MANOHAR PARRIKAR INSTITUTE FOR DEFENCE STUDIES AND ANALYSES
मनोहर पर्रिकर रक्षा अध्ययन एवं विश्लेषण संस्थान

MP-IDSA
Issue Brief

UN Cyber OEWG Ends after Five-Year Run

Cherian Samuel

September 03, 2025

Summary

The United Nations Open-Ended Working Group (2021–2025) concluded in July 2025 with a consensus report recommending a permanent 'Global Mechanism' to institutionalise negotiations on responsible State behaviour in cyberspace.

The second and final United Nations Open-Ended Working Group (OEWG) on Security of and in the Use of Information and Communications Technologies (ICTs) 2021–2025 concluded its five-year mandate in July 2025 and submitted a report. This report, adopted after intense discussions among 193 states, has laid out the framework for future international engagement on cybersecurity.

Proposed Global Mechanism

Its main recommendation was establishing a permanent mechanism, the 'Global Mechanism on developments in the field of ICTs in the context of international security and advancing responsible State behaviour in the use of ICTs' to take on the mandate of negotiating a framework for responsible state behaviour in cyberspace. This mechanism is intended to institutionalise cybersecurity discussions within a permanent UN forum, moving beyond *ad hoc* processes like the UN Group of Governmental Experts (UNGGE) and OEWG.

The format under the proposed permanent mechanism is not too different from the OEWG process, with a plenary session to run for five days every year, where member-states would discuss the so-called core five pillars. The **International Law** pillar will focus on how existing international law applies to the use of ICTs by States, aiming to identify areas of convergence and consensus on principles such as State sovereignty, peaceful settlement of disputes, and non-intervention.

The second pillar on **Rules, Norms, and Principles of Responsible State Behaviour** will look into further developing and implementing voluntary, non-binding norms, first outlined in the UNGGE report of 2015, to reduce risks to international peace and security and provide guidelines for responsible State behaviour in cyberspace. The third pillar of **Confidence Building Measures** aims to build trust and increase interaction among member states. The main deliverable agreed upon was a Global Points of Contact (POC) directory, launched in May 2024, among the eight confidence-building measures, put forth in the third annual report of the OEWG.

The other voluntary and non-binding confidence-building-measures (CBMs) contained in that report include: (1) continued exchange of views and undertaking bilateral, sub-regional, regional, cross-regional and multilateral dialogue and consultations between States; (2) sharing of information, voluntarily, such as national ICT concept papers, national strategies, policies and programmes, legislation and best practices; (3) encouraging cooperative development and exercise of CBMs; (4) regular organisation of seminars, workshops and training programmes on ICT security as a means to build trust and enhance confidence between States; (5) promoting information exchange between States; (6) regular exchange of information and best practices on the protection of critical infrastructure (CI) and

critical information infrastructure (CII); and (7) strengthening public–private sector partnerships and cooperation on ICT security.

The fourth pillar, **Capacity Building**, is a central focus area, described as "foundational to developing the resources, skills, policies and institutions necessary to increase the resilience and ICT security of States and to accelerate the digital transformation of States...".[1] The final pillar is **Regular Institutional Dialogue**, which is operationalised through the Global Mechanism.

In addition to the plenaries, two Dedicated Thematic Groups (DTG) will meet for five days annually, in a hybrid format, enabling larger participation.[2] While proposals were made to have separate groups looking at issues such as building resilience of cyber ecosystems and critical infrastructure, cooperating in managing ICT-related incidents, and preventing conflict and increasing stability in cyberspace, these were all combined into one group. A second group will specifically look at capacity building. There are also provisions for intersessional meetings to address issue-specific discussions and for a review conference to be held every five years. These would be crucial to address a growing list of emerging threats, including the malicious use of AI to create malware and deep fakes.

The Road to the Global Mechanism

These outcomes result from five years of intense discussions, which were built on the consensus reports of the preceding five UNGGEs, which ran over nearly two decades, and an earlier iteration of the Open-Ended Working group from 2019 to 2021.[3] In fact, the issue of information security first appeared on the UN agenda when the Russian Federation introduced a draft resolution in the First Committee of the UN General Assembly. This was a response to the perceived US dominance in ICT and military technology after the 1991 Gulf War.[4]

The first GGE on cyber issues was established in 2004–2005 under the UN Disarmament Committee following a Russian proposal in 2002.[5] This initial attempt did not result in a consensus report due to lack of agreement among UN Security Council permanent members and limited international interest in cyber stability.

