Concept Note: Proposal for a Main Session on Modern Warfare, Timeless Emblems: International Standardization of Digital Protective Signs

Theme: Digital Trust and Resilience

Session Title: Modern Warfare, Timeless Emblems: International Standardization of Digital Protective Signs

Organizers: International Committee of the Red Cross (ICRC), Microsoft, and Global Cybersecurity Forum (GCF)

Background: Since its inception at IGF Kyoto, the Digital Emblem initiative is enhancing global peace and stability by creating a universally recognized symbol that signifies protected digital infrastructure during times of armed conflict. This initiative is inspired by the Geneva Conventions' Red Cross emblem, which marks specifically protected people, objects, and places. An emblem is a device, symbol, or figure adopted and used as an identifying mark to represent a particular person, group, or idea. In culture, emblems such as a flag, badge or coat of arms communicate group identity. Such emblems are often comprised of a set of attributes, each with symbolic meaning. To date, this initiative has: 1.) Achieved International legal consensus in that all 196 states that have signed the Geneva Conventions adopted a resolution supporting the work on the digital emblem and a legal study on its use. 2.) Established an engineering protocol working group within the Internet Engineering Task Force (IETF) to create standardized governance protocols for the Digital Emblem. This group is tasked with developing the technical standards necessary for its implementation. 3.) Secured adoption by Cyber Tech Accord signatories, on International Human Rights Day, over 160 Cyber Tech Accord signatories pledged to support the digital emblem. This broad commitment from the tech industry signifies a collective effort to integrate and uphold the principles of the digital emblem.

Under International Humanitarian Law (IHL), the Red Cross, Red Crescent, and Red Crystal emblems are symbols of protection – used to identify persons and objects that benefit from certain specific protections under that body of law. Today often these emblems/symbols require a sense of sight, or touch to become known to the receiver. There is a need to sense emblems/symbols through digital communication channels. Digital emblems extend the range of identifying marks from the physical (visual and tactile) to the digital realm. The presence of a digital emblem represents a new signal available to cyber operators.

Objective: The primary goal of this session is to demonstrate tangible progress within the Internet Engineering Task Force (IETF) that is developing a digital emblem based on international humanitarian law and security standards. This digital emblem project includes engineering comprehensive architecture and model that defines a standard digital emblem to be used globally. This group will then address specific initial use cases such as in the technology sector and government.

Format: Main Session

Duration: 60 minutes

Format Description: This open forum will feature a 20-minute keynote, a 30-minute moderated panel discussion, and a 20-minute Q&A. Using a theater setup, panelists will discuss the cyberthreat landscape, especially in terms of destruction and disruption of specially protected civilian digital assets, describe the work at the IETF to standardize the technology, and ongoing initiatives and diplomatic processes. The 60-minute format ensures a focused agenda while accommodating attendees' schedules. A dedicated Q&A session will foster meaningful dialogue between panelists and the audience. This structure allows panelists to provide comprehensive insights, helping attendees understand cybersecurity challenges posed by digital infrastructure and propose actionable steps to protect civilians globally.

What participants will gain from attending the session: Participants will gain a clear understanding of the progress made toward the creation and standardization of a Digital Emblem, why it matters. and how this will be deployed once the standards will be available. Experts will share insights into the ongoing work at the IETF, the challenges and opportunities for legal recognition, and how different stakeholders, from governments to the private sector, can contribute to its operationalization. Attendees will also learn about real-world implications of the Digital Emblem and how it can enhance cyber protections for humanitarian organizations, medical facilities, and other specially protected entities in future conflicts.

Policy Questions:

- Why is the standardization of a digital emblem necessary for protecting critical civilian digital infrastructure during armed conflict, and how does it build on existing legal protections under international humanitarian law?
- How has the development of the Digital Emblem progressed within the Internet Engineering Task Force (IETF), and what key milestones have been achieved so far?
- How can the international community, including governments, industry, and civil society, contribute to the successful deployment and enforcement of the Digital Emblem once standards are finalized?
- Why is there a need to create a digital emblem to protect digital infrastructure and services during times of armed conflict?
- What are the technical, legal, and diplomatic challenges of standardizing a digital emblem, and what strategies can stakeholders take to ensure its adoption and implementation?
- From technological standards to legally binding obligations. How to make a digital emblem a reality?

SDGs

1, 2, 3, 4, 5, 5, 6, 7, 8, 9, 10, 11, 12, 13, 16, 17

Co-Organizers:

- ICRC and Microsoft

Moderator:

- Chelsea J. Smethurst, Director Digital Diplomacy, Microsoft, private sector, United States

Speakers:

- International Committee of the Red Cross, Dr. Cordula Droege, Head of Legal
- Microsoft, Amy Hogan-Burney, Corporate Vice President, Customer Security and Trust
- Global Cyber Forum, [Speaker to-be-determined]

Expected Outcomes:

- The session will produce a summary report outlining the key takeaways and recommendations for further actions.

Contact Information: For more information, please contact:

- Mauro Vignati, Legal Adviser, ICRC, International organization, Switzerland
- Chelsea J. Smethurst, Director Digital Diplomacy, Microsoft, private sector, United States
- Global Cyber Forum, Saudi Arabia, non-profit