Towards a 'digital emblem'? Five questions on law, tech, and policy

November 3, 2022, Analysis / Humanitarian Action / Law and Conflict / New Technologies

🕐 10 mins read

Tilman Rodenhäuser
Thematic Legal Adviser, ICRC

Mauro Vignati
Adviser on new digital technologies of warfare, ICRC

Doctors who provide care for the war wounded and ICRC delegates who work in areas affected by armed conflict rely on a unique and universally recognized symbol of protection: the distinctive red cross or red crescent emblems. For over 150 years, these have conveyed a simple message: facilities, vehicles, or people displaying the emblem must not be attacked.

Today, medical facilities and humanitarian operations use digital technologies to respond to peoples' needs more efficiently and effectively. This digitalization, however, exposes them to new threats. As armed conflicts digitalize, can digital technology be leveraged to strengthen the protection of medical facilities? Can we incorporate the century old idea that 'hospitals, ambulances and evacuation parties … shall bear a red cross on a white ground' into the digital environment? Is it technically possible, and what would be the benefits and risks of doing so?

Since 2020, the ICRC has partnered with the Centre for Cyber Trust, Johns Hopkins University Applied Physics Laboratory, and, more recently, ITMO University St Petersburg and convened a global group of experts to assess the possible solutions, benefits, and risks associated with a 'digital emblem'. Its new report launched today on 'Digitalizing the Red Cross, Red Crescent and Red Crystal Emblems' presents technological solutions, expert views on the benefits and risks, and possible ways forward. In this post, ICRC Advisers Tilman Rodenhäuser and Mauro Vignati answer five essential questions on the idea of a 'digital emblem'.

What is a 'digital emblem', and what can it achieve?

As societies digitalize, cyber operations have become a reality of armed conflict. States have *identified* the increasing likelihood of 'the use of ICTs in future conflicts between States' as a threat to international security. The ICRC has warned against the potential human cost of cyber operations and raised concerns about the vulnerability of the medical sector and humanitarian organizations to cyber operations, including by cyber criminals. Indeed, since the onset of the COVID-19 pandemic, *cyber operations against hospitals* have disrupted life-saving treatment for patients, and forced doctors and nurses to resort to pen and paper at a time when their urgent work was needed most. And in 2022 alone, the Red Cross and Red Crescent Movement members have been *the target of different cyber operations*, as have other humanitarian organizations. In times of armed conflict, such operations put already vulnerable people – the wounded, the sick, persons in vulnerable situations – at even greater risk.

The idea of a 'digital emblem' is to develop a digital sign to identify – and signal protection of – primarily medical facilities and to incorporate it into international legal framework. A 'digital emblem' would add a layer of protection against cyber operations, just as the red cross, red crescent, or red crystal emblems do in the physical world. Such an emblem would provide a clear signal that the marked entity enjoys special protection under international humanitarian law and must be protected against harm.

It is important to understand that a 'digital emblem' is not a cyber-security measure that actually protects systems against intrusion or damage – it is a sign of legal protection. This means that any medical facility that employs such emblem would have to also take cyber security measures in addition to using a digital emblem – just as a hospital in a war zone normally employs a range of physical measures to protect itself against incidental harm.

What could a 'digital emblem' look like, and what characteristics would it need to have?

In simple terms, our *research partners* have developed three possible technical solutions for a 'digital emblem':

The first option is what we call a *'Domain Name System (DNS)-based' emblem*. This solution would use a special label to associate the 'digital emblem' with the domain name (e.g., www.hospital.*emblem*). This would be a straightforward, human-readable 'digital emblem' identifying the protected system.

The second option would be a 'Internet Protocol (IP)-based' emblem. This type of emblem would require embedding semantics in IP addresses to identify both protected digital assets and protected messages traversing a network.

The third option goes under the name of *ADEM ('Authenticated Digital Emblem')* and essentially uses certificate chains to signal protection. Under that approach, these certificates (such as the small lock often found next to the address in your browser window) can be authenticated by different authorities and be communicated via different internet protocols.

We are currently refining and testing these different options with our partners. In this research, we are guided by a number of characteristics that medical, humanitarian, and military experts have emphasized as important.

For its use by medical facilities, a 'digital emblem' would need to be easy to deploy and maintain at low cost throughout the world, bridging linguistic, technological, resource, and cultural differences. It would need to integrate into the existing technological environment (including clouds) and be adaptable to future technological and infrastructure developments. A 'digital emblem' should also be easily removable, as that is crucial for addressing possible security risks. Moreover, a 'digital emblem' would need to be deployable under the direction of the competent authority of parties to an armed conflict.

