DIGITALIZING THE RED CROSS, RED CRESCENT AND RED CRYSTAL EMBLEMS

BENEFITS, RISKS, AND POSSIBLE SOLUTIONS

ETH zürich

APL Johns Hopkins
Applied Physics Laboratory

Universität Bonn

Australian Red Cross

COMITE INTERNATIONAL GENEVE
ICRC

DIGITALIZING THE RED CROSS, RED CRESCENT AND RED CRYSTAL EMBLEMS

BENEFITS, RISKS, AND POSSIBLE SOLUTIONS

Report drafted by Tilman Rodenhäuser (Legal Adviser, ICRC), Mauro Vignati (Adviser on New Digital Technologies of Warfare, ICRC), Larry Maybee (Legal Adviser, Australian Red Cross) and Hollie Johnston (Legal Adviser, Australian Red Cross)

Citation: ICRC, *Digitalizing the Red Cross, Red Crescent and Red Crystal Emblems: Benefits, Risks, and Possible Solutions*, ICRC, Geneva, 2022.

CONTENTS

ACKNOWLEDGEMENTS

The present report is the outcome of two years of research and consultations among experts from different fields and backgrounds, led by the International Committee of the Red Cross (ICRC). The conceptualization, drafting and publication of the report would not have been possible without the commitment and contributions of several individuals and organizations.

Our gratitude goes first to the Centre for Cyber Trust (CECYT, a joint endeavour of ETH Zurich and the University of Bonn) and the Johns Hopkins University Applied Physics Laboratory (APL) for working and researching *pro bono* on technical possibilities for developing a 'digital emblem'. Both institutions invested significant time and effort in developing ways of digitally marking protected assets and data, as well as providing expertise and presenting their solutions at numerous expert consultations.

We are also indebted to the global group of experts who shared their knowledge and experience throughout a series of expert consultations. We sincerely thank them for having taken the time to analyse the proposals identified by the CECYT and APL, reflect on possible solutions, and participate in several consultations. A full list of experts is presented in Annex I.

The ICRC is also grateful to the Australian Red Cross for partnering in organizing and facilitating a series of global expert consultations to discuss the benefits and risks of using a 'digital emblem' to signal legal protection in times of armed conflict, and to contemplate possible solutions in this connection. The distinctive emblems are part of our shared identity and we were delighted to work with them on this project.

We would also like to express our gratitude, for drafting this report, to Tilman Rodenhäuser (legal adviser, ICRC), who has been leading this project for the past two years, and to Mauro Vignati (adviser on new digital technologies of warfare, ICRC), Larry Maybee (legal adviser, Australian Red Cross) and Hollie Johnston (legal adviser, Australian Red Cross), who were instrumental in organizing and facilitating expert consultations. Moreover, this project could not have advanced without the expertise and involvement of ICRC colleagues from different departments and delegations, in particular Laurent Gisel, Vincent Graf Narbel, Stephane Hankins, Jonathan Horowitz, Fabrice Lauper, Kubo Mačák, Cedric Maire, Lorenzo Redalie, Vitaly Savenkov, Bertrand Stivalet, and Delphine Van Solinge, as well as the support of the ICRC Innovation Facilitation Team.

FOREWORD

The digital transformation of our world extends to armed conflicts, to people affected by them, and to people seeking to alleviate the suffering they cause. For humanitarian and medical actors, including the International Committee of the Red Cross (ICRC), digital technologies provide extraordinary opportunities for making our response to peoples' needs in armed conflicts more efficient and effective. For example, we use satellite imagery to discover people in need and plan relief operations. We analyse large amounts of data to identify missing people and reunite them with their families. We offer a digital space during humanitarian crises for people to store their most important documents. And medical professionals use digital technologies in many different ways, for instance, to provide real-time guidance to medical personnel in health facilities behind front lines.

