive and equitable. While recognizing the significance of a global information-sharing mechanism for raising awareness, UN member states proposed the development of a "threat repository." This repository could be further

linked with the global directory of point of contact (PoC) and technical PoC to achieve synergy.[1] With respect to the militarization of ICTs, Pakistan has a consistent position. Pakistan considers cyberspace a "common heritage of mankind" and calls for a complete ban on the development of all kinds of offensive applications of ICTs.[2]

Rules, Norms, and Principles of Responsible State Behaviour

UN member states recognized the importance of voluntary norms and the exchange of best practices vis-à-vis responsible state behavior for the protection and recovery of CI and CII from malicious use of ICTs. While recognizing the substantial role of existing norms, states agreed to the development of additional norms in collaboration with the tech industry and non-governmental organizations. They also proposed developing norms and rules to ensure the integrity and security of global supply chains. These proposals include exchanging multilateral, regional, and bilateral cooperative measures regarding supply chain risk management and preparing a set of global standards for supply chain security and stability. States also proposed the development of a glossary of national definitions of technical terms to assist each other in understanding and interpreting the norms and principles voluntarily. To assist developing and small states in the implementation of these norms, an additional "norm implementation checklist" will be developed.[3]

Pakistan not only supports the existing 11 voluntary norms but also the formulation of new norms. Pakistan also maintains a position that these norms would be beneficial during peacetime only and lose their effectiveness in case of an armed conflict. However, these voluntary norms, rules, and principles should not be used as a substitute for a legally binding instrument, supported by a robust enforcement, verification, and accountability mechanism.

Applicability of International Law

With respect to the applicability of international law to the use of ICTs, UN member states agreed that the principles of "state sovereignty and sovereign equality" would be applicable. As per Articles 2(3) and 33(1) of the UN Charter, all states would settle their disputes by peaceful means to ensure international peace, security, and justice. These peaceful means include but are not limited to

1 Chair Open-Ended Working Group on Security of and in the use of Information and Communications Technologies 2021-2025, *Zero Draft of the Second Annual Progress Report of the OEWG,* accessed September 28, 2023, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Letter_from_OEWG_Chair_13_June_2023_(with_Zero_Draft_Second_APR_enclosed).pdf.

2 Permanent Mission of Pakistan to the United Nations, *Pakistan's Position on the Application of International Law in Cyberspace* (New York, March 3, 2023), https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/UNODA.pdf.

3 *Zero Draft of the second Annual Progress Report of the OEWG.*

inquiry, mediation, negotiation, conciliation, judicial settlement, and arbitration. In accordance with Article 2(4) of the UN Charter, states would refrain from the use of force against the political independence and territorial sovereignty of other states. Furthermore, all states shall follow the principle of non-interference in the internal affairs of another state. The most contentious aspect of this report is that the international humanitarian law (IHL) is only applicable to the use of ICTs in an armed conflict. Furthermore, the applicability of principles of humanity, distinction, proportionality, and necessity without any detailed study would encourage and legitimize the conflict.[4]

With respect to the applicability of international law to the use of ICTs, Pakistan maintains a position that the UN charter along with the principles of non-intervention, peaceful settlement of disputes, non-use of force, and sovereign equality applies to the use of ICTs. Keeping in view the complexities involved, Pakistan emphasizes the need for further debate vis-à-vis the applicability of principles of self-defence, sovereignty, and attribution. Pakistan also believes that IHL applies to ICTs. However, the real debate is how to apply the IHL as member states have conflicting views on this subject. Pakistan believes that there is a need to transform the IHL to accommodate the complex and unique nature of modern warfare. The key issues like defining a cyber-attack, attribution, threshold for an armed conflict, and distinction between a civilian and a combatant largely remain unsettled. Furthermore, the complexities surrounding the applicability of two other cardinal principles of IHL, namely, proportionality and preaution to dual-use ICTs are still unsolved. Pakistan believes that till the achievement of this transformation, the Geneva Conventions and its Additional Protocols (APs) related to distinction will continue to apply to the use of ICTs during an armed conflict. Member states must refrain from causing indiscriminate damage through cyber weapons. They must also make a clear distinction between military and civilian targets to avoid collateral financial and human loss. [5]

Confidence-Building Measures (CBMs)

In addition to the implementation of an existing set of CBMs vis-à-vis the use of ICTs at the global level, there is a need for additional measures that could be recognized as CBMs through further deliberations. In order to achieve this goal, the establishment and operationalization of the global PoC directory is the first and foremost step. They further proposed that certain aspects of these CBMs also involve participation and cooperation from regional as well as sub-regional organizations. A detailed List of Voluntary Global CBMs is also included in Annex B of this annual progress report.