In order to effectively signal protection, a 'digital emblem' will have to be 'visible' to and easily identifiable and understood by those conducting cyber operations ('cyber operators'). Operators have further emphasized that they should be able to probe for a 'digital emblem' without being identifiable as a potential threat actor. Ideally, a 'digital emblem' should be part of the information that any intruder asks of a system. It should also be possible to easily verify the authenticity of a 'digital emblem'.

What are the main benefits and risks associated with a 'digital emblem'?

The main benefit expected from a digital emblem is that it would make it easier for cyber operators to identify and spare protected entities by visualizing and operationalizing legal protections in the digital environment. In the 'fog of war', this additional signal can have real added value. It will primarily enhance protection for marked entities against the risk of harm caused by law-abiding operators and it may also have a deterrent effect on malicious ones.

At the same time, digitally marking and identifying medical and humanitarian entities risks increasing their exposure to harmful operations. The severity of this risk will vary. For many operators, it is already easy to identify medical or humanitarian organizations in cyberspace; the additional risk of facilitating their identification as marked entities may be relatively small. The use of a 'digital emblem' might, however, run the risk of greater exposure to operations by less sophisticated actors; however, these actors will also have less capabilities to cause harm.

A different risk is the potential misuse of a 'digital emblem' to falsely mark military or otherwise unprotected infrastructure. This risk also exists in the physical domain, and misuse of the emblem is widely prohibited under international and domestic law.

Who may use a 'digital emblem', and when?

The use of the distinctive emblems and signals is regulated in international humanitarian law (see, among other, article *44* First Geneva Convention; article *18* and *38* Additional Protocol I; *Annex 1* of Additional Protocol I) and corresponding national laws and regulations. Based on these provisions, the distinctive emblems may be used for two purposes:

First, to signal legal protection. For this 'protective' purpose, the distinctive emblems may only be used in times of armed conflict, not in times of peace (except as a preparatory step to ensure protection once conflict breaks out). Their use is further limited to, most notably, authorized medical

actors (medical services of armed forces; authorized civilian medical facilities) as well as the ICRC and the International Federation of Red Cross and Red Crescent Societies.

Second, in times of peace and in times or armed conflict members of the International Movement of the Red Cross and Red Crescent (RCRC Movement) may use the emblem for indicative purposes, meaning to identify themselves as members of the RCRC Movement.

While international humanitarian law limits the use of the distinctive emblems to medical entities and humanitarian operations linked to the RCRC Movement, other emblems or signals exist, for example, to identify the United Nations or cultural property.

Possible roads towards a 'digital emblem'

Based on the research and consultations conducted, the generally positive feedback received from the international group of experts, and the *unanimous encouragement of the RCRC Movement* 'to continue researching the technical feasibility of a digital emblem … and assess the benefits of such an emblem', the ICRC will continue research and consultation on a possible 'digital emblem'. On the technical side, this will require further work on the technical development as well as validation and verification of possible solutions, which the ICRC intends to do with its research partners. On the diplomatic side, it will now be for States to consider the idea and decide on possible next steps. The ICRC aims to convene consultations for this purpose with all relevant stakeholders – in particular States and the RCRC Movement.

A key strength of the distinctive emblems and signals is that their form, function, use, and protection are regulated in international humanitarian law, and their misuse prohibited. If a 'digital emblem' is considered desirable by States, different avenues exist for incorporating such emblem in the international legal framework. These include, but are not limited to:

- The adoption of a new additional protocol to the Geneva Conventions. This approach was taken in 2005 to establish the *'red crystal'*
- A revision of *Annex I of Additional Protocol I*, which regulates the use of 'distinctive signals' (light and radio signals, electronic identification) or communication (radio communication, codes). A procedure for regularly updating this annex is foreseen in Additional Protocol I (see *article 98*).

As cyber threats to medical facilities and impartial humanitarian organizations grow, it is time for the international community to come together to ensure that new threats are addressed by updating and innovating long-standing practical protection measures.

See also:

- Antonio DeSimone, Brian Haberman, & Erin Hahn, *Identifying protected missions in the digital domain*, September 23, 2021
- 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: digital emblem, Geneva Conventions, humanitarian, IHL, international humanitarian law

You may also be interested in:

Dangerous forces: the protection of nuclear power plants in armed conflict

🕐 25 mins read

 Analysis / Humanitarian Action / Law and Conflict / New Technologies

Abby Zeith & Eirini Giorgou

As the international armed conflict between Russia and Ukraine drags on, the international community continues …

Safeguarding humanitarian organizations from digital threats

🕐 9 mins read

 Analysis / Humanitarian Action / Law and Conflict / New Technologies

Tilman Rodenhäuser, Balthasar Staehelin & Massimo Marelli

For decades, there has been consensus in the international community that in times of armed …