GLOBAL SOUTH PERSPECTIVES ON CYBER GOVERNANCE: PAKISTAN'S ADVOCACY FOR A LEGALLY BINDING ICT FRAMEWORK AT THE UN

Iraj Abid*

Abstract

This paper examines Pakistan's position at the United Nations (UN) for the responsible use of Information and Communication Technologies (ICTs). While ICTs have become a powerful driver of socio-economic development, their dual-use poses significant risks to national and international security. The governance of ICTs and broader questions of cybersecurity have been on the UN agenda since 1998. The World Summit on the Information Society (WSIS), held in two phases in Geneva (2003) and Tunis (2005), was the first global UN platform where states collectively debated the political, economic, and developmental implications of ICTs. The issue holds significance for all the member states; however, as with other security-related matters, states have diverse and often conflicting positions on the governance of ICTs. In this paper, Pakistan's call for a legally binding international instrument on ICTs is examined as an expression of both its security concerns and broader approach to multilateral governance of ICTs. Pakistan's stance has been articulated through its interventions at and position papers submitted to various UN forums, including the WSIS, the UN General Assembly, the Group of Governmental Experts (GGE) on ICTs, and the Open-Ended Working Group (OEWG) on ICTs. However, there is a lack of scholarly analysis of Islamabad's position on the governance of these crucial technologies. This study analyzes Pakistan's advocacy under the theoretical framework that combines constructivism with a Global South perspective. This approach highlights how developing states shape their stance and advocacy regarding technology governance. The study is qualitative in nature and relies on secondary data sources for analysis.

Keywords: *Information and Communication Technologies (ICTs), Cybersecurity, Pakistan, United Nations, Global South, National Security*

* Research Officer at the Center for International Strategic Studies Sindh (CISSS), Karachi. Email : irajabid@cisss.org.pk

Introduction

Information and Communication Technologies (ICTs) have become ubiquitous in today's world. From individual life to governance, economy, and even security, every aspect of human life involves ICT tools. According to the United Nations Educational, Scientific, and Cultural Organization (UNESCO), ICTs are defined as "diverse set of technological tools and resources used to transmit, store, create, share or exchange information. These technological tools and resources include computers, the Internet (websites, blogs, emails), live broadcasting technologies (radio, television, and webcasting), recorded broadcasting technologies (podcasting, audio and video players and storage devices), and telephony (fixed or mobile, satellite, video-conferencing)".[1] The UN recognizes ICTs as pivotal in driving social, economic, and political development and facilitating the implementation of global initiatives, such as the Sustainable Development Goals (SDGs).[2]

However, as ICTs become increasingly integrated into critical infrastructure, their dual-use nature has raised concerns about their potential misuse, particularly in the context of cyber threats for both national and international security. The governance of ICTs and their security implications have been central to discussions at the UN since 1998. Despite the growing acknowledgment of their role in national and international security, the global community remains divided on how best to regulate and secure cyberspace. The issue gained formal attention during the World Summit on the Information Society (WSIS) in Geneva (2003) and Tunis (2005), where global discussions began to coalesce around issues of ICT governance, digital access, and cybersecurity. Since then, Pakistan has consistently advocated for the establishment of a legally binding international instrument to govern ICTs. Pakistan's advocacy reflects both its national security concerns and broader principles of multilateral governance in the digital age.

This paper argues that Pakistan's advocacy for a legally binding international cybersecurity framework reflects broader Global South concerns regarding sovereignty, strategic inequality, and exclusion from norm-making processes dominated by technologically advanced states. Through a constructivist Global South lens, the paper demonstrates that Pakistan's position is not merely a national security response, but a

---

1 UNESCO Institute for Statistics, "Information and Communication Technologies (ICT)," *UNESCO UIS Global Education Glossary,* https://uis.unesco.org/en/ glossary-term/information-and-communication-technologies-ic

2 Phillippa Biggs (editor), "Fast-Forward Progress: Leveraging Tech to Achieve the Global Goals," *International Telecommunication Union,* 122, https://www.itu.int/en/sustainable-world/Documents/Fast-forward_ progress_report_414709%20FINAL.pdf.

normative challenge to the prevailing voluntary and non-binding cyber governance model promoted within existing UN processes. Through an analysis of Pakistan's interventions in various UN forums including the WSIS, the UN General Assembly, the Group of Governmental Experts (GGE), and the Open-Ended Working Group (OEWG), this study explores how Pakistan's stance aligns with the broader interests of the Global South. By employing a theoretical framework that combines constructivism with a Global South perspective, this study seeks to understand how Pakistan, as a developing state, shapes its position on ICT governance and the need for a legally binding cybersecurity framework. The study is qualitative in nature, drawing on primary and secondary sources to analyze Pakistan's advocacy for a treaty-like international cybersecurity regime, its implications for global cyber governance and potential impact on the future of international cyber law.

The central questions in this study are:

1. How does Pakistan's position on ICT governance reflect the broader concerns of the Global South?
2. How can Pakistan's position inform the broader debate on the regulation of cyberspace?

In addressing these questions, the paper also explores the significance of a legally binding framework for international cyber governance and its potential to create a more secure and equitable cyberspace for all nations.

The significance of this study lies in its examination of Pakistan's call for a legally binding treaty on ICT governance, which highlights the challenges of ensuring both security and sovereignty in cyberspace. Given the increasing militarization and weaponization of ICTs, Pakistan's stance provides valuable insight into the demands of the Global South for a more equitable and inclusive cyber governance framework. The paper argues that Pakistan's position reflects broader Global South concerns regarding sovereignty, equity, and the need for a legally binding framework.

Cyberspace and ICTs

Cyberspace and ICTs are two different yet closely related concepts. Cyberspace is the global domain within the information environment consisting of an interdependent network of information systems infrastructure, including the internet, telecommunications networks, computer systems, and embedded processors and controllers.[3] Cyberspace operates through the function of ICTs. According to the International Telecommunication Union (ITU), 5.5 billion people, about 68 percent of

[3] National Institute of Standards and Technology, "cyberspace," *NIST Computer Security Resource Center Glossary*, https://csrc.nist.gov/glossary/term/cyberspace. accessed on 12 November 2025

humanity, were online or connected with cyberspace in 2024.[4] The omnipresence of cyberspace poses opportunities as well as threats.