In recent years, however, we have also learnt that the vast opportunities provided by digital technologies come with risks. 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. At the beginning of 2022, we discovered that ICRC servers hosting personal data belonging to more than half a million people worldwide had been hacked, through a massive and highly sophisticated cyber operation. This put already vulnerable people – detainees, unaccompanied minors, migrants – at even greater risk. While cyber security and data protection have been strategic priorities for the ICRC, this data breach highlighted the urgency of our work in this area. Protecting personal data, and ensuring the availability and integrity of our data and systems in the digital space, is essential to assist and protect people in the real world.

To achieve this objective in a digital age we need to be reliable and innovative. For medical personnel and medical facilities, and for the humanitarian operations of the International Red Cross and Red Crescent Movement, the red cross and red crescent emblems – a simple red cross or red crescent painted on the roof of a hospital or vehicle – have long served as a sign of protection. Any ICRC delegate or Movement colleague can testify to this. I experienced the protective power of the emblem at first hand in many sensitive situations: for example, when we facilitated the evacuation of civilians from besieged rural Damascus, Syria, in 2018; when we went into the besieged city of Taiz, Yemen, in 2017; or over the course of my many visits to the Gaza Strip during or immediately after the intense fighting of 2014 and 2021.

Is it possible to use this reliable and battle-proven emblem in the digital space? Can we find a way to digitally mark the assets, services and data of medical and humanitarian operations? How can we ensure that concepts and solutions derived from international humanitarian law keep pace with technological developments? And how do we make sure that in future everyone operating in cyberspace knows that computers marked with a 'digital emblem' serve an exclusively medical or humanitarian purpose and must not be attacked? Every hospital IT system that is spared disruption, and every humanitarian organization that is able to use all its strength to assist and protect victims of armed conflict, requires our collective thinking, efforts, and innovation. We need to bring all relevant stakeholders to the table. In recent years, the ICRC has worked with renowned research institutions, and a diverse group of experts from throughout the world, to explore possible solutions and analyse the benefits and risks associated with a 'digital emblem'. We are proud to share our findings with you – not as a conclusion of this work but as a basis on which we can build collectively.

I invite you – states, members of the Movement, IT experts working in the medical, humanitarian, military, and security sectors, and internet organizations – to join the conversation and help us identify concrete and practical ways to protect medical and humanitarian services against harm – online as well as offline.

Robert Mardini
ICRC Director General

EXECUTIVE SUMMARY

As societies digitalize, cyber operations are becoming a reality of armed conflict. A growing number of states are developing military cyber capabilities, and their use during armed conflicts is likely to increase. The ICRC has warned against the potential human cost of cyber operations in armed conflicts, especially as a result of the destruction or disruption of civilian infrastructure by cyber means. In particular, the ICRC has raised concerns about the vulnerability of the medical sector and humanitarian organizations to cyber operations, both having been targeted in recent years. This report focuses on that particular vulnerability and how to address it.

In its quest for concrete measures to operationalize the protection afforded in cyberspace to certain medical and humanitarian entities by international humanitarian law, the ICRC decided to investigate the idea of developing a new signal, digital marker, or other means of identification for the digital assets of especially protected entities, i.e. a 'digital emblem'. The idea and objective of a 'digital emblem' are straightforward: for over 150 years, the distinctive emblems (the red cross and red crescent, and more recently the red crystal) have been used to convey a simple message: in times of armed conflict, those who wear them, or facilities and objects marked with them, must be protected against harm. The obligation of all belligerents to respect and protect medical and humanitarian actors applies online as it does offline.

Since 2020, the ICRC has led a research project – in partnership with the Johns Hopkins University Applied Physics Laboratory (APL) and the Centre for Cyber Trust (CECYT, which is a joint endeavour of ETH Zurich and the University of Bonn) – to explore the technological feasibility of developing a 'digital emblem'. Together with the Australian Red Cross, it also convened a global group of experts to assess the expected benefits and the risks associated with a 'digital emblem', and the key characteristics that a 'digital emblem' would need to present. Participating experts came from diverse professional, geographic and gender backgrounds. They included representatives of tech and cyber-security companies, former government officials, former cyber operators, medical and humanitarian experts in information and communications technology (ICT), experts with backgrounds in criminology and police work, white-hat hackers, and academic scholars.

