HUMANITARIAN LAW & POLICY

IHL's lighthouse: navigating towards a digital emblem

January 14, 2026, Cyber / Cybersecurity and data protection in humanitarian action / IHL / Law and Conflict / New Technologies / Special Protections / Technology in Humanitarian Action

16 mins read


Samit D'Cunha
Legal Adviser, ICRC


Mauro Vignati
Adviser on new digital technologies of warfare, ICRC

As cyber operations are increasingly taking place during armed conflicts, and this trend is likely to continue, certain specific protections afforded under IHL and identified in the physical world by the distinctive emblems of the Red Cross, Red Crescent, and Red Crystal must also be visible in an environment the drafters of the very first Geneva Convention in 1864 could never have imagined.

In this post, Samit D'Cunha, Legal Adviser at the ICRC, and Mauro Vignati, Technical Adviser at the ICRC, examine the rationale behind the Digital Emblem Project and the significant progress made in recent months. Drawing on ongoing standardization efforts and a growing list of supporters of the project, this post explores how a simple, globally recognizable marker is being developed to help distinguish specifically protected medical and humanitarian assets online.

In their nearly 2,500-year *history*, the function of lighthouses has remained largely unchanged. Vital in guiding ships safely through treacherous waters, signaling danger, and marking safe passage, their often-standardized design and broadly recognized signals have become crucial for maritime safety. As a result of the rapid advancements in technology over the last 50 years, traditional lighthouses have also been complemented, not replaced, by digital navigation aids like GPS, electronic charts, and radio beacons.

While ultimately dependent on information and communication technologies (ICTs) and other modern technologies, GPS is powerful when paired with charts. Modern electronic chart systems depict lighthouses and coastal hazards, extending protection beyond a light's line-of-sight and in poor visibility. Today, all these technologies, both new and old, work together to establish a sort of layered redundancy, using both visual and electronic aids to serve the quintessential purpose of protecting ships and seafarers from risks while at sea.

We have used navigational aids as metaphors in discussing new technologies of warfare before, for example to shine a light on the risk of harm from certain *information operations* during armed conflict. This time, we use the prodigious lighthouse to explore how the distinctive emblem of the red cross, *conceived in the 1860s*,

as well as the red crescent and crystal, have over time been complemented by new technologies. This evolution must continue with the advent of cyber operations in armed conflict.

Bright ideas

The pressing need for certain digital assets to be able to signal themselves as protected has been the primary concern driving the *Digital Emblem Project*. The project seeks to create a specially authenticated symbol in cyberspace (a "digital emblem") to signal a legal protection that international humanitarian law (IHL) grants to certain medical and humanitarian digital assets during armed conflict. It is not a cybersecurity tool, just as the physical emblems are not shields; rather, the digital emblem aims to extend the purpose of the physical red cross, red crescent, and red crystal emblems into a digital environment through standardized, interoperable protocols so that these assets can be more visibly and reliably protected and spared from cyber operations.

This post explores some of the specific protections the digital emblem will identify and provides updates on the ongoing process of standardization. It also considers some of the key milestones the project achieved in 2024 and 2025, including:

- the adoption of *Resolution 2* (colloquially the "ICT resolution") at the 34th International Conference of the Red Cross and Red Crescent;
- the start of significant discussions on the standardization of digital emblems at the Internet Engineering Task Force (IETF) leading to the adoption of a Working Group Charter and a Use Case and Requirements document;
- the adoption of a *Digital Emblem Pledge* by the Cybersecurity Tech Accord, and;
- the establishment by the *Global Cybersecurity Forum* of an Impact Network on the Protection of Critical Infrastructure, with an initial focus on accelerating implementation of the Red Cross/Red Crescent digital emblem.

IHL *affords* specific protections to medical services and *certain* humanitarian activities, and the distinctive emblem was developed as a means of making these protected functions visible in times of conflict. Once specific protections were established, there had to be an easy way to discern them to ensure that they are respected in complex security environments (including on the battlefield). Aside from being a *compliment* to Switzerland (by inversing its flag), part of the reason for the simple design of a red cross (later crescent and crystal) was that, given its protective function and use in warfare, it had to be possible to rapidly *reproduce* it with the means available during war. Indeed, the physical design stood the test of time for over 160 years and became an archetypal symbol of medical and humanitarian assistance in war.