Weaponization of ICTs

The inherent dual-use nature of ICTs makes them susceptible to weaponization. Weaponization of cyberspace refers to the deliberate use of digital networks, data, and information systems as instruments of conflict to achieve strategic, military, or political objectives. These include espionage, critical infrastructure disruption, information warfare, and employment of destructive malware or cyber weapons. With exponential growth in computing power and the rise of artificial intelligence (AI) in the past few years, the involvement of ICTs has increased manifold both as civilian conveniences as well as critical components of warfare. Modern armies increasingly rely on integrated data links, satellite communication, unmanned systems, and cyber weapons as vital components of their command, control, communications, computers, intelligence, information surveillance, and reconnaissance (C4I2SR) operations.[5]

The growing interdependence between ICTs and military operations has become a global concern, as ICTs are being increasingly employed by states for offensive purposes as a tool of hybrid warfare. The increasing weaponization of ICTs has prompted a global debate on regulating ICTs to make cyberspace safer.[6]

Owing to rapid technological advancements in ICTs and their implications for national security, the subject has gained increasing scholarly and policy relevance. However, Pakistan's position on the regulation of these technologies, particularly within multilateral forums, remains relatively underexplored in existing literature. This paper seeks to address this gap by examining Pakistan's contributions to ongoing international debates on ICT governance. This paper aims to bridge this research gap by examining Pakistan's advocacy for a treaty-like international cybersecurity regime under the auspices of the UN. While Pakistan has engaged in other multilateral and regional forums, including the Shanghai Cooperation Organisation (SCO)[7] and International

---

4 ITU-D Statistics, *International Telecommunication Union*, https://www.itu.int/en/ ITU-D/Statistics/Pages/stat/default.aspx. accessed on 18 November 2025

5 Evan Beebe, "C4ISR & JADC2: Navigating the Next Frontier in Military Command and Control," *IDGA C4ISR & Command-and-Control,* August 9, 2024, https://www.idga.org/command-and-control/articles/c4isr-jadc2-the-next-frontier-in-military-command-and-control.

6 YIRIS/YIRA, "The Weaponization of Data: International Legal Responses to Digital Espionage and State-Sponsored Cyber Warfare," *YIRIS Column*, May 15 2025, https://yris.yira.org/column/the-weaponization-of-data-international-legal-responses-to-digital-espionage-and-state-sponsored-cyber-warfare/.

Telecommunication Union (ITU),[8] its most detailed and consistent articulation of positions on international cyber governance has taken place within UN processes, which remain the primary focus of this study. This study analyzes Pakistan's advocacy under the theoretical framework that combines constructivism with a Global South perspective. This approach highlights how developing states shape their perception and advocacy on technology governance. The study is qualitative in nature and relies on primary and secondary data sources for analysis.

Theoretical Framework

The Global South constructivist lens offers a useful framework for understanding how states such as Pakistan articulate their positions on ICT governance in terms of norms, identity, and equity. Rooted in constructivist insights that international behavior is shaped by shared ideas and social interactions, this approach highlights how developing states seek to reshape dominant narratives in global governance. Scholars such as Amitav Acharya,[9] Arlene Tickner, and David Blaney[10] emphasize the need to incorporate non-Western experiences and perspectives, challenging the historical dominance of Western-centric international relations theory. In the context of cyberspace, this perspective is reflected in calls for more inclusive, rules-based, and development-oriented governance frameworks.

André Barrinha and Arindrajit Basu discuss a concurrent "rise of the Global South" in world politics as cyber diplomacy matures. They argue that countries outside the "Western core" now contest cyberspace governance previously dominated by the US-led liberal order. In this view, cyberspace is no longer an uncontested global common but a domain where emerging powers exert influence.[11] At the same time, the persistence of disagreements over a legally binding cybersecurity framework cannot be explained by normative perspectives alone. Competing interests among major powers, asymmetries in technological capabilities, and divergent preferences over governance models contribute

---

8 Pakistan Ranks Among Top Countries in Global Cybersecurity," *Islamabad Post*, September 14, 2024, https://islamabadpost.com.pk/pakistan-ranks-among-top-countries-in-global-cybersecurity/.

9 Amitav Acharya, "Global International Relations (IR) and Regional Worlds: A New Agenda for International Studies." *International Studies Quarterly* 58, no. 4 (2014): 647–659. https://doi.org/10.1111/isqu.12171.

10 Tickner, Arlene B., and David L. Blaney, eds. *Thinking International Relations Differently: Worlding Beyond the West*. (London: Routledge, 2012), 255.

11 André Barrinha and Arindrajit Basu, "Cyber Diplomacy and the Rise of the 'Global South,'" *E-International Relations*, June 10, 2025, https://www.e-ir.info/2025/06/10/cyber-diplomacy-and-the-rise-of-the-global-south/.

to ongoing contestation in cyber diplomacy.[12] As cyberspace governance evolves, states outside the Western core increasingly challenge existing norms and institutional arrangements, yet these efforts often encounter resistance within UN-led processes. In this regard, Pakistan's advocacy reflects a normative alignment with broader Global South concerns that continues to shape the prospects for consensus on binding international regulation.

Multilateral Initiatives for Cyber Governance

International cyber law is a rapidly evolving field that seeks to regulate state and non-state behavior in cyberspace. One of the earliest treaties is the Budapest Convention on Cybercrime that was adopted by the Council of Europe in 2001. The Convention was the first legally binding international instrument on cybercrime, designed to harmonize national laws, enhance investigative techniques, and foster international cooperation. The Convention covers nine core offenses. These include: (i) Illegal Access (Hacking); (ii) Illegal Interception; (iii) Data Interference; (iv) System Interference; (v) Misuse of Devices; (vi) Computer-related Forgery; (vii) Computer-related Fraud; (viii) Offenses Related to Child Pornography; and (ix) Infringement of Copyright and Related Rights.[13] The Convention does not cover the broader category of cyber-enabled crimes, which are traditional crimes facilitated or increased in scale by the use of ICTs but do not constitute the core computer offenses. This limitation has been widely noted as a gap.[14] Pakistan has consistently opposed joining the Budapest Convention on Cybercrime, arguing that it is a highly intrusive instrument that would compromise national data sovereignty. According to the Ministry of Foreign Affairs, the Convention grants external jurisdiction significant authority over data access and transfer, raising concerns about the protection of domestic information systems. Islamabad also highlights that many non-European states, including China, Russia, Indonesia, Malaysia, and Singapore, share the view that the Budapest Convention is essentially a regional initiative of the European

---

12 Jill Stoddard, interview with Jim Lewis, "Cybercrime, Global Policy, and the New UN Treaty," *The Global Observatory*, 12 March 2025, https://theglobalobservatory.org/2025/03/cybercrime-global-policy-and-the-uns-new-treaty-interview-with-jim-lewis/

13 Council of Europe, "*Convention on Cybercrime", European Treaty Series No. 185,* Budapest, 23 November 2001, accessed September 23, 2025, https://rm.coe.int/1680081561.

14 Digital Watch, "Comparative Analysis: The Budapest Convention vs. the UN Convention against Cybercrime," accessed September 23, 2025, https://dig.watch/updates/comparative-analysis-the-budapest-convention-vs-the-un-convention-against-cybercrime.

Union rather than a universally negotiated treaty.[15] The Global South Constructivist lens shapes Pakistan's perspective that this Eurocentric and externally imposed arrangement undermines its legitimacy as a global framework, particularly when it comes to sensitive issues of jurisdiction and cross-border data exchange. Consequently, Pakistan has favored UN-led negotiations for an inclusive international convention on cybercrime that respects the sovereignty and legal traditions of all states.