The research and consultation resulted in the following main takeaways for the ICRC:
In the view of a majority of experts consulted, the benefits expected from a 'digital emblem' tend to outweigh the risks foreseen.

- The main benefit expected from a digital emblem is that it would make it easier for **those conducting cyber operations (hereafter called 'cyber operators')** to identify and spare protected entities by visualizing and operationalizing legal protections in the ICT 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; however, 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 sophisticated operators, and even for those with less advanced capabilities, it is already easy to identify medical or humanitarian organizations in cyberspace; the additional risk of facilitating their targeting of 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 who would otherwise not be able to easily identify these targets.
- 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 domestic laws. A cyber-specific risk that may pose new challenges is the speed, scale and reach that characterizes the ICT environment and might enable new types or a greater magnitude of harmful operations.

A ‘digital emblem’ signals legal protection; thus it cannot be seen as a technical ‘silver bullet’ for resolving the security challenges faced by protected entities in cyberspace.

- Protection against harmful cyber operations requires cyber-security measures to be implemented by each protected entity. A ‘digital emblem’ cannot replace such measures. It could, however, supplement them by signalling that the marked entity enjoys special protection under international law and must be protected against harm.

If developed, a ‘digital emblem’ needs to be easy to deploy, remove, and maintain at scale.

- A ‘digital emblem’ would need to be easy to deploy and maintain at low cost. It will have to be suitable for use and maintenance with minimal resources in places affected by armed conflict throughout the world, bridging linguistic, technological, resource, and cultural differences.
- To be a viable option, it should be capable of integrating into the existing technological environment, and capable also of marking different types of assets, services and data. A ‘digital emblem’ should also be easily removable, as that is crucial for addressing possible security risks. Moreover, it should be adaptable to future technological and infrastructure developments. For example, it would be important to identify a technological solution for marking protected data in a ‘cloud’.
- A ‘digital emblem’ would need to be deployable under the direction of the competent authority of any party to an armed conflict.

If developed, a ‘digital emblem’ needs to be ‘visible’ to and easily identifiable and understood by cyber operators.

- It must be possible for a cyber operator to easily identify the presence of a ‘digital emblem’. Looking for and understanding a ‘digital emblem’ must not be a burden for a cyber operator.
- Operators have 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 cyber operator asks of a system. It needs to be seen early on in an operation and must signal protection unambiguously.
- It should be possible to easily verify the authenticity of a ‘digital emblem’; this is essential for such an emblem to be respected and trusted.

To ensure proper use, and to prevent and prosecute misuse, a ‘digital emblem’ would need to be anchored in law and such law enforced by relevant authorities.

An important strength of the existing distinctive emblems is that their form, function, use, and protection are regulated under international and domestic law, and their misuse prohibited. Different avenues exist for incorporating a ‘digital emblem’ in the international legal framework, such as:

- a new Protocol additional to the Geneva Conventions, to recognize and regulate a ‘digital emblem’, like the approach taken in 2005 to establish the red crystal emblem
- 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), an avenue last pursued by states in 1993.

Irrespective of which avenue is adopted at the international level, it would need to be incorporated in domestic law and enforced by national authorities.

THE WAY FORWARD

Based on the research and consultations conducted as part of this project, the generally positive feedback received from the international group of experts, and the unanimous encouragement of the International Red Cross and Red Crescent Movement (Movement) "to continue researching the technical feasibility of a digital emblem … and assess the benefits of such an emblem",[1] the ICRC will continue research and consultation on a possible 'digital emblem'. This will require further work on the technical development, validation and verification of possible solutions (notably of those proposed by the APL and the CECYT) and consultations with all relevant stakeholders – in particular, states, National Red Cross and Red Crescent Societies (National Societies), and internet organizations.