The distinctive emblem is IHL's lighthouse. Instead of shining a light on dangers, it illuminates the often-invisible protection the law affords to certain persons and objects and contributes to the safeguarding of the victims of war that IHL was designed to protect. But as communication technologies developed rapidly in the second half of the twentieth century, discussions on how the distinctive emblem could be complemented were also taking shape.

By the 1970s, the International Committee of the Red Cross (ICRC) *observed* that it was "no longer possible today to base effective protection solely on a visual distinctive emblem." Additional Protocol I, adopted in 1977, defined and elaborated rules on a "distinctive signal" in *Article 8(m)* and Chapter 3 of *Annex I*. Distinctive signals, including light and radio signals, are used today by certain medical marine vessels and aircraft as a complement to the distinctive emblem. As warfare extends into the digital realm, the development of a digital emblem reflects the endeavor to help ensure that the protections afforded to certain digital assets by IHL are upheld in cyberspace. Like the distinctive signal, it *complements*, and does not replace, the distinctive emblem.

Respect and protect

With respect to the digital assets of military and civilian medical services exclusively assigned to medical purposes, the ICRC, the International Federation of the Red Cross and Red Crescent Societies, and *certain activities* of National Red Cross and Red Crescent Societies, IHL provides them with unequivocal protection. Indeed, parties to conflict must *respect and protect* these services and activities. This carefully worded obligation encompasses broad and unqualified *commitments* and does not only require refraining from attack. For example, to respect and protect medical units also means not interfering with their work in order to allow them to continue to treat the wounded and sick in their care.

As the ICRC noted in its *2024 Challenges Report*, there is ongoing discussion regarding whether data can be considered an "object" under IHL and thus benefit from the protection afforded to civilian objects, including from being directly targeted. Also, a number of states suggest that a cyber operation causing only a loss of functionality *is not an attack*. However, these debates are largely inconsequential with respect to the clear and unambiguous protection afforded to medical and humanitarian data (see, for example, the *Tallin Manual 2.0*, *rule 132(3)*), or a more detailed explanation of this protection in this *ICRC short paper*.

Parties to a conflict who conduct malicious cyber activities affecting medical and humanitarian digital assets violate IHL. For example, deleting or encrypting medical data (including patient data or data tracking medical supply chains), interfering with the functioning of medical equipment, or compromising ICRC databases are all IHL violations.

The international community and other stakeholders clearly agree. On October 31, 2024, at the quadrennial *International Conference* (which brings together the 196 states party to the Geneva Conventions and all 193 components of the Red Cross and Red Crescent Movement) *Resolution 2* was adopted. After calling on parties to conflict to (1) "respect and protect medical personnel, units, and transports in accordance with their international legal obligations, *including with regard to ICT activities*" and (2) "allow and facilitate impartial humanitarian activities during armed conflict, *including those that rely on ICTs*, and to respect and protect humanitarian personnel and objects in accordance with their international legal obligations, *including with regard to ICT activities*," the Resolution goes on to encourage "the ICRC to continue consulting and actively engaging with states and Movement components" on the development and potential future use of the digital emblem.

Building on this growing chorus of voices, only a few weeks later, the Cybersecurity Tech Accord, a global coalition of some of the world's largest technology companies representing around a billion customers (all *signatories are listed here*), endorsed a *Digital Emblem Pledge*. The first operative paragraph commits to ensuring that their products and services are "developed, designed, distributed, and used in compliance with the principles and rules of international humanitarian law," and the second advocates for the adoption and widespread use of a digital red cross/red crescent emblem. This is a particularly important milestone given that the authorized users of the distinctive emblem, including the ICRC, often rely on the products and services of technology companies. In 2025, the Secretary-General of the *International*

Committee of Military Medicine also expressed its support for the ICRC's work on a digital emblem.

Standardize and integrate

Leveraging this momentum, as well as a rapidly growing list of supporters, partners, and contributors already on board, the ICRC hopes to contribute to clearly defining the digital emblem's technical parameters by answering the question of exactly how a digital technology such as *Authentic Digital Emblem (ADEM)* will identify protected digital assets in cyberspace.