While these concerns reflect broader Global South anxieties regarding unequal control over cross-border data flows and exclusion from norm-setting processes, they also point to an inherent tension between sovereignty and the operational requirements of international cybercrime cooperation.

An analysis by the Stimson Center (2025) highlights Pakistan's principled and measured approach to international cyber norms. The report notes that Pakistan has "refrained from acceding to the Budapest Convention… citing concerns over external jurisdiction and data sovereignty," thereby aligning with a broader group of states that seek to safeguard national prerogatives in cyberspace. The analysis underscores Pakistan's consistent view that any legal instruments on state conduct in the cyber domain must be inclusive, equitable, and respectful of sovereignty. This position reinforces Islamabad's preference for UN-led multilateral processes, which provide a universal and consensus-driven platform, over regional or externally driven frameworks that may not reflect the interests of all states equally.[16]

Another notable instrument is the Tallinn Manual (2013; expanded in 2017), a non-binding academic study led by the NATO Cooperative Cyber Defense Centre of Excellence that interprets how existing international law, particularly jus ad bellum and international humanitarian law (IHL), applies to cyber operations.[17] Pakistan recognizes the value of initiatives such as the Tallinn Manual and the Cyber Law Toolkit, describing them as academic, non-binding studies that examine the applicability of international law and IHL to cyberspace. Islamabad acknowledges that the Tallinn Manual provides important guidance, particularly in clarifying how traditional legal principles may extend to the digital domain. However, Pakistan emphasizes that despite its utility, the Manual does not resolve several key legal uncertainties. In its interventions, Pakistan has highlighted that fundamental questions remain

---

15 "Why Pakistan Is Not Joining Global Forum on Cybercrime," *Dawn*, 1 February 2020, https://www.dawn.com/news/1531734.

16 Gulraiz Iqbal, "How Does International Law Byte into Pakistan's Cyber Governance?" *Stimson Center,* 2025, https://www.stimson.org/2025/how-does-international-law-byte-into-pakistans-cyber-governance

17 "Tallinn Manual", *The Nato Cooperative Cyber Defence Centre of Excellence Research,* accessed on 18 October 2025, https://ccdcoe.org/research/tallinn-manual/

unsettled, such as the definition of the threshold for an "armed conflict" in cyberspace, the status of actors engaged in cyber operations, and the challenge of attribution, given the anonymity and technical complexity inherent in cyber activities.[18] From Pakistan's perspective, these unresolved issues demonstrate the limitations of relying solely on non-binding academic studies and reinforce the need for a universally negotiated, legally binding framework under UN auspices.

Issue of ICTs at the UN

The UN first formally acknowledged the security implications of information and communications technologies (ICTs) in 1998, when the Russian Federation introduced a resolution (A/RES/53/70) in the General Assembly titled *Developments in the field of information and telecommunications in the context of international security*. The resolution reflected growing concern that state and non-state actors could exploit cyberspace to compromise national and international security. The resolution was adopted without a vote, marking the beginning of the UN's involvement in global cyber governance.[19] Thereafter, the General Assembly's First Committee which deals with disarmament treated ICTs security as an emerging domain of international peace and security.

The World Summit on the Information Society (WSIS)

The WSIS was endorsed by UN General Assembly Resolution 56/183 on 21 December 2001. The resolution recognized "the urgent need to harness the potential of knowledge and technology for promoting the goals of the UN Millennium Declaration" and called for a two-phase summit in Geneva (2003) and Tunis (2005) to forge a common vision and understanding of the emerging global information society. The Resolution tasked the ITU with leading preparations, in coordination with other UN bodies, through an open-ended intergovernmental preparatory committee, and emphasized broad stakeholder participation, including governments, civil society, the private sector, and UN agencies.[20]

---

18 United Nations Office for Disarmament Affairs, Open-Ended Working Group on security of and in the use of information and communications technologies 2021–2025, Open-Ended Working Group documents (UNODA), https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/UNODA.pdf

19 United Nations General Assembly, *Resolution 53/70*, A/RES/53/70, 4 January 1999, https://docs.un.org/en/A/RES/53/70

20 United Nations General Assembly, *Resolution 56/183 (World Summit on the Information Society)*, A/RES/56/183, 21 December 2001, https://www.itu.int/net/wsis/docs/background/resolutions/56_183_unga_2002.pdf

The WSIS program was built around the Geneva Plan of Action and the Tunis Agenda, which turned its vision into concrete Action Lines. They covered areas such as infrastructure, access to information, capacity building, e-governance, and security. The Action Lines set key priorities including expanding broadband networks, ensuring universal access for marginalized communities, improving digital literacy, developing inclusive policies for public information, and addressing security concerns such as resilience, privacy, and trust.[21] It also established the Internet Governance Forum (IGF) as a permanent platform for dialogue. Crucially, WSIS institutionalized the principle of multistakeholder governance of ICTs.[22] It laid foundational norms 'to build a people-centered, inclusive and development-oriented Information Society.' It was based on sovereign equality and stakeholder engagement, serving as a precursor to later UN processes on ICT security and governance.[23]

For countries in the Global South, WSIS emphasized that ICTs development is integral to advancing sustainable development while addressing broader challenges related to security, capacity building, and equitable access to technology. The G77 underscored that ICTs must be shaped by principles favoring an inclusive, people-centered, and development-oriented information society. The outcome of WSIS, particularly the Tunis Agenda and Geneva Declaration of Principles, provided foundational guidance for digital cooperation rooted in sovereign equality and multilateralism.[24] It paved the way for subsequent UN processes such as the establishment of the Group of Governmental Experts (GGE) and the Open-Ended Working Group (OEWG) on ICTs.

Pakistan viewed the WSIS as a crucial platform recognizing the transformative impact of ICTs on all aspects of human life and development. In the statement delivered by Prime Minister Mir Zafarullah Khan Jamali at the WSIS held in Geneva in 2003, Pakistan emphasized the

---

21 International Telecommunication Union, "*The Geneva Plan of Action,* adopted at the World Summit on the Information Society (WSIS)", (Geneva 2003), https://www.itu.int/net/wsis/docs/geneva/official/poa.html

22 Global Partners Digital, "Everything You Need to Know About the WSIS+20 Review," *GP-Digital* blog, 18 February 2025, https://www.gp-digital.org/everything-you-need-to-know-about-the-wsis20-review/

23 "United Nations Conference on Trade and Development", **UNCTAD/TCS/DTL/INF/2025/D2**, https://unctad.org/system/files/official-document/tcsdtlinf2025d2_en.pdf.