[1] See Council of Delegates of the International Red Cross and Red Crescent Movement, Safeguarding Humanitarian Data (resolution), CD/22/R12.

INTRODUCTION

As societies digitalize, cyber operations are becoming a reality of armed conflict. The number of states developing military cyber capabilities continues to grow, and it is expected that the use of these capabilities during armed conflict will increase.[2] In recent years, the ICRC has raised concerns about the vulnerability of the medical sector to cyber operations.[3] This risk exists at all times, but is particularly acute in times of armed conflict, when functional medical systems and infrastructure are needed most. Similarly, as the ICRC – and other components of the International Red Cross and Red Crescent Movement – continue to expand digitalization of their systems and operations, there is a real risk that they too may fall victim to hostile cyber operations: in fact, they already have.[4]

Against this background, the ICRC has, in recent years, discussed with cyber-security experts whether and how the internationally recognized symbols of protection for armed forces' medical and religious services, authorized medical units, transports and personnel, and certain humanitarian actors in armed conflict – namely, the distinctive red cross, red crescent and red crystal emblems – could be reflected in the information and communications technology (ICT) environment. In the quest for concrete measures to strengthen the protection afforded to these entities, the idea of developing a new signal, digital marker, or other means of identification in cyberspace[5] (hereafter, 'digital emblem') emerged.

Since 2020, the ICRC has led a research and consultation project[6] – in partnership with the Johns Hopkins University Applied Physics Laboratory (APL) and the Centre for Cyber Trust (CECYT, which is a joint endeavour of ETH Zurich and the University of Bonn) – to explore the technological feasibility of developing a 'digital emblem'. First, the research focused on technical means to mark and identify the digital assets, services and data of protected entities, militaries, and other relevant actors in a manner that takes their behaviour and operations into account'.

Second, the ICRC, together with the Australian Red Cross convened a global group of experts to assess the potential benefits and risks associated with a 'digital emblem', in order to enable the ICRC to make an informed decision on whether or not to recommend to states that they further consider the idea. Expert consultations were conducted over a period of three months, bringing together 44 experts from 16 countries. Participating experts came from diverse professional, geographic and gender backgrounds. They included representatives of tech and cyber-security companies, former government officials, former cyber operators, medical and humanitarian ICT experts, experts with backgrounds in criminology and police work, white-hat hackers, and academic scholars. Consultations were conducted in two plenary meetings, seven consultations in smaller groups, and a number of bilateral discussions.

[2] See UN Open-Ended Working Group, *Final Report*, 2021, para. 16; UN Group of Governmental Experts, *Final Report*, 2021, para. 7.

[3] ICRC, *The potential human cost of cyber operations*, 2018. Echoing this concern, see also *Call by global leaders: work together now to stop cyberattacks on the healthcare sector*, Humanitarian Law & Policy Blog, 2020.

[4] See ICRC, *Cyber-attack on ICRC: What we know*, 2021.

[5] In this report, the terms 'cyberspace' and 'ICT environment' are used interchangeably.

[6] This project has been publicly explained in Rodenhäuser et al, Signaling legal protection in a digitalizing world: a new era for the distinctive emblems? Humanitarian Law & Policy Blog, 2021.

The technological research (stage 1) and the expert consultations (stage 2) both aimed at:

- examining the concept of a ‘digital emblem’ from operational, technical, legal, military, humanitarian and policy perspectives
- better understanding the potential benefits, risks and challenges associated with a ‘digital emblem’
- identifying the characteristics of a potentially effective ‘digital emblem’
- examining different technical solutions for devising a ‘digital emblem’.

