STATEMENT TO BE DELIVERED BY THE PERMANENT REPRESENTATIVE OF GHANA TO THE UNITED NATIONS IN GENEVA DURING THE 2ND STATE CONSULTATION ON UPHOLDING INTERNATIONAL HUMANITARIAN LAW IN THE USE OF ICTS DURING ARMED CONFLICTS, GENEVA – 24TH NOVEMBER, 2025

Excellencies, Distinguished Delegates, Colleagues,

On behalf of the co-chairs, Ghana, Mexico, Luxembourg and Switzerland, allow me to thank all delegations for their committed engagement in this second consultation on upholding International Humanitarian Law in the use of ICTs during armed conflict. Our collective task remains clear: to deepen our shared understanding of how existing IHL applies in the digital domain and to identify concrete measures that protect civilians, humanitarian actors, and medical services from the harmful effects of cyber operations.

On the first guiding question, concerning practical measures to ensure that ICT activities during armed conflict do not damage or disrupt medical services, humanitarian activities or objects indispensable to civilian survival, Ghana has taken deliberate steps at the legal, institutional, and operational levels.

The **Cybersecurity Act of 2020**, which established the Cyber Security Authority, provides the legal foundation to designate and protect **Critical Information Infrastructure**, including hospital networks and ICT systems depended upon by humanitarian organisations. Our **Data Protection Act of 2012** imposes strong confidentiality, integrity, and security obligations on those who handle health and humanitarian data. These laws are complemented by the **National Cybersecurity Policy and Strategy** and the **National Security Strategy**, both of which prioritise the resilience of critical services in ways that directly support compliance with IHL.

Institutionally, Ghana has strengthened its **national Computer Security and Incident Response Team (CSIRT) architecture**, enabling coordinated incident reporting, threat intelligence sharing and rapid mitigation across health, humanitarian, and security actors. We maintain structured collaboration between the Cyber Security Authority, the Ministry of Health, the Data Protection Commission, and defence and security organs. Complementing this, significant investment is being made in cybersecurity capacity-building for uniformed personnel, civilian agencies, and operators of critical infrastructure.

At the technical level, Ghana encourages or requires operators of medical and humanitarian ICT to adopt baseline controls: multi-factor authentication, role-based access, network segmentation separating clinical from administrative systems, regular patching, encryption of data in transit and at rest, and continuous monitoring. We emphasise **offline backups** and disaster-recovery mechanisms, ensuring that essential services, including emergency and surgical care, can continue if digital systems fail during conflict.

Ghana also highlights operational restraint, which is a core IHC consideration, by integrating IHL principles and cyber-specific scenarios into training for military planners. This is done in collaboration with institutions such as the **Kofi Annan International Peacekeeping Training Centre** and the ICRC and it includes maintaining and communicating lists of specially protected medical and humanitarian facilities and ensuring that cyber operations are planned and conducted with full respect for the principles of distinction, proportionality, and precautions in attack.

Excellencies,

The second guiding question asks whether the specific protection of medical facilities extends to the **confidentiality, integrity, and availability** of the digital data they hold.

Ghana's view aligns with the ICRC's position, as enshrined in the principles captured under the Geneva Conventions of 1949 which states inter-alia the protection of medical units under IHL extends to the systems and data essential for their functioning. A cyber operation that exfiltrates, corrupts, or encrypts patient data, including data of wounded soldiers, may, in effect, disable the medical unit and impede life-saving treatment. This would be inconsistent with the special protection accorded to medical facilities, equipment, and personnel.

Similarly, humanitarian organisations rely on sensitive digital data for registration, logistics, tracing and protection case management. A cyber operation that compromises the confidentiality of this data could expose vulnerable populations, including displaced persons, women, and children, to targeted harm. If data integrity or availability is undermined, essential humanitarian operations may be paralysed. Accordingly, Ghana holds that the specific protection of humanitarian objects encompasses the digital information and systems indispensable to their functioning.

On the third guiding question, concerning risks arising from ICT activities relating to the prohibition of sexual violence and unlawful recruitment or use of children in hostilities.

Ghana recognises that digital platforms have expanded the reach and sophistication of such abuses.

ICTs can enable **online grooming, sexual exploitation, blackmail, extortion**, and the creation or circulation of child sexual abuse materials. Digital spaces can serve

as propaganda and recruitment channels for armed actors seeking to target children remotely. Poorly secured humanitarian or medical databases may expose survivors of sexual violence to reprisals, stigma, or further victimisation. And cyber disruptions affecting telecom networks or humanitarian coordination may impede child-protection services and gender-based-violence response mechanisms.

In response, Ghana launched a **National Child Online Protection Framework in 2024** which strengthened reporting systems, takedown procedures for harmful content, and public awareness campaigns. The Cyber Security Authority works closely with law enforcement, civil society, and industry partners to combat online exploitation and hold perpetrators accountable. These efforts align with broader African Union initiatives to harmonise child-online-safety measures across the region.

Distinguished Delegates,

In closing, Ghana reaffirms that **International Humanitarian Law fully applies to cyber operations during armed conflict**, and that protecting civilians, medical services, and humanitarian missions in the digital age requires both legal adherence and practical implementation. We must ensure that cyber technologies, powerful as they are, are never used to deepen the suffering of wounded persons, humanitarian workers, or children.

We thank all participants for their constructive engagement and look forward to further dialogue as we advance this essential agenda.

Thank you.