[1] **"Final Report of the Open-ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025"**, United Nations, p. 2.

[2] Ibid., pp. 19–20.

[3] Heli Tiirmaa-Klaar, **"The Evolution of the UN Group of Governmental Experts on Cyber Issues: From a Marginal Group to a Major International Security Norm-Setting Body"**, The Hague Centre for Strategic Studies & Global Commission on the Stability of Cyberspace, December 2021.

[4] Ibid., p. 3.

[5] **"Resolution Adopted by the General Assembly: A/RES/56/19"**, United Nations General Assembly, p. 2.

Cybersecurity was primarily considered a technical issue, not a strategic risk. Significant cyber-attacks against Estonia in 2007 and during the 2008 Russia–Georgia cyber conflict led to renewed attention being paid to cyber threats and the establishment of the subsequent GGEs, with their reports moving the needle on recommendations to deal with cyber threats.

The 2010 GGE Report recognised cyber threats as "among the most serious challenges of the 21st century". The 2013 Report referenced application of existing international law (particularly the UN Charter and Universal Declaration of Human Rights) to cyberspace, voluntary non-binding peacetime norms, confidence and cooperation measures, and capacity-building measures.[6] The 2015 Report introduced 11 non-binding voluntary peacetime norms for responsible state behaviour into the cyber-lexicon and highlighted concepts such as attribution, supply chain security and vulnerability disclosure.[7] However, the wheel came full circle with the 2016–2017 GGE failing to reach consensus, mainly due to worsening geopolitical relations between major powers, particularly after the Russian interference in the 2016 US presidential elections. The GGE process was also criticised for being too opaque and exclusive, comprising experts from the five permanent members and experts from 10 (later 15) other states chosen based on geography.[8]

After a hiatus of three years, the General Assembly passed two resolutions in 2018, creating two parallel processes: a Russian-backed resolution calling for establishing an Open-Ended Working Group and a US-backed resolution calling for establishing a new UNGGE.[9] While the GGE process lapsed in 2021, a second OEWG was established in 2021which, which came out with a Final Report in 2025, after adopting three Annual Progress Reports (APR) by consensus.

Whilst the final report might seem quite underwhelming against the rising tsunami of cyber threats, the fact that they are being discussed at the intergovernmental level at the United Nations and progress has been made towards a Permanent Mechanism are significant achievements in themselves. Also, arriving at a consensus report in an area where most countries have differing perspectives is a considerable

---

6 **"Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: Note by the Secretary-General"**, United Nations, 24 June 2013, p. 8.

7 **"Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: Note by the Secretary-General"**, United Nations, 22 July 2015.

8 Andrijana Gavrilović,**"What's New with Cybersecurity Negotiations? The UN GGE 2021 Report"**, *DiploFoundation*, 6 June 2021.

9 **"Resolution Adopted by the General Assembly on 22 December 2018: A/RES/73/266"**, United Nations General Assembly.

achievement, even if, by all accounts, these outcomes are watered down compared to the many proposals put forward by member states during the deliberations.[10]

However, the fact that all issues were raised and many of the proposals were referenced for potential future consideration means that they will "serve as building blocks for future discussions".[11] The report said, "States increasingly recognised the interconnections between all the issues addressed under the OEWG."[12] Both participants and observers have described the OEWG process as a confidence-building mechanism.[13] Over the five years, there was increasing participation from countries, particularly those from the Global South, and this was also reflected in the emphasis on capacity building in the Final Report.[14] Another catalyst was that the smaller states, such as Costa Rica, had experienced cybercriminal activities first-hand and wanted to record their experiences and highlight the dangers posed to the security of states.

Geopolitical Impact on Contentious Issues

The geopolitical stresses led to drawing red lines and avoiding detailed discussions.[15] On the issue of using ICTs in cyber conflict, many countries, including the USA, Italy and Brazil, called for acknowledging the reality that ICTs were already being used in conflicts and hybrid operations and pushed to remove references to the peaceful use of ICTs. Another set of countries, including Iran, Pakistan, Indonesia, Cuba and China, insisted on adhering to the exclusive peaceful use of ICTs. They felt that weakening this principle could be interpreted as legitimising the use of force in cyberspace. Similarly, while ransomware was widely discussed as a growing threat to national security, and several countries pushed for its inclusion in the report, China and Russia's view that it came within the purview of the recently signed Cybercrime Treaty prevailed.[16]

---

[10] Vladimir Radunović et al., **"UN OEWG Concludes, Paving Way for Permanent Cybersecurity Mechanism"**, *Digital Watch Observatory*, 17 July 2025.