This report draws on the research, analysis, consultations and discussions – during both stages of the project – that was carried out by or took place between the ICRC, researchers at the APL and CECYT, the Australian Red Cross, and the group of experts. It aims to give a balanced account of the different views that were expressed on the concept and necessary characteristics of a ‘digital emblem’, and the benefits and risks associated with it. The report was prepared jointly by the ICRC and the Australian Red Cross; the annexes were prepared by the CECYT and the APL. Thus, the findings and recommendations presented do not necessarily reflect the views of research partners or participating experts.

Chapter 1 of the report introduces the concept of ‘distinctive emblems’ under international humanitarian law (IHL), and the idea of a ‘digital emblem’. Chapter 2 discusses the main benefits, risks, and challenges associated with a ‘digital emblem’, which were identified primarily through a series of consultations with a global group of multidisciplinary experts. Chapter 3 presents desirable operational and technical characteristics for a ‘digital emblem’. Chapter 4 contains an initial assessment of the technical solutions considered thus far. Chapter 5 summarizes the main findings and presents possible next steps.

CHAPTER 1

THE DISTINCTIVE EMBLEMS: IDENTIFICATION AND PROTECTION DURING ARMED CONFLICT

In times of armed conflict, the red cross, red crescent and red crystal signal specific legal protection for certain medical and humanitarian entities.[7] Distinctive emblems have been used for over 150 years; a widely accepted legal and policy framework regulates their form, function, use, and protection.

Ideally, a 'digital emblem' would integrate into the existing framework – that is, its functions, employment, and use should correspond to those defined in IHL for the existing distinctive emblems. The following sections present an overview of the legal and policy framework in which a 'digital emblem' could function.

THE LEGAL FRAMEWORK

What is the purpose of the distinctive emblems?

A core rule of IHL is that during armed conflict the wounded and sick, and those who tend to them – authorized medical and humanitarian personnel, and their facilities, units and transports – must be respected and protected at all times. The obligation to respect and protect medical and humanitarian personnel and facilities extends to cyber operations conducted within the context of an armed conflict.[8]

The distinctive emblems – the red cross and red crescent, and more recently, the red crystal – were created as signs of protection during armed conflict for armed forces' medical and religious services and for authorized civilian medical personnel, units and transports. The emblems are the visible expression of their protection under IHL. The legal protection provided to those displaying the emblem lawfully is significant: entities displaying a distinctive emblem must be respected and protected. Moreover, it is a war crime to "intentionally direc[t] attacks against buildings, material, medical units and transport, and personnel using the distinctive emblems of the Geneva Conventions [of 1949] in conformity with international law".[9]

The emblems also symbolize the neutral, impartial and independent humanitarian action of the components of the International Red Cross and Red Crescent Movement (the Movement).[10]

These purposes and uses of the distinctive emblems are established by the Geneva Conventions of 1949 and their Additional Protocols of 1977 and 2005, which provide a comprehensive legal framework covering who – and under what conditions and circumstances – is entitled to use the emblems.

[7] There is also the distinctive emblem of the red lion and sun. This emblem has, however, not been used since 1980.

[8] ICRC, *International humanitarian law and cyber operations during armed conflicts*, 2019; UN Group of Governmental Experts, *Final Report*, 2021, para. 71(f).

[9] Articles 8(2)(b)(xxiv) and 8(2)(e)(ii) of the Rome Statute of the International Criminal Court.

[10] The International Red Cross and Red Crescent Movement consists of the International Committee of the Red Cross, the International Federation of Red Cross and Red Crescent Societies and all National Red Cross and Red Crescent Societies.

Practical use case of the distinctive emblems

During an armed conflict between the countries of Boronia and Banksia, two Boronian F-15 fighter planes fly towards a pre-planned military objective. What the pilots do not know, however, is that operational planners have identified the wrong target. Instead of the military warehouse they thought they were targeting, the fighter planes' pilots are heading towards a hospital in Banksia, an establishment serving a community of 55,000 people.

