Egypt at the First Plenary Session of the UN Global Mechanism on ICT Security

Rana Moustafa Essawy & Mahmoud Hatem El Shafaey
Cyberspace | Jul 24, 2026

During the first substantive plenary session of the Global Mechanism on ICT Security, held from 20 to 24 July 2026 at United Nations Headquarters in New York, Egypt delivered a national statement on how threats should be discussed in the mechanism. It also joined two cross-regional joint statements on international law.

Egypt's statement focused on the following points:

1. **Threats are not specific to certain regions or countries**. All countries and regions have an equal right to see the challenges and threats they consider national priorities reflected and discussed equally, in both the plenary and the thematic groups.
2. **Thematic group discussions should not replicate the plenary**.
3. **Discussions should be dynamic and based on real case scenarios**. A threat should be examined from all aspects: first analysing it, then considering how to deal with it in coordination with national and regional authorities, and through international cooperation.
4. **An agreed pool of experts is very important.** Egypt called for compiling and agreeing on a pool of experts accepted by delegations, since discussing threats without professional expertise would be a waste of time. Egypt clarified that this is not meant to block particular experts. While consensus is key, the bigger picture is to have relevant experts who help diplomats understand threats and produce tangible outcomes.

The joint statements joined by Egypt emphasised the following:

1. **International law applies to the use of ICTs and is a key pillar of the framework for responsible state behaviour.** It is essential to maintaining peace and stability and to an open, secure, stable, accessible and peaceful ICT environment. This was established in the consensus reports of the GGEs of 2010, 2013, 2015 and 2021 and the final reports of the 2019–2021 and 2021–2025 OEWGs. The task now is to deepen common understanding of how exactly it applies. Such understandings increase the predictability of state behaviour, lower the risk of miscalculation and clarify the consequences of unlawful state behaviour.
2. **The mechanism should build on previous work.** This includes the discussions in the GGEs and OEWGs, the national and regional positions published by states, the resolution of the 34th International Conference of the Red Cross and Red Crescent (2024), and the ICT work stream of the Global Initiative to Galvanize Political Commitment to International Humanitarian Law (IHL). The OEWG final report did not fully reflect all of these positions.
3. **Two cross-regional working papers from the OEWG 2021–2025 should serve as a basis.** The first, on the application of international law in the use of ICTs, identified emerging common understandings on state responsibility, human rights obligations, the peaceful settlement of disputes and the application of IHL in armed conflict. The second, on the

application of IHL to ICT operations, elaborated the IHL rules and principles applicable to cyber operations and identified measures to ensure respect for IHL.

4. **IHL should now be a priority for the mechanism, as the OEWG final report did not retain explicit language on it.** Applying IHL does not increase the risk of armed conflict in cyberspace. Failing to apply it leaves that risk unaddressed and leaves civilians and other protected persons and objects less protected.
5. **Five areas of international law should be addressed in a structured and inclusive manner**:
    - Sovereignty and the prohibition of intervention.
    - State responsibility and due diligence.
    - The prohibition of the use of force and the right of self-defence under Article 51 of the UN Charter.
    - IHL as it applies to cyber operations in armed conflict, including the principles of distinction, proportionality, precaution, necessity and humanity, and the protection of protected persons and objects.
    - International human rights law as it applies to state conduct in cyberspace, including privacy, freedom of expression, non-discrimination and freedom of association.
6. **International law, including IHL, should feature prominently in the first dedicated thematic group (DTG 1) and be discussed in an integrated, policy-oriented and cross-cutting manner.** Continuity on international law, including IHL, is “not optional”. The Chair, in coordination with the DTG 1 co-facilitators, was encouraged to initiate dedicated discussions on real-world scenarios. These include protecting critical infrastructure such as hospitals, water systems and energy networks from malicious ICT operations, in peacetime and in armed conflict.
7. **Capacity-building,** including through the second dedicated thematic group, should enable states to participate meaningfully in these discussions, develop national positions and enhance implementation of international law.
8. **Emerging common understandings** reached in the mechanism’s discussions must be reflected in its reporting.

Printed from EGYPIL.com