24 Group of 77 and China, "Statement on Behalf of the Group of 77 and China by the South African Minister of Telecommunications and Postal Services, H.E. Minister Siyabonga Cwele, at the UN General Assembly High-Level Meeting on the Overall Review of the Implementation of the Outcomes of the World Summit on the Information Society (New York, 15 December 2015)," G-77 (website), accessed September 23, 2025, https://www.g77.org/statement/getstatement.php?id=151215c.

need to bridge the vast digital divide that separated people within and across countries. The statement underscored the goal of creating an inclusive information society that provides equal opportunities for all, especially in developing countries, and called for international cooperation to develop ICT infrastructure, ensure information system security, and protect universal moral and spiritual values.[25] From a Global South constructivist perspective, WSIS represented an important moment where developing states sought to frame ICT governance not merely as a technical issue, but as a question of equity, sovereign equality, and inclusive participation. Pakistan's support for these principles reflects its broader normative preference for multilateral and development-oriented cyber governance.

While these UN-led processes established important normative foundations and institutional platforms for ICT governance, they have not resulted in a legally binding international framework. This outcome reflects persistent divergences among states over the nature of cyberspace governance. Major powers differ on issues such as sovereignty, the applicability of international law, and the balance between state control and the open, multistakeholder model promoted through processes such as WSIS. These disagreements have led to a preference for voluntary norms and confidence-building measures rather than binding commitments. Additionally, asymmetries in technological capabilities and institutional capacity have further complicated consensus, as developing states seek greater equity and safeguards against external control, while technologically advanced states prioritize flexibility and operational freedom.

In this context, Pakistan's position can be understood as a response to both structural and normative concerns within the existing framework. The absence of a binding instrument reinforces Pakistan's emphasis on a treaty-based approach that ensures sovereign equality, legal clarity, and capacity-building for developing states. Thus, Pakistan's advocacy is not merely rhetorical but emerges from the limitations of current multilateral processes, which, despite their inclusivity, have struggled to reconcile competing interests and produce enforceable outcomes.

---

[25] International Telecommunication Union, "Statement of the Pakistan Delegation to the World Summit on the Information Society (Geneva Phase, December 10–12, 2003)," accessed September 23, 2025, https://www.itu.int/net/wsis/geneva/coverage/statements/pakistan/pk.pdf.

Group of Governmental Experts (GGE)

In 2004, the UN General Assembly established the first GGE to explore threats in cyberspace and consider cooperative measures.[26] Although the 2004-2005 GGE failed to produce a consensus report, subsequent GGEs made significant progress. The 2009-2010 GGE (A/65/201) produced the first consensus report acknowledging that international law and the UN Charter apply to cyberspace.[27] This was a turning point, setting the legal and normative foundation for future work.

The 2012-2013 GGE further solidified this position in its report (A/68/98), which explicitly affirmed that international law applies to the behavior of states in cyberspace.[28] The 2014-2015 GGE (A/70/174) advanced the discussion by articulating eleven voluntary norms of responsible state behavior in cyberspace. These include: (i) Cooperation for international stability and security; (ii) Contextual assessment of ICT incidents; (iii) Prohibition of wrongful acts from national territory; (iv) International cooperation against criminal and terrorist use of ICTs; (v) Respect for human rights and privacy in cyberspace; (vi) Prohibition of attacks on critical infrastructure; (vii) Protection of national critical infrastructure; (viii) Assistance to states facing malicious ICT acts; (ix) Integrity and security of ICT supply chains; (x) Responsible disclosure of ICT vulnerabilities; and (xi) Protection and non-misuse of emergency response teams.[29] These norms formed a "voluntary framework" and were endorsed by UN General Assembly Resolution 70/237.[30]

Progress on the issue of ICTs stalled in the 2016-2017 GGE due to disagreement over the interpretation of international law and proposals

---

26 United Nations General Assembly, "*Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security,"* A/59/116, 2 July 2004, https://docs.un.org/en/A/59/116.

27 United Nations General Assembly, "*Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security"* A/65/201, 30 July 2010, https://docs.un.org/ en/A/65/201.

28 United Nations General Assembly, "*Developments in the Field of Information and Telecommunications in the Context of International Security," UN Doc A/68/98* (24 June 2013), https://docs.un.org/en/A/68/98.

29 United Nations, "*Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security" UN Doc. A/70/174* (22 July 2015), https://docs.un.org/en/A/70/174.

30 United Nations General Assembly, "Developments in the Field of Information and Telecommunications in the Context of International Security" *UN Doc. A/RES/70/237,* 30 December 2015, https://docs.un.org/en/A/res/70/237.

by Russia and China for a legally binding code of conduct.[31] Western states, particularly the US and its allies, opposed the idea of a binding treaty, preferring voluntary norms and Confidence Building Measures (CBMs) in the field of regulating ICTs.[32] Six GGEs have been convened so far.

The GGE's emphasis on voluntary norms reflects the preference of major powers for strategic flexibility, whereas developing states such as Pakistan view the absence of binding obligations as reinforcing structural inequalities in cyberspace governance. This divergence highlights how Global South states contest norm-making processes dominated by technologically advanced powers.

Open-Ended Working Group (OEWG) on ICTs

In response to growing demands for inclusive dialogue, the UN General Assembly adopted Resolution 73/27 in 2018, which established the first **OEWG** on ICTs. Unlike the GGE, which was composed of 25 experts, the OEWG was open to all member states, allowing for broader participation, especially from developing countries.[33]

The **first OEWG (2019-2021)** conducted inclusive consultations and released a consensus report in March 2021 (A/75/816). The report reaffirmed the applicability of international law, endorsed previously agreed norms, and emphasized CBMs and capacity-building. Notably, it recommended the creation of Points of Contact (PoC) directories and increased technical assistance to developing countries.[34] Simultaneously, the **sixth GGE (2019-2021)** released its consensus report (A/76/135), echoing the OEWG findings and stressing the importance of continued dialogue.[35] The convergence of GGE and OEWG outcomes reflected a

---

31 Elaine Korzak, "Cyber Norm Emergence at the United Nations-An Analysis of the UN's Activities Regarding Cyber-security," *Stanford University Center for International Security and Cooperation discussion paper (2016),* https://www.belfercenter.org/publication/cyber-norm-emergence-united-nations-analysis-uns-activities-regarding-cyber-security.

32 Elaine Korzak, *Cyber Norm Emergence at the United Nations*, 2016

33 United Nations General Assembly, "*Developments in the Field of Information and Telecommunications in the Context of International Security," UN Doc. A/RES/73/27*, 5 December 2018, https://documents-dds-ny.un.org/doc/UNDOC/GEN/N18/431/74/PDF/N1843174.pdf.

34 United Nations General Assembly, "*Developments in the Field of Information and Telecommunications in the Context of International Security" UN Doc. A/75/816,* 18 March 2021, https://disarmament.unoda.org/en/our-work/emerging-challenges/developments-field-information-and-telecommunications-context.

35 United Nations General Assembly, "*Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*" *UN Doc. A/76/135*, 14 July 2021, https://docs.un.org/en/A/76/135.

growing consensus on the normative framework for state behavior in cyberspace, despite continuing disagreements over legal interpretations and enforcement mechanisms.

