Session Outcome Document

Law, Tech, Humanity, and Trust: A Working Session on the Digital Emblem Project

International Committee of the Red Cross

11.07.2025 11:30 – 12:30

https://www.itu.int/net4/wsis/forum/2025/Agenda/Session/508

Key Issues discussed: Looking Beyond 2025 (5–8 bullet points highlighting achievements, emerging trends, challenges in 20 years, figures, success stories and opportunities for WSIS beyond 2025)

- **Digital emblem as a success story in norm development**: The ICRC's Digital Emblem project was showcased as a concrete example of how international humanitarian law can be adapted to the digital age— and without substantive changes to the applicable rules - using a technical marker to ensure medical and humanitarian digital assets remain 'visible' even online.
- **Evolving threats to critical infrastructure**: The threat landscape has grown from digital divide and access issues to include cyberattacks against hospitals, power grids, and humanitarian organizations. The Digital Emblem responds to this evolution by creating a visual indicator for cyber actors to distinguish protected entities in cyberspace – but the importance of the digital divide cannot (and will not) be set aside, even in the development of such tools.
- **Recognition of the humanitarian layer of cybersecurity**: Discussions at WSIS+20 highlighted a growing consensus on the need to account for humanitarian impact in the design of cybersecurity norms, standards, and capacity building. The digital emblem is helping to frame this space.
- **Cross-sectoral support and momentum**: The Digital Emblem project has received strong backing from both governmental and private sector actors. Its development in consultation with States, technology companies, and technical standardization bodies (like the IETF) is increasingly recognized as a model for inclusive, multistakeholder norm-making.
- **Figures of reach and engagement**: At the 34th International Conference of the Red Cross and Red Crescent, which brings together all 196 States party to the Geneva Conventions as well as all 193 components of the Red Cross and Red Crescent Movement, Resolution II was adopted by consensus, encouraging the ICRC's work on a digital emblem. The Cybersecurity Tech Accords adopted, in December 2024, the "Digital Emblem Pledge", similarly pledging support. At WSIS + 20, the Global Cybersecurity Forum also voiced support for the project.
- **Operationalizing protection in cyberspace**: A key takeaway from the session was recognizing the difficulty of ensuring respect for protective symbols in cyberspace, particularly given the challenges of attribution, proxy actors, and automated systems. The project underscores the need for complementary technical, legal, and policy tools to buttress the respect and trust in a digital emblem.
- **Beyond 2025**: As the WSIS process continues, the ICRC offered the Digital Emblem as an example of how WSIS principles can be applied to emerging issues.

Tangible Outcomes of the session

- The session positioned the Digital Emblem as a leading example of humanitarian innovation in cyberspace, earning praise from diplomats and participants for its clarity, credibility, and relevance. The ICRC team—Joelle, Samit, and Mauro—effectively conveyed the seriousness and technical grounding of the initiative, reinforcing the ICRC's role as a critical voice in digital governance where it relates to armed conflict and other situations of violence.
- During the session, both the ITU and the Global Cybersecurity Forum (GCF) publicly voiced support for advancing technical discussions on standardizing the digital emblem. Notably, Luxembourg's Ambassador for Cybersecurity and Digitalization also expressed explicit support for the project, marking a new diplomatic ally in the process.
- Several stakeholders signaled their interest in collaborating with the ICRC in the next phase of the project, particularly on issues related to Internet standards (notably the ITU), protection mechanisms, and resilience. Follow-up discussions have been initiated to convene technical and policy actors, with the emblem now seen as a concrete point of convergence for humanitarian and cybersecurity communities.

Key Recommendations and Forward-Looking Action Plan for the WSIS+20 Review and Beyond (2–5 bullet points presenting concrete actions and guidance to inform the WSIS+20 Review by UNGA and build the multistakeholder vision of WSIS beyond 2025)

- **Embed humanitarian protection into digital policy frameworks**: As digital infrastructure becomes increasingly entangled with conflict dynamics, the protection of humanitarian digital infrastructure should be recognized as a strategic objective.
- **Advance inclusive norm- and standard-setting for digital protection**: The WSIS process should catalyze and support multistakeholder mechanisms—especially those involving humanitarian actors, States, industry, and technical bodies—to co-develop standards that enable the identification and protection of medical and humanitarian actors in cyberspace. Building on momentum from WSIS+20, this could include encouraging collaboration and harmony with standards bodies (including notably the ITU and IETF), integrating humanitarian use cases into cyber norm dialogues, and promoting interoperability between legal frameworks and technical protocols.