The digital emblem will require certain key attributes that must be incorporated into international standards. Returning to our metaphor, international standards have helped ensure that lighthouses use signals that mariners from any country can interpret correctly and avoid accidents. Moreover, by adhering to international treaties, countries can ensure navigation in their waters meets globally recognized procedures, minimizing the risk of misunderstandings or navigation errors. Both international standards and international law also help promote innovation, ensuring collaboration on future technologies in the face of evolving maritime challenges. The technical standardization of the digital emblem and its incorporation into IHL largely share these same objectives.

To meet these objectives, the technology used for the digital emblem must be accepted by a wide range of stakeholders, including not only by states, but also the technology sector. The internet is composed of networking peers that communicate with one another and must understand each other. Standardization and universal acceptance is therefore a critical element for the project. The ICRC's years-long inclusive and ongoing consultative processes (see *here*, for example) already yielded several insights on functional and security attributes of the digital emblem that must be integrated into the standards and would encourage universal acceptance.

For example, in the ICRC's view, the digital emblem must be *decentralized*. Like its physical precursor, the digital emblem must not have a central control and distribution body. While standards will provide a blueprint for civilian and military medical personnel and objects and the components of the Red Cross and Red Crescent Movement to use the digital emblem, no international body will centrally control or authorize specific instances of its use.

Likewise for the physical distinctive emblems, decentralization ensures that the competent authority in relation to each authorized user, consistent with IHL and with measures in place to suppress misuse, can decide, in real time and in light of operational and security considerations, when, where, and how to display the emblem to best protect medical and humanitarian services and activities. There is no need for external authorization. The digital emblem must also have the ability to be observed without arousing suspicion or alerting users that it is being perceived, an attribute we call *covert inspection* or undetectable validation. While emerging as a somewhat peculiar requirement at first, the need for covert inspection is actually both simple and self-evident (albeit field-specific), reflecting into cyberspace the current reality that observing the physical emblem doesn't inform its bearer that someone is watching; the inverse would likely prove detrimental to its effectiveness in armed conflict.

Anchored in standards

The ICRC has turned to key international standardization bodies, the Internet Engineering Task Force (IETF) and the *International Telecommunications Union* (ITU), to ensure the digital emblem is built on globally recognized, interoperable, and trustworthy technical foundations.

The *IETF* is a large open international community of network designers, operators, vendors, and researchers who aim to make the internet work better by producing technical documents, particularly internet standards, that influence the way people design, use, and manage the internet. Notably, the IETF is the leading standards development organization for the internet and counts participation from many of the world's largest technology companies.

Participation, however, is not limited to technology experts. Many civil society organizations also participate. The IETF adopted a charter for the work on digital emblems and a dedicated working group began its work in July 2025 at *IETF 123*, tasked with developing use cases and requirements related to the working group's initial scope, including the digital analogs of IHL emblems. The working group is also tasked with developing a digital architecture that captures the relationships between entities utilizing digital emblems, a protocol describing the binding of emblems to assets, and a protocol specification describing the emblem discovery mechanism for the initial use cases. The IETF is an attractive venue for current and future technical development of the digital emblem, given it is a forum open to all nationalities and professions.

Interested stakeholders are encouraged to *join the conversation*. Indeed, recent meetings have collided the law and technology to positive effect. The spirit of universality, coupled with rigor and a culture of transparent, consensus-driven dialogue, make the IETF an appropriate forum for fostering the technical development of the digital emblem.

While the IETF plays a central role in developing the technical protocols that underpin the internet, the role of the ITU is equally important. As the United Nations specialized agency for information and communication technologies and the *world's oldest intergovernmental organization*, the ITU brings together governments, regulators, industry, academia, and civil society actors to develop and adopt global telecommunications standards. Its intergovernmental nature provides the Digital Emblem Project with an essential bridge between the technical and diplomatic communities, contributing to ensuring that any standard developed through the IETF can gain formal recognition and legitimacy at the international level and align with existing telecommunications regulations and infrastructures. This is necessary in addition to eventual integration into IHL.