The UN General Assembly, through Resolution 75/240, created a **second OEWG (2021-2025)** to build on previous progress.[36] Over multiple sessions, member states engaged in discussions on threats, legal applicability, CBMs, and capacity development. The second OEWG also integrated perspectives from regional organizations, civil society, and the private sector. In its Final Report adopted in July 2025, the second OEWG officially reaffirmed the eleven voluntary, non-binding norms of responsible state behavior in cyberspace, originally agreed in the 2015 GGE report and endorsed unanimously under UNGA Resolution 70/237. It also recommended the establishment of a "**Permanent UN Cyber Programme,**" also referred to as the "Global Mechanism," to institutionalize discussions beyond 2025.[37] The OEWG's inclusive structure aligned more closely with Global South demands for broader participation in international cyber governance.

All the GGEs and OEWGs have focused on a consistent set of themes that have recurred in each resolution and report.[38] They include:

i. **Threats:** States have catalogued cyber espionage, cybercrime, attacks on infrastructure and disinformation campaigns as risks to international peace.
ii. **Application of international law:** From the outset, experts have discussed how the UN Charter, law of state responsibility, and law of armed conflict govern cyber operations.
iii. **Norms of responsible state behavior:** All of the GGEs and OWEGs have proposed non-binding norms, such as not to target critical infrastructure, not to use ICTs to impede elections, and to provide assistance to states.
iv. **CBMs:** Member States have suggested mechanisms like contact points, incident notification, and expert exchanges to increase transparency.
v. **Capacity-building and development:** All processes stress technical assistance and training for less-developed states,

---

36 United Nations General Assembly, "Developments in the Field of Information and Telecommunications in the Context of International Security" *UN Doc. A/RES/75/240,* 31 December 2020, https://docs.un.org/en/A/RES/75/240.

37 United Nations General Assembly, "*Final Report of the Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025," UN Doc. A/AC.292/2025/CRP.1,* 11 July 2025, https://undocs.org/A/AC.292/2025/CRP.1.

38 United Nations General Assembly, "Developments in the Field of Information and Telecommunications in the Context of International Security," *UN Doc. A/75/816,* 18 March 2021, https://docs.un.org/en/A/75/816

recognizing that equitable cybersecurity capacity is essential for international stability.

In parallel, the UN General Assembly has adopted annual resolutions tracking the discussions in GGEs and OEWGs. For example, the Resolutions A/RES/76/19 (2021)[39] and A/RES/77/36–37 (2022)[40] reflected OEWG consensus. In 2022, the General Assembly for the first time adopted a separate Programme of Action (PoA) on responsible state behavior in ICTs (A/RES/77/37). The PoA called for regular, inclusive dialogues and requested the Secretary-General's report[41] on implementation, which was submitted as A/78/76 in 2023.[42] In December 2023, the GA passed the resolution A/RES/78/237 on "Developments in ICT", which reaffirmed earlier commitments and invited further work on the issue.[43] These resolutions signal an agreement to entrench the GGE/OEWG consensus into more enduring UN processes.

The UN has advanced its engagement with ICTs through the General Assembly's Third Committee and the UN Office on Drugs and Crime (UNODC). Pursuant to General Assembly resolution 74/247 (2019), an Ad Hoc Committee was established to elaborate a comprehensive international convention on countering the use of ICTs for criminal purposes. This process culminated in the General Assembly's adoption of the UN Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes on 24 December 2024, under resolution 79/243. The Convention opened for signature in Hanoi, Viet Nam on 25 - 26 October 2025 and will remain open at the UN Headquarters in New York until 31 December 2026. At the opening ceremony, 65 nations signed the treaty. The instrument seeks to enhance international cooperation, criminalize specific cyber and ICT-related

---

39 United Nations General Assembly, "Developments in the Field of Information and Telecommunications in the Context of International Security," *UN Doc. A/RES/76/19,* 8 December 2021, https://docs.un.org/en/A/RES/76/19

40 United Nations General Assembly, "Developments in the Field of Information and Telecommunications in the Context of International Security," *UN Doc. A/RES/77/36,* 12 December 2022, https://docs.un.org/en/A/RES/77/36

41 United Nations Institute for Disarmament Research, "Towards a Regular Institutional Dialogue on International ICT Security: Review of Current Proposals and Considerations for Effective Dialogue" (Geneva: UNIDIR, 29 November 2024), https://unidir.org/wp-content/uploads/2024/11/UNIDIR_Towards_Regular_Institutional_Dialogue_web.pdf

42 United Nations General Assembly, "Programme of Action to Advance Responsible State Behaviour in the Use of Information and Communications Technologies in the Context of International Security" *UN Doc. A/RES/77/37* (12 December 2022), https://docs.un.org/en/A/RES/77/37

43 United Nations, General Assembly, "Developments in the Field of Information and Telecommunications in the Context of International Security" *A/RES/78/237* (adopted 2023), https://docs.un.org/en/A/RES/78/237

offences, and facilitate cross-border access to electronic evidence while upholding human rights and fundamental freedoms.[44]

The UN Secretary-General has advanced broader initiatives on ICT governance, notably the High-Level Panel on Digital Cooperation (2018-2019), which in its report *The Age of Digital Interdependence* emphasized that digital technologies underpin all aspects of modern life and therefore require strengthened international cooperation grounded in inclusivity, transparency, and human rights.[45] Building on these recommendations, the Secretary-General's *Roadmap for Digital Cooperation* (2020) outlined action areas such as digital connectivity, human rights online, global digital commons, and capacity-building, thereby linking cybersecurity to sustainable development and digital trust.[46] These efforts directly inform the proposed Global Digital Compact, which was adopted as an annex to the "Pact for the Future" at the United Nations Summit of the Future on 22 September 2024, during the 79th session of the General Assembly in New York. The Compact commits member states to upholding international law and human rights online, promoting connectivity and data governance, countering fragmentation, enhancing AI governance through initiatives such as an Independent International Scientific Panel on AI and global dialogue, and accelerating progress towards the SDGs by 2030.[47]

The UN Security Council addresses ICTs issues related to peace and security in discussions on terrorism and the protection of critical infrastructure, but it has not yet adopted a standalone cyber resolution.[48] This also reflects a significant gap in advancing concrete measures for the governance of ICTs.

Overall, the UN ICTs security regime has converged on several key points. All member states agree that cybersecurity intersects with peace and security, and that UN Charter principles apply to the cyber domain. All major powers have endorsed a set of voluntary norms for peacetime

---

44 "Sixty-Five Nations Sign First UN Treaty to Fight Cybercrime, in Milestone for Digital Cooperation," *UN News*, October 25, 2025, https://news.un.org/en/story/2025/10/1166182.