4 Ibid.

5 Permanent Mission of Pakistan to the United Nations, *Pakistan`s Position on the Application of International Law in Cyberspace* (New York, March 3, 2023), https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/UNODA.pdf.

Pakistan has always supported the idea of developing and implementing CBMs on security and the use of ICTs. Pakistan is in favor of establishing a global directory of PoC as an important CBM. It would promote trust, transparency, and cooperation and facilitate crisis management. This global directory of PoC could be established under UNODA where states could seek information related to an incident and engage in cyber dialogue. In addition to states, Pakistan insists on including private entities as well. However, states would be solely responsible for data upgradation.[6] Furthermore, Pakistan also acknowledges the Initial List of Voluntary CBMs.[7]

Capacity-Building and Regular Institutional Dialogue

The report recommends developing a holistic, sustainable, effective yet affordable approach to capacity-building efforts. This approach must include short-term initiatives for urgent threats as well as long-term capacity-building initiatives to ensure sustainability like South-South, South-North, and triangular cooperation. Acting as a leading international body, the UN would conduct a "mapping exercise" to enlist all the capacity-building initiatives within and outside the UN to develop a better synergy among them. Furthermore, the new "Global Cyber Security Cooperation Portal (GCSCP)" would be developed under the auspices of the UN which would act as a "one-stop-shop." The operations of GCSCP would be synergized with the existing portals maintained by the United Nations Institute for Disarmament Research (UNIDIR) and the Global Forum on Cyber Expertise (GFCE).

In the report, the UN member states recognized the centrality and importance of the OEWG as a mechanism within the UN for raising awareness and discussing security in the use of ICTs. States also considered the proposal to establish a Programme of Action (PoA) and its relationship with OEWG. States also proposed the establishment of a permanent group, conference, convention, or commission to not only address all aspects and issues related to security in the use of ICTs but also oversee the implementation of norms, rules, principles, CBMs, and legally binding instruments in the future. However, states also agreed that any of these proposed institutional dialogues or mechanisms would be established as a single-track, state-led, and permanent mechanism under the

6 United Nations Office for Disarmament Affairs (UNODA), *Pakistan's Views on the Establishment of a Global Directory of Points of Contact (PoCs)*, accessed https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Pakistan_Views_on_global_PoC__.pdf.

7 United Nations Office for Disarmament Affairs (UNODA), *Pakistan's Interventions during the 5th Substantive Session of the UN Open Ended Working Group (OEWG) on Security of and in the Use of Information and Communication Technologies (ICTs) in the Context of International Security*, accessed on September 30, 2023, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Pakistan_Statements_5th_Session_OEWG.pdf.

auspices of the UN and reporting directly to the First Committee of the UN General Assembly (UNGA).[8]

Pakistan views an equitable and non-discriminatory capacity-building of all the UN member states as critical for the establishment and success of a global cyberspace regime. Pakistan also believes that the OEWG is a suitable platform to discuss the issues related to the security and use of ICTs and the proposal of the PoA. After the conclusion of the existing OEWG process, any future platform should be consensus-based and all-inclusive, and established under the auspices of the UN.[9]

Conclusion

The consensus report came at a crucial time as the UN is celebrating 25 years of discussions on the topic of ICTs in the context of international security. Since the introduction of the first UNGA resolution on this subject in 1998, the geopolitical, strategic, and technological landscape has evolved drastically. Simultaneously, the challenges, risks, and threats generated by the malicious use of technologies are increasing in scale, scope, and severity. With each passing day, it is becoming difficult for states to keep up with these shifts and align the UN processes with them. Still, states successfully achieved consensus on various norms, principles, rules, CBMs, and capacity-building initiatives. The issues like applicability of international law and IHL and the formulation of legally binding instruments need further debate and analysis. This consensus report proposes a future roadmap for all necessary aspects. It is now the responsibility of member states to materialize this roadmap through effective communication, cooperation, and political will.

8 *Zero Draft of the second Annual Progress Report of the OEWG*

9 Permanent Mission of Pakistan to the United Nations, *Pakistan`s Position on the Application of International Law in Cyberspace* (New York, March 3, 2023), https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/UNODA.pdf.