The pilots reach their objective, and prepare to drop their guided munitions according to the pre-planned target list. Just before they do so, one pilot notices, on the head-up display in her cockpit, that the assigned target has something painted on its roof: a large red cross on a white background, about ten square metres in size. She knows that under international humanitarian law, medical establishments are protected from attack, and that the red cross is a sign of that protection. She immediately aborts the attack.

What form do the distinctive emblems take?

Under IHL, the distinctive emblems take the physical form of a red cross, red crescent or red crystal on a white background. The distinctive emblems must be affixed to or displayed by or on protected persons, objects or facilities to express, visually, the protection accorded to them.[11]

IHL also foresees the possibility of using 'distinctive signals', including lights, radio or electronic signals to indicate that an entity is protected.[12]

Who may use the distinctive emblems?

The following entities are permitted to use the emblems to signal the specific legal protection afforded them by IHL during armed conflict (i.e. 'protective use' of the emblems):

- medical services of armed forces
- religious personnel and chaplains attached to armed forces
- civilian medical units and transports, subject to the authorization of the competent authority (a state or possibly an 'armed group' during an armed conflict).
- the ICRC and the International Federation of Red Cross and Red Crescent Societies (International Federation)
- National Societies placed at the disposal of the medical services of armed forces, or assigned to them.

These entities (hereinafter 'protected entities') are permitted to use the emblem, but are not obliged to do so. Their legal protection against harm is derived from IHL and is not dependent on displaying the distinctive emblem; in other words, protected entities do not forfeit their legal protection even when not displaying the emblem or while removing it.

In peacetime, armed forces' medical services may display the distinctive emblems as a preparatory measure, to ensure that they are in place if or when a conflict breaks out. Moreover, components of the Movement may use the emblem to identify their units, transports, personnel and volunteers. This is known as 'indicative use' of the emblems.[13]

[11] See articles 38-44 Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, 12 August 1949 (First Geneva Convention); article 18 Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977.

[12] See articles 6-9 Annex I to Protocol Additional I to the Geneva Conventions of 1949 : Regulations concerning identification, as amended on 30 November 1993.

[13] When used as an indicative device, the emblem must always be displayed together with the name or the initials of the Movement component concerned and in small dimensions.

Who is responsible for enforcing the legal framework regulating the use of the distinctive emblems?

No single authority is entrusted to regulate, monitor and/or enforce the use or misuse of the emblems throughout the world. It is each state's responsibility to regulate the use of the emblems under domestic law, prevent and suppress misuse, and enforce the protections due to the emblems, both in peacetime and during armed conflict.[14] For that purpose, many states have adopted comprehensive laws on the use of the distinctive emblems and on their protection, or incorporated related legal norms in domestic law and regulations that include penalties for misuse.[15] National Societies and/or the ICRC may help states to fulfil this duty.

A POSSIBLE 'DIGITAL EMBLEM'

As the distinctive emblems were conceived of for use in the physical domain, no distinctive emblem (or distinctive signal) exists in the digital domain. The idea of adapting protective emblems or signals to technological progress, however, is not new: IHL foresees, and states have made use of, possibilities for introducing new means of identification in the form of 'distinctive emblems' or 'distinctive signals' – namely light, radio or electronic signals – to indicate that an entity enjoys specific protection under IHL.[16]

A 'digital emblem' could – in pursuit of the same protective purpose as the display of the distinctive emblems in their physical form – become an additional component in the identification and protection of medical and certain humanitarian actors during armed conflict. Over the past decade, this idea has been discussed repeatedly by academic experts and by the ICRC.[17]

Practical use case of a 'digital emblem'

In the armed conflict between the countries of Boronia and Banksia – mentioned earlier – Banksia has started developing malware that spreads automatically and affects logistical software used by Boronia to manage its military supplies. While conducting reconnaissance, the Banksian cyber command discovers that the targeted software is more commonly used than previously thought, including in systems marked by a 'digital emblem'. Upon further investigation, the operators realize that these systems belong to a hospital.

