PAKISTAN MISSION TO THE UNITED NATIONS
8 EAST 65TH STREET, NEW YORK, NY 10065
TEL: (212) 879-8600 FAX: (212)-744-7348

No. First-1/12/2023

The Permanent Mission of Pakistan to the United Nations in New York presents its compliments to the United Nations Office for Disarmament Affairs in New York, has the honour to attach Pakistan's position on the Application of International Law in Cyberspace.

The Permanent Mission of Pakistan to the United Nations avails itself of this opportunity to renew to the United Nations Office for Disarmament Affairs, the assurances of its highest consideration.

New York, the 3rd March 2023

Pakistan Mission to the United Nations
New York

United Nations Office for Disarmament Affairs (UNODA),
United Nations Headquarters,
New York

Email: prizeman@un.org

Pakistan's Position on the Application of International Law in Cyberspace

The crucial role of the internet in driving socio-economic growth is undeniable. Information and Communication Technologies (ICTs), particularly cyberspace, have proven to be a powerful tool for economic advancement, with broad-ranging applications in areas such as communication, information access, commerce, health care, and industry. ICTs are essential for governments to provide efficient governance and deliver essential services to citizens

2. However, at the same time, the ubiquitous use of ICTs poses new challenges as well. The usageof cyberspace by cybercriminals for destructive purposes and its militarizationis an undeniable reality. The possession of offensive cyber capabilities by certain Statesand a spree of cyberattacks against the critical civilian infrastructure by both States and Non-States actors witnessed in recent years are gradually turning cyberspace into an arena of conflict. Both State and Non-State actors are employing cyber weapons to degrade, disrupt, destroy and damage the critical infrastructure (CI) *i.e. health, energy, transportation, industry, governmental, banking, and financial system,* responsible for the delivery of basic necessary services to the civilian population.

3. In addition to this, the last reports of GGE and OEWG express concerns about the implications of the malicious use of ICTs for the maintenance of international peace and security and its use for military purposes[1]. According to the reports, threat actors in cyberspace which include **i)** State actors, **ii)** Non-State actors, **iii)** Cybercriminals and hackers[2] are responsible for posing existing and potential threats such as attacks on critical infrastructure, ransomware attacks, Distributed Denial of Services (DDoS) attacks, fake news, and disinformation campaigns through fictitious domain names and social media platforms. Such a situation calls for the urgent attention of the international community for the formulation of a mechanism to ensure the peaceful and responsible use of cyberspace.

4. The paper takes stock of Pakistan's position on the militarization of cyberspace and the application of International Law including the UN Charter as well the International Humanitarian Law (IHL) in cyberspace.

Pakistan's Position on the Militarization of Cyberspace

5. 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 an arena of military confrontation. Therefore, Pakistan calls for an outright ban on the development of offensive cyber weapons.

---

[1] GGE 2021 Report, OEWG 2021 Report
[2] Ibid

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

6. 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, continue to apply in cyberspace as in the physical world.

7. Moreover, there also exists an agreement among the States, as reflected in the reports of GGE and OEWG[3], that "*Internationallaw, and in particular the Charter of the United Nations, is applicable and essential to maintainingpeace and stability and promoting an open, secure, stable, accessible and peaceful ICT environment. In this regard, States were called upon to avoid and refrain from taking anymeasures not in accordance with international law, and in particular the Charter of the UnitedNations*".

8. However, Pakistan acknowledges the fact that considering the unique attributes of cyberspace and the transnational nature of cyber technologies applicability of international law poses certain challenges which need to be addressed. Therefore Pakistan supports an objective debate among the Member States to agree on defining the mechanism for the application of the concepts of sovereignty, self-defense, non-use of force, peaceful settlement of disputes, and attribution in cyberspace. The reports of OEWG and GGE also concluded that further common understandings need to be developed on how international law applies to State use of ICTs[4].

Application of International Humanitarian Law (IHL) in Cyberspace

9. Like international law including the UN Charter, there also exists a consensus among the States that International Humanitarian Law (IHL) does have applicability in cyberspace. However, the real debatable point is how IHL applies to cyberspace. Moreover, States have divergent set views on modifying the existing framework of IHL in view of the constantly changing nature of warfare.

10. In the past, efforts were made in the form of projects like the Tallinn Manual 3.0 or the Cyber Law Toolkit, which are academic, non-binding studies to examine the applicability of international law and IHL in cyberspace. The Tallinn Manual provides much guidance in this regard. However, key issues relating to the defining of a threshold for an armed conflict, status, and attribution remain unsettled.

11. The most important issue, while discussing the application of IHL in cyberspace, is that of ensuring the transposition of the three cardinal principles of International Humanitarian Law, namely, *distinction*, *proportionality*, and*precaution* during cyber operations. Their application is complicated because of the complexity of cyber-operations, the interconnectedness of computer systems, and the use of the same internet infrastructure

[3] GGE 2021 Report, OEWG 2021 Report
[4] ibid

by both civilians and the military. Militaries utilize the same internet backbone and transmission lines for communication, used by the civilian critical infrastructure. Targeting an adversary's military internet infrastructure during a conflict may result in civilian human and financial loss.