[11] Allison Pytlak et al., **"The Rules of the Road in Cyberspace, 10 Years Later"**, Royal United Services Institute, 13 August 2025. Among the many issues raised were "commercially-available ICT intrusion capabilities", AI security, sub-sea cables and quantum computing.

[12] **"Final Report of the Open-ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025"**, no. 1.

[13] **"Breaking Down the OEWG's Legacy: Hits, Misses, and Unfinished Business"**, *Digital Watch Observatory*, 18 June 2025.

[14] Joe Devanny, **"Two (or Too Many) Cheers for UN Cyber Diplomacy?"**, Carnegie Endowment for International Peace, 29 July 2025.

[15] Louise Marie Hurel, **"The Rocky Road to Cyber Norms at the United Nations"**, Council on Foreign Relations, 6 September 2022.

[16] Ibid.

On norms, while many countries called for the implementation and operationalisation of existing norms, others wanted work to begin on new norms, including legally binding ones. Some countries adopted a middle path, with Singapore noting that unless the existing norms were implemented, it would not be clear what new norms were required. There was agreement that the 11 non-binding norms for responsible state behaviour agreed on in the 2015 UNGGE report continued to form the cornerstone of any framework.[17]

While the 2015 UNGGE reached a consensus that international law applies in cyberspace, the applicability of international humanitarian law remains a contentious topic not included in the final report, even though it was widely discussed in many sessions. The United States opposed the DTG on the International Law proposal, fearing it would be used to advance new, legally binding obligations or a binding treaty proposal.[18]

Funding, Resourcing and Implementation Issues

With the successful conclusion of the OEWG and a roadmap for the way forward, several wrinkles still need to be ironed out, beginning with the issue of funding the proposed mechanism, especially for the DTGs. A United Nations voluntary fund was proposed to support the capacity-building of states and to facilitate the participation of national representatives and experts, particularly from developing countries. However, there was opposition and scepticism about the proposal as to whether countries would actually contribute in the light of the financial crisis that the United Nations itself was going through.[19] The future effectiveness of the mechanism, especially its capacity-building pillar, is directly tied to progress on securing predictable and sufficient funding.

India proposed the establishment of the Global ICT Security Cooperation and Capacity-Building Portal (GCSCP) to facilitate practical cooperation by providing a centralised resource for sharing information, best practices, guidelines, national policies, strategies, surveys, trend reports and a Global Points of Contact (PoCs) directory. While other portals existed, this aimed to go beyond that by facilitating cyber incident reporting and direct communication between member states. The UN

[17] The above reportage on the proceedings is taken from a number of sources including podcasts, blogs as well as reports from the Digital Watch Observatory in Geneva which has been providing up-to-date information on developments in the OEWG. Vladimir Radunović et al., **"UN OEWG Concludes, Paving Way for Permanent Cybersecurity Mechanism"**, no. 10; James Lewis and Chris Painter, **"Inside Cyber Diplomacy Redux"**, Center for European Policy Analysis, 2025.

[18] Pavlina Pavlova and Christopher Painter, **"The UN's Permanent Process on Cybersecurity Faces an Uphill Battle"**, *Lawfare*, 13 August 2025.

[19] Ibid.

Secretariat would be responsible for its development, deployment, maintenance and management.

In the final report, it was decided that the portal should be developed incrementally, initially functioning as the website of the permanent mechanism and the location of the Global Points of Contact directory. The UN Secretariat has been requested to provide an initial report outlining a proposal for the portal's development and operationalisation based on states' views. Still, fears were expressed that it would also require vast resources.