The Banksian cyber command knows that distinctive emblems and signals are signs of protection. Having been alerted to the use of the software by medical units, thanks to the 'digital emblem' and effective reconnaissance, the commander directs programmers to review procedures and program cyber capabilities with a view to ensuring that no harm comes to systems marked by a 'digital emblem'.

[14] See articles 53–54 First Geneva Convention.

[15] For an overview of such laws, see ICRC, National Implementation of IHL, at https://ihl-databases.icrc.org/applic/ihl/ihl-nat.nsf/vwLawsByCountry.xsp?xp_topicSelected=GVAL-992BU8.

[16] See Annex I to Protocol Additional I to the Geneva Conventions of 1949: Regulations concerning identification, 6 June 1977 (as amended in 1993).

[17] See, for instance, Rauscher and Korotkov, *Working Towards Rules for Governing Cyber Conflict: Rendering the Geneva and Hague Conventions in Cyberspace*, EastWest Institute, 2011, pp. 30–31; Pilyugin, *Problems of creating technical means to control compliance with the emerging norms of international law for cyberspace*, Eighth International Forum "Partnership of State Authorities, Civil Society and the Business Community in Ensuring International Information Security," 2014; Sutherland et al, The Geneva Conventions and Cyber-Warfare, 160 The RUSI Journal 2015; ICRC, *International Humanitarian Law and the Challenges of Contemporary Armed Conflict*, 2015, p. 43; ICRC, *The potential human cost of cyber operations*, 2018, pp. 4041; ICRC, *Avoiding Civilian Harm from Military Cyber Operations During Armed Conflicts*, 2021, pp. 27–28; Adriano Iaria, *Digital Emblems: The Protection of Health Care Facilities in the Cyber Domain in the Age of Pandemics*, Opinio Juris, 2020.

Ideally, a ‘digital emblem’ would enable the marking or identification in cyberspace of a variety of digital components used by protected entities, such as:

- electronic assets – for instance, servers, computers, smartphones, IoT devices, and network devices – used by protected entities,
- digital services used by protected entities (e.g. an FTP server to store documents and VPN, a technical service to manage electronic devices remotely),
- data of protected entities that are stored on IT equipment/servers/clouds (such as data stored in a commercial cloud), which can include sensitive medical or personal data
- communication (data transfer) between protected devices and servers (such as communications between an ambulance and a hospital or between an ICRC delegate and headquarters).

If a new signal or ‘digital emblem’ is developed, it may be necessary to amend existing treaties to incorporate that new digital marker in the existing legal framework.

No technical solution has been found so far to meet these purposes and the additional requirements presented in this report. However, the ICRC – together with its partners – has studied a number of technical solutions that could be pursued (see Chapter 4 and Annexes 2 and 3).

At a glance: key points to understand the idea of a ‘digital emblem’

What would a ‘digital emblem’ do?

A ‘digital emblem’ would identify the digital components (assets, services, and data) of protected entities. It would signal that under IHL these entities must not be targeted and must be protected against harm. It would not provide any other cyber defence or security, and would signal protection only against disruption and destruction.

Who could use a ‘digital emblem’?

A ‘digital emblem’ could be used by authorized medical and humanitarian actors. The use of distinctive emblems or signals is regulated by international and domestic law. The use of a ‘digital emblem’ would be permitted solely for marking infrastructure or entities that enjoy specific protection and are entitled to use the distinctive emblem under IHL.

When could a ‘digital emblem’ be used?

The distinctive emblems are used in times of armed conflict to signal specific protection of certain medical and humanitarian entities under IHL. Thus a ‘digital emblem’ is not envisaged to mark medical and humanitarian facilities outside the context of armed conflict (except as a preparatory step to ensure protection once conflict breaks out). Note, however, that members of the Red Cross and Red Crescent Movement may use the emblem for indicative purposes (i.e. for