12. Pakistan believes that the Geneva Conventions and its Additional Protocols (APs) related to distinction whereby, parties to a conflict must distinguish between civilians andcombatants and between civilian objects and military targets, continue to apply during cyber conflicts. Moreover, the use of any type of cyber weapon which causes indiscriminate damage is outlawed under IHL and the critical civilian infrastructure and the civilian population shall remain protected during cyber conflicts. Pakistan is of the view that owing to the interconnected nature of the internet and related infrastructure, the existing framework of IHL needs transformations to accommodate the needs of modern warfare to guarantee that the cardinal principles of IHL i.e. *distinction*, *proportionality*, and*precaution*are upheld.

13. *In view of the above-mentioned limitations of the existing framework of IHL, Pakistan calls for the formulation of a legally-binding instrument to not only promote the responsible behavior of States in cyberspace and to regulate the use of cyber and other digital technologies to ensure that they will not be violating the IHL.*

What Constitutes a Cyber-attack?

14. Furthermore, Pakistan also proposes to get definitional clarities of the terms "*cyber-attack*", "*cyber-terrorism*", "*Critical Infrastructure (CI)*" and "*Critical information infrastructure (CII)*", etc for a more focused discussion on the application of international law including the IHL in cyberspace. Pakistan considers the following uses of cyber and other digital technologies, which constitute a cyber-attack and must be outlawed under IHL:

- Cyber and any digital weapon with the capacity to indiscriminately and disproportionately target critical civilian infrastructure and may cause human and financial loss at a mass scale.
- The employment of cyber and other digital weapons which undermines the confidentiality, integrity, and the availability of a critical civilian infrastructure which includes but is not limited to health, transportation, energy, banking and financial sector, civilian logistical supply chains, undersea fiber optic cables, satellites, and other telecommunication networks.
- Any attempt to delete, destroy and manipulate the data essential for the smooth functioning of the critical civilian infrastructure and may impair its operations.
- Employment of cyber and other digital technologies to spread fear and chaos among the civilian population through disinformation.

The Conundrum of Attribution

15. Pakistan hold the view that until the conundrum of the attribution doesn't get resolved, the proper application of international law and IHL in cyberspace will not be

possible. Because of the factors like the use of cyberspace byboth State and Non-State actors, anonymity, and the transnational nature of the internet, the fair attribution of a cyber-attack to its actual perpetrator is complex, but not insurmountable. Strong coordination and cooperation among the Member States may result in an accurate tracing of IP addresses back to the origin of the attack.

16. It is indispensable to solve the conundrum of attribution to ensure that the attackers, whether State or Non-State actors, shall be held accountable if found violating international law.

Pakistan's Position on the Development of Norms, Rules, and Principles of Responsible Behavior of States in the Cyberspace

17. Pakistan supports the implementation of the 11 already agreed voluntary norms[5] as well as the formulation of additional norms over the period of time. However, at the same time, Pakistan considers that voluntary norms can't be a substitute for a legally binding instrument backed by an effective enforcement mechanism. A legally-binding instrument imposes certain obligations and their violation triggers the law of State responsibility. In addition to this, norms are effective during peacetimes only and will lose efficacy in the event of a conflict.

Data Security

18. Pakistan advocates the global regulations on data security and cross-border exchange of data. Pakistan supports the formulation of a mechanism for the protection of data contained by critical infrastructures and to criminalize any act aimed at stealing, deletion, destroying, and manipulating data essential for the smooth functioning of critical civilian infrastructure.

19. In addition to this, private entities having transnational operations, should respect the local laws and regulations about data security and data residency and must not indulge, without prior permission, in an act of transferring citizens' critical data to other States. Moreover, international private entities associated with ICT-related businesses must cooperate with law enforcement agencies in combating cybercrimes and cyberattacks.

Capacity Building

20. Pakistan views capacity building of all States on equal footing is indispensable for a secure and stable cyberspace and the effective implementation of international law in cyberspace. Pakistan calls for fair, equitable, and non-discriminatory access to cyber technologies and products.

21. There is a need for providing scholarships, fellowships, and training for cybersecurity professionals from developing states in the areas of critical infrastructure security, cyber policymaking, application of international law in cyberspace, etc. In this regard, United Nations Institute for Training and Research (UNITAR), International Telecommunication

[5] 2015 GGE Report

Union (ITU), United Nations Institute for Disarmament Research (UNIDIR) can play an important role.

Future Platform for Discussions on ICT Security

22. Pakistan opines that after the conclusion of the existing OEWG, any future platformfor discussions on the matters pertaining to the ICTs and their impact on international security shouldbe all-inclusive and consensus-driven, and must be constituted under the auspices of the United Nations.

23. Pakistan believes that the future mechanism and its mandate areas should be finalized through a consensus-driven process and the ongoing work of the OEWG is ideally suited for this conversation. Therefore in Pakistan's view, it would be better to examine the proposal of a Programme of Action (PoA)within the ongoing OEWG.

****