45 United Nations Secretary-General's High-Level Panel on Digital Cooperation, "*The Age of Digital Interdependence: Report of the High-Level Panel on Digital Cooperation",* June 2019, https://www.un.org/en/pdfs/DigitalCooperation-report-for%20web.pdf.

46 United Nations Secretary-General, "*Roadmap for Digital Cooperation*," *UN General Assembly, A/74/821*, 29 May 2020, https://www.un.org/en/content/digital-cooperation-roadmap/.

47 "Global Digital Compact-Office for Digital and Emerging Technologies," *United Nations,* https://www.un.org/en/summit-of-the-future/global-digital-compact.

48 "Information and Communications Technologies", *United Nations Security Council, Counter-Terrorism Committee (CTC),* https://www.un.org/securitycouncil/ctc/content/information-and-communications-technologies.

conduct, and the latest GGE and OEWG reports capture a shared "normative framework" for responsible state behavior. Agreements on transparency measures such as PoC, threat information exchange and assisting developing countries in improving cyber resilience are also relatively uncontroversial.

Despite these institutional advancements, major disagreements remain. Russia and China continue to advocate for a legally binding treaty and a greater role for state sovereignty in cyberspace.[49] Western states emphasize the voluntary nature of norms, multi-stakeholder involvement, and the primacy of human rights online. Contentious issues also include defining thresholds for cyberattacks, verifying compliance, and the role of non-state actors.[50] Debates also persist over how much responsibility wealthy states should bear for assisting poorer states with cybersecurity and how to measure compliance with the norms.

Despite these institutional developments, the UN has not produced a comprehensive, legally binding ICT framework. There remains persistent norm contestation among states over cyberspace governance. While some favor a sovereignty-based, treaty-driven approach, others prioritize voluntary norms and multistakeholder models. These competing preferences, along with asymmetries in capabilities and interests, have limited consensus to non-binding measures. As a result, UN processes exhibit a degree of institutional paralysis, where agreement exists on principles but not on enforceable rules. This deadlock explains both the absence of a binding treaty and the continued push by states such as Pakistan for a more formalized legal framework.

Pakistan's Position

Pakistan considers cyberspace as the "common heritage of mankind" and an essential domain for socio-economic development, governance, and the delivery of critical public services. At the same time, Islamabad expresses growing alarm over the militarization of ICTs, the weaponization of the cyber domain, and the malicious exploitation of digital technologies by both state and non-state actors. It warns that such trends threaten international peace and security, heighten mistrust among states, and risk turning cyberspace into a theatre of conflict.[51] Pakistan

---

49 Russian Federation, "Proposal for an International Code of Conduct for Information Security," letter dated 9 January 2015, *submitted to the UN Secretary-General (A/69/723),* https://docs.un.org/en/A/69/723

50 James A. Lewis, "Multilateral Agreements and Cybersecurity Norms," *Center for Strategic and International Studies (CSIS),* 2022, https://www.csis.org/analysis/multilateral-agreements-and-cybersecurity-norms

51 United Nations Office for Disarmament Affairs (UNODA), *Open-Ended Working Group on Information and Communication Technologies (2021),* https://docs-

links cyber threats to national and regional security challenges, especially terrorism. It argues that terrorist groups and extremists exploit the Internet to plan attacks, recruit militants, and spread propaganda.

Pakistan participated in the 2014-2015 GGE[52], the 2019-2021 OEWG, and remained an active member of the 2021-2025 UN OEWG On the Security of and in the Use of ICTs." It engaged in deliberations across all six agenda items of the OEWG: (i) examining existing and potential threats in the information security domain; (ii) clarifying the application of international law in cyberspace; (iii) developing norms, rules, and principles of responsible state behavior; (iv) advancing CBMs; (v) promoting capacity-building; and (vi) maintaining regular institutional dialogue. Pakistan presented a Working Paper[53] and made interventions in Substantive Sessions of the OEWG,[54] and provided written inputs on General Assembly initiatives, including its views on Resolution 78/237.[55] A formal Position Paper on the Application of International Law in Cyberspace was also submitted by Islamabad in March 2023.[56]

---

library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/UNODA.pdf

52 United Nations, "*Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," UN Doc. A/70/174*, 22 July 2015, https://docs.un.org/en/A/70/174

53 Pakistan Mission to the United Nations, "*Working Paper by Pakistan to the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security"* (2023), https://ceipfiles.s3.amazonaws.com/pdf/CyberNorms/UNGGE/Working+Paper+by+Pakistan+to+the+Open-Ended+Working+Group+on+Developments+in+the+Field+of+Information+and+Telecommunications+in+the+Context+of+International+Security+.pdf

54 Pakistan Mission to the United Nations, "*Statement Delivered by Pakistan at the Fourth Substantive Session of the Open-Ended Working Group on Information and Communication Technologies (2021–2025)",* Fourth substantive session, UN Office for Disarmament Affairs (UNODA), https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_%282021%29/Satements_Delivered_by_Pakistan-_4th_substantive_session.pdf

55 Pakistan Mission to the United Nations (via UNODA), *"Pakistan's Views on the Resolution 78/237: "Developments in the Field of Information and Communication Technologies in the Context of International Security" First Committee, 79th UN General Assembly session,* 2024, https://docs-library.unoda.org/General_ Assembly_First_Committee_-Seventy-Ninth_session_%282024%29/78-237-Pakistan-EN.pdf

56 United Nations Office for Disarmament Affairs (UNODA), *"Open-Ended Working Group on Information and Communication Technologies (2021)" established by General Assembly resolution 75/240,* 31 December 2020, https://docs-library.unoda.org/Open-

Over time, Pakistan's position on security of ICTs has remained consistent. As a developing country, Pakistan aligns with many states of the Global South in advocating for a legally binding UN framework on "conduct of states" in cyberspace.[57] From a constructivist perspective, Pakistan's diplomacy on the issue reflects an identity as a steward of the "common heritage of mankind," framing cyberspace as a shared global common that demands rules-based governance. Central to Pakistan's advocacy is the categorical prohibition of offensive cyber capabilities, particularly those capable of degrading, disrupting, or destroying critical civilian infrastructure. Pakistan argues that such capabilities not only present unacceptable risks of escalation and converting cyberspace into an arena of conflict but also undermine the foundational principles of the UN Charter. It has therefore called for an outright ban on the development of offensive cyber weapons.[58]

While supporting CBMs such as a UN PoC directory as useful instruments for trust-building, Pakistan emphasizes that these should complement, rather than replace, binding legal obligations. Consequently, it has participated constructively in CBM discussions while reserving its position on certain institutional proposals, pending assurances that any new mechanism will safeguard inclusivity, consensus-based decision-making, and a credible pathway toward formal, legally binding commitments.[59]

Pakistan's discourse on ICT security centers on three main pillars**:** (i) protecting state sovereignty; (ii) establishing binding international arrangements; and (iii) capacity-building in developing countries. Islamabad stresses that states must retain jurisdictional authority over ICT infrastructure in their territory and that cyber operations that interfere in domestic affairs, including state-sponsored disinformation, constitute violations of the UN Charter.[60] For Islamabad, the integrity of its digital