Once the technical standards are finalized, the ICRC intends to work with states to explore the most appropriate avenues for integrating the digital emblem, and the standards that will underpin it, into IHL. This could take several forms, including an amendment to an existing instrument, or the adoption of new provisions that formally establish the digital emblem as a protective tool for digital assets. This interplay between the legal, policy, and technical dimensions of the project has been presented and discussed at several international fora this year, including at the *Internet Governance Forum*, *AI For Good*, and the World Summit on the Information Society (*WSIS*). Notably, at WSIS this year, the ITU voiced strong support for the project and a willingness to collaborate on developing standards.

Conclusion

At the confluence of law, politics, and technology, the Digital Emblem Project is an important component of the ICRC's work on protecting persons and objects from harmful ICT activities during armed conflict. Embracing the innovative nature of this work, the future might yet hold new and meaningful opportunities for the

technology developed for digitalizing the distinctive emblems. While the focus of the ICRC's work is currently the red cross, red crescent, and red crystal, there are other protective IHL emblems that can also be digitalized: the distinctive emblem of the 1954 Hague Convention colloquially known as the "*Blue Shield*" (see *Draft Regulation 14* for the use of the Blue Shield emblem adopted by the Committee for the Protection of Cultural Property in the Event of an Armed Conflict), the *international special sign for dangerous forces,* and the *international distinctive sign for civil defense* are the main examples.

Of course, these technologies will not replace nor alter their physical analogs, and, importantly, the substantive rules that currently apply will remain entirely unchanged by this project. Rather, the digital emblem, a necessary complement to existing IHL, will contribute to ensuring that the medical services and certain humanitarian activities are respected and protected, so that medical and humanitarian personnel can continue their work of reducing suffering and harm in the era of cyber operations in armed conflict. It will be for parties to conflict, and those watching, to ensure that these rules are ultimately respected. To conclude our metaphor: lighthouses don't fire cannons to *call attention* to their shining. They just shine. The digital emblem is being built in that same spirit – to quietly mark what must be respected and protected.

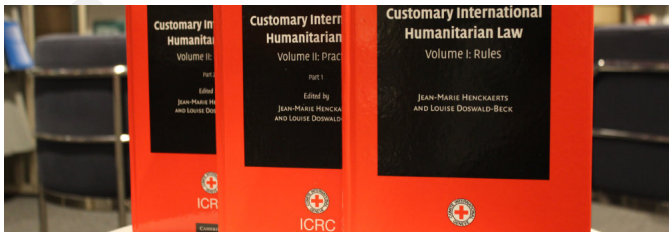
Acknowledgement: The authors wish to thank colleagues at **Articles of War** *for encouraging the development of this post and their helpful comments on an earlier draft.*

See also

- Samit D'Cunha, *Conceive, standardize, integrate: the past, present, and future of adopting distinctive emblems and signs under IHL*, September 12, 2024
- Tilman Rodenhäuser, Mauro Vignati, *Towards a 'digital emblem'? Five questions on law, tech, and policy*, November 3, 2022
- Felix E. Linker, David Basin, *Signaling legal protection during cyber warfare: an authenticated digital emblem*, September 21, 2021
- Tilman Rodenhäuser, Laurent Gisel, Larry Maybee, Hollie Johnston, Fabrice Lauper, *Signaling legal protection in a digitalizing world: a new era for the distinctive emblems?*, September 16, 2021

Tags: Civilians, Cyber and Information Operations, Respect for IHL, Techplomacy, Use of Emblems

You should also read these articles



Twenty years on: the enduring impact of the ICRC customary IHL study and database

10 mins read

Cyber / Cybersecurity and data protection in humanitarian action / IHL / Law and Conflict / New Technologies / Special Protections / Technology in Humanitarian Action

Claudia Maritano & 2025 British Red Cross-ICRC customary IHL research team

The ICRC's 2005 study on customary international humanitarian law – along with the free, public ...

Complying with IHL in large-scale conflicts: How should states prepare to allow and facilitate delivery of humanitarian relief?

10 mins read

Cyber / Cybersecurity and data protection in humanitarian action / IHL / Law and Conflict / New Technologies / Special Protections / Technology in Humanitarian Action Ellen Policinski

Large-scale armed conflicts consistently sever the systems that sustain civilian life, leaving populations without essential ...