Participation and Multi-Stakeholder Engagement

The participation of NGOs and multi-stakeholders remains unresolved, with the existing practice of United Nations Economic and Social Council (ECOSOC)-accredited stakeholders having observer status remaining. In contrast, others are subject to a non-objection process where a single state can veto accreditation.[20]

Russia had used the veto to block as many as 27 Western NGOs during the OEWG process,[21] initially in response to the US refusal to issue a visa to the Russian delegation leader, Andrei Krutskikh.[22] Visa refusals have continued even into 2025, with Russia incorporating its objection in its country statement, stating, "We consider it unacceptable that negotiations within the OEWG and the future permanent mechanism are undermined by visa barriers".[23] Multi-stakeholder participation, therefore, remained muted, even if nominally present, with experts complaining that their expertise was "not adequately reflected in the negotiation process".[24]

This underscores the rocky road traversed in search of cyber stability at the United Nations, especially in the last decade, as 'geo-political storms' swirled around, with the ongoing Ukraine and Gaza conflicts and attendant cyber-conflicts. The OEWG's Final Report (2025) noted that the sessions took place in a "geopolitical environment that has become very challenging, with rising concerns over the malicious use of ICTs by State and non-state actors that impact international peace and security".[25] The

[20] Allison Pytlak et al., **"The Rules of the Road in Cyberspace, 10 Years Later"**, no. 11.

[21] Louise Marie Hurel, **"The Rocky Road to Cyber Norms at the United Nations"**, no. 15.

[22] **"UN Working with US on Issue of Visa Refusal to Top Kremlin Cyber Official: Spokesperson"**, *The Print*, 27 July 2022.

[23] **"Statement by the Russian Interagency Delegation at the Tenth Session of the UN Open-Ended Working Group on Security of and in the Use of ICTs 2021–2025"**, Russian Federation, UNODA Documents Library, 17 February 2025, p. 3.

[24] **"Breaking Down the OEWG's Legacy: Hits, Misses, and Unfinished Business"** no. 13.

[25] **"Final Report of the Open-ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025"**, no. 1, p. 1.

Chair, Amb. Burhan Gafoor of Singapore reiterated this in his opening remarks in the 11th and final substantive session on 7 July 2025.[26] The battles within the group are also reflected in the lengthy official name of the permanent mechanism, which considers the various groups' requirements.[27]

Assessment

As the geopolitical landscape becomes increasingly fractured, and cyber threats become even more potent, it remains to be seen whether the proposed mechanism will attain the required heft to provide a modicum of stability in cyberspace. Western observers have been largely pessimistic about the outcome, to some extent because Western countries are now less able to shape the result of these deliberations.[28] One report noted that the existing norms were routinely flouted, undermining confidence in the normative process. Furthermore, given the lack of enforceability or meaningful accountability for these voluntary and non-binding norms, there was nothing to hold states to account.[29] Christopher Painter and James Lewis, US representatives in earlier UNGGEs, felt that capacity building through a UN process was "frankly unworkable" due to lack of resources, secretariat and private sector involvement.[30]

To conclude on an optimistic note, when the OEWG mechanism was set up with 193 countries participating, it was felt that it stood even less chance of fulfilling its mandate of arriving at consensus reports since a 15-member UNGGE had twice ended its two-year tenure without producing a consensus report. Some credit must go to the countries of the Global South and the middle powers who stood their ground and ensured the successful completion of the OEWG process. As it stands today, the OEWG's Final Report is a meaningful institutional advance that moves from the intermittent diplomacy of the past into a standing UN mechanism for responsible State behaviour in cyberspace.

[26] **"(1st Meeting) Open-Ended Working Group on Information and Communication Technology (ICT) – Eleventh Substantive Session"**, *UN Web TV*, 7 July 2025.

[27] Pavlina Pavlova and Christopher Painter, **"The UN's Permanent Process on Cybersecurity Faces an Uphill Battle"**, no. 18.

[28] James Lewis and Chris Painter, **"Inside Cyber Diplomacy Redux"**, no. 17.

[29] Joe Devanny, **"Two (or Too Many) Cheers for UN Cyber Diplomacy?"**, no. 14.

[30] James Lewis and Chris Painter, **"Inside Cyber Diplomacy Redux"**, no. 17.

About the Author

Dr. Cherian Samuel is Research Fellow at the Manohar Parrikar Institute for Defence Studies and Analyses, New Delhi.

Manohar Parrikar Institute for Defence Studies and Analyses is a non-partisan, autonomous body dedicated to objective research and policy relevant studies on all aspects of defence and security. Its mission is to promote national and international security through the generation and dissemination of knowledge on defence and security-related issues.

Manohar Parrikar Institute for Defence Studies and Analyses
1, Development Enclave, Rao Tula Ram Marg
New Delhi 110 010 India
T +91-11-2671 7983 F +91-11-2615 4191
www.idsa.in
Twitter @IDSAIndia
www.facebook.com/ManoharParrikarInstituteforDefenceStudiesAnalyses