---

Ended_Working_Group_on_Information_and_Communication_Technologies_-_%282021%29/UNODA.pdf

57 *"Cybercrime, Global Policy, and the New UN Treaty: Interview with Jim Lewis," The Global Observatory,* March 12, 2025, https://theglobalobservatory.org/2025/03/cybercrime-global-policy-and-the-uns-new-treaty-interview-with-jim-lewis/

58 Pakistan Mission to the UN, "*Statement Delivered by Pakistan at the Fifth Substantive Session of the Open-Ended Working Group on Information and Communication Technologies (ICTs 2021–2025),"* March 2023, https://reachingcriticalwill.org/images/documents/Disarmament-fora/other/icts/oewg-II/documents/Pakistan_2023.pdf

59 Pakistan Mission to the UN, "*Statement at the Fifth OEWG Session on ICTs*," March 2023.

60 **Pakistan Mission to the UN, "***Views on Res. 78/237***," First Committee (79th UNGA session, 2024),** https://docs-library.unoda.org/General_Assembly_

infrastructure is as inviolable as its territorial borders. The National Cyber Security Policy 2021 of Pakistan clearly states that it "will regard a cyber-attack on Pakistan's Critical Infrastructure (CI) and Critical Information Infrastructure (CII) as an act of aggression against national sovereignty and will defend itself with appropriate response measures." This reflects a stance equating cyber-attacks to violation of its sovereignty, akin to physical attacks on its territorial borders.[61] This underscores Pakistan's viewpoint that international law must explicitly recognize states' sovereign rights over ICTs within their territory.

Pakistan anchors its position on the primacy of international law (UN Charter) and International IHL in cyberspace, insisting that core principles such as non-use of force, sovereign equality, non-intervention, and peaceful settlement are also applicable online. Pakistan recognizes that the distinctive attributes of cyberspace and the transnational nature of cyber technologies complicate the application of international law. It therefore advocates structured deliberations among UN member states to clarify how principles such as sovereignty, self-defense, non-use of force, peaceful dispute settlement, and attribution should be operationalized in the cyber domain.[62]

As militaries increasingly rely on the same Internet backbone and transmission lines that support civilian CI, attempts to target an adversary's military networks in armed conflicts risk causing severe civilian harm, including both human casualties and financial losses. This interconnectedness of systems, combined with the technical complexity of cyber operations, makes it especially difficult to apply the three fundamental principles of IHL, including distinction, proportionality, and precaution, in the cyber domain. In cyber conflicts, civilian populations and CI must remain protected, and the use of cyber weapons that can cause indiscriminate damage is prohibited under IHL. Pakistan therefore emphasizes that the Geneva Conventions and their Additional Protocols (APs) continue to apply in cyberspace, especially the rule of distinction requiring parties to differentiate between civilians and combatants, and between civilian and military targets. Pakistan recognizes that the application of IHL is not possible without the resolution of issues of

---

First_Committee_-Seventy-Ninth_session_%282024%29/78-237-Pakistan-EN.pdf

61 Ministry of Information Technology & Telecommunication (Pakistan), *National Cyber Security Policy 2021*, approved by the Federal Cabinet in July 2021, https://moitt.gov.pk/SiteImage/Misc/files/National%20Cyber%20Security%20Policy%202021%20Final.pdf

62 United Nations Office for Disarmament Affairs (UNODA), "*Open-Ended Working Group on Information and Communication Technologies (2021)"* established by General Assembly resolution 75/240, 31 December 2020, https://docs-library.unoda.org/Open- Ended_Working_Group_on_ Information_and_ Communication_Technologies_-_(2021)/UNODA.pdf

attribution. In this regard, it proposes attribution mechanisms with the support and coordination of member states. Islamabad also presses for agreed legal definitions of cyber-attack, cyber-terrorism, CI and CII for predictable legal applications and state responsibility.[63]

Pakistan is in favor of development of global regulatory frameworks on data security and the cross-border exchange of data. In particular, it advocates the establishment of an international mechanism to ensure the protection of data integral to CI and calls for the criminalization of acts involving the theft, deletion, destruction, or manipulation of such data. Pakistan underscores that capacity building for all states on an equal footing is indispensable for a secure and stable cyberspace and for the effective implementation of international law in the cyber domain. From a Global South perspective, Islamabad stresses that existing digital divide and structural inequities must be addressed through fair, equitable, and non-discriminatory access to cyber technologies and products to ensure that developing states are not marginalized in global cyber governance.[64]

Islamabad argues that the current legal architecture contains gaps such as thresholds for the use of force, attribution rules, and IHL application. Therefore, it favors a legally binding instrument, such as a treaty or convention, rather than merely voluntary norms. Pakistan's call for a legally binding treaty reflects more than a security concern; it represents a normative challenge to the existing cyber order shaped largely by powerful states. Through a Global South constructivist lens, this advocacy seeks to redefine cyberspace governance around sovereignty, legal equality, and distributive justice rather than voluntary compliance alone.

Pakistan's Advocacy for a Legally Binding International Cybersecurity Framework

While Western states have generally prioritized non-binding norms, CBMs, and the reaffirmation that existing international law including the UN Charter governs state activity in cyberspace, Pakistan, alongside many Global South states, contends that voluntary guidelines alone are inadequate to deter the increasingly militarized and weaponized use of ICTs. Drawing on its OEWG submissions, Pakistan advances several arguments in support. First is enforceability. Pakistan states that legally binding obligations would create clear legal duties, enable the invocation of state responsibility, and furnish predictable dispute-settlement and remedial pathways when violations occur. On the other hand, non-binding

63 UNODA, Open-Ended Working Group on ICTs (2021).
64 UNODA, Open-Ended Working Group on ICTs (2021).

norms, by their nature, lack a compulsory enforcement mechanism and risk being disregarded in times of crisis.[65]

The second argument is comprehensiveness. According to Pakistan, a convention could close both practical and doctrinal gaps in the existing body of international law by specifying how thresholds such as "use of force" and "armed attack" apply in cyber operations. It could also clarify attribution standards and evidentiary procedures, while detailing how IHL principles of distinction, proportionality, and precaution should be operationalized in hostilities involving cyberspace.[66]

The third issue is equity and capacity. A multilateral treaty can and should embed obligations for technical assistance, technology access, and sustained capacity-building financing so that developing states are not left unable to comply with or benefit from new rules, thereby narrowing the digital divide that otherwise would leave less-resourced countries exposed and marginalized. In Pakistan's view, therefore, voluntary norms and CBMs remain useful confidence-building tools in peacetime but are insufficient substitutes for legally binding instruments capable of delivering clarity, accountability, and distributive justice in a geopolitically fraught cyber environment.[67]

Pakistan's official texts and oral statements at the UN identify concrete components it believes a legally binding framework should contain, including the recognition of cyber sovereignty and jurisdictional rights, whereby states have enforceable authority over ICTs and data located within their territory, and cyber intrusions impairing essential services are treated as violations of sovereignty.

---

65 Pakistan Mission to the United Nations, "*Working Paper by Pakistan to the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security"* (March 2023), https://ceipfiles.s3.amazonaws.com/pdf/CyberNorms/UNGGE/Working+Paper+by+Pakistan+to+the+Open-Ended+Working+Group+on+Developments+in+the+Field+of+Information+and+Telecommunications+in+the+Context+of+International+Security+.pdf

66 Usman Jadoon, "Remarks by APR Ambassador Usman Jadoon: Formulation of Position on the Application of International Law in Cyberspace – Pakistan's Experience" (July 11, 2024), *United Nations Institute for Disarmament Research,* July 11, 2024, https://pakun.org/uploads/07112024_01_8801ac2dd2.pdf

67 Pakistan Mission to the United Nations, *"Working Paper by Pakistan to the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security"* (March 2023), https://ceipfiles.s3.amazonaws.com/pdf/CyberNorms/UNGGE/Working+Paper+by+Pakistan+to+the+Open-Ended+Working+Group+on+Developments+in+the+Field+of+Information+and+Telecommunications+in+the+Context+of+International+Security+.pdf

While Pakistan's advocacy presents a coherent normative case for a binding framework, important analytical questions remain. Why have such proposals failed to gain universal acceptance, and under what conditions could they become viable? The persistence of divergent state preferences—particularly between sovereignty-driven and multistakeholder approaches—suggests that resistance is rooted not only in legal disagreement but also in strategic and technological asymmetries. At the same time, it remains unclear how a binding regime would address challenges of enforcement, attribution, and compliance in a contested cyber environment. These questions highlight the need to assess both the strengths and limitations of Pakistan's position within the broader dynamics of global cyber governance.

Pakistan's Framework Proposal

Overall, Pakistan seeks a comprehensive multilateral agreement addressing cybercrime, cyberterrorism, and cyber warfare under the umbrella of international law. Pakistan's model for a "legally binding cybersecurity framework" can be summarized as follows:

1. **National Sovereignty and Jurisdiction:** Pakistan insists that any framework recognize states' sovereign rights over ICTs infrastructure within their borders. In practice, this means each country could regulate content and data flows on its networks without external interference. Pakistan's position is that cyber-attacks on a state's networks violate sovereignty and thus breach international law. The framework should affirm that principle and hold attacking states accountable.
2. **Combating Cyberterrorism:** Islamabad argues that the framework must criminalize and facilitate the prosecution of cyber terrorism, extremism, and other malicious uses of ICTs. This includes mandating cooperation on law enforcement (e.g. evidence-sharing, extradition of hackers) and obliging states to prevent their territory from being used by terrorists online. A binding convention, Pakistan believes, should require all states to enact laws against such abuse and to assist each other under clear legal rules.
3. **International Law and Accountability:** Pakistan supports codifying these obligations into international law**.** Rather than relying on voluntary confidence-building, Pakistan advocates a treaty or UN convention. Under such a pact, there would be defined rules for example, outlawing attacks on critical infrastructure, and possibly a mechanism to review compliance. This would give countries legal standing to demand action or sanctions if another state violates its cyber commitments. Pakistan's UN statements

have similarly stressed the need for binding language, not just soft norms.

4. **Development Support:** Pakistan emphasizes that all countries, big or small, should have equal rights in governing cyberspace. It calls for capacity-building assistance so that developing states can meet the treaty's requirements. In practice, this may involve technology transfer, training, and financial assistance to enforce cybersecurity laws. Pakistan frames this as a fairness issue. Many developing countries fear being held to standards they lack the resources to implement. Thus, Islamabad insists that the international framework include provisions for mutual assistance and technology sharing.

Malicious Use of ICTs: Indian Misinformation and Propaganda Warfare Against Pakistan

Misinformation and propaganda remain potent tools of hybrid warfare. Throughout the years, Pakistan has been a victim of a malicious Indian disinformation campaign. In its 2019-20 report, a Brussels-based non-governmental organization (NGO), the EU DisinfoLab, uncovered a malicious Indian propaganda campaign against Pakistan. According to it, over ten NGOs, approximately 750 fabricated media outlets, and around 550 counterfeit websites, including some registered under the names of deceased individuals, were employed to disseminate disinformation against Pakistan. By weaponizing both technology and narrative, such campaign actions undermine international legal norms and destabilize South Asia's security environment. As a continuing victim of Indian cyber warfare, Pakistan has raised the issue on various multilateral forums, including the UN Security Council high-level debate on evolving threats in cyberspace.[68] Pakistan calls for addressing such non-kinetic attacks including state-sponsored disinformation and information operations and recognizes them as a violation of the principle of non-intervention and the UN Charter.

Conclusion

Pakistan's advocacy for a legally binding international cybersecurity framework reveals a deeper structural divide in global cyber governance between technologically advanced states that favor flexible voluntary norms and developing countries that seek enforceable legal protections rooted in sovereignty, equity, and multilateralism.

---

[68] "*Pakistan pushes for global protocol on cyberwarfare amid Indian disinformation allegations," The Express Tribune (APP),* June 21, 2024, https://tribune.com.pk/story/2472770/pakistan-pushes-for-global-protocol-on-cyberwarfare-amid-indian-disinformation-allegations

Despite the absence of a global treaty, Pakistan continues to encourage dialogue at the UN, urging sustained momentum toward a formal accord. Pakistan's position reflects broader Global South concerns regarding unequal participation in cyber norm-making, asymmetries in technological power, and the risks of governance models shaped primarily by major powers. Through its interventions at the UN, Pakistan consistently argues that cyberspace should be governed through universally negotiated legal obligations rather than voluntary commitments alone. This stance resonates with many developing countries, particularly across Africa and the Arab world, that support stronger international legal mechanisms against cyber threats. Pakistan has co-sponsored and supported initiatives calling for a global cybercrime convention, arguing that international law must evolve to address ICT-related challenges and violations of sovereignty.[69]

In its diplomatic efforts, Pakistan has been consistently advocating that cyberspace should be governed by law and should not be left to unilateral measures. Rooted in its domestic view that cyber defense is a key aspect of national security, Pakistan envisions a UN-led framework in which member states commit to securing ICT systems, refraining from malicious activities, sharing information, and assisting developing countries to bridge the digital divide. While a binding global instrument has yet to materialize, Pakistan's advocacy reflects and reinforces ongoing efforts to maintain the relevance of a rule-based approach to cyberspace governance within UN processes.

[69] Aftab Ahmad Khokher, *"Pakistan–United Nations Office on Drugs and Crime (UNODC): A Lasting Partnership,"* Special Guest Article, *Institute of Strategic Studies Islamabad (ISSI),* 18 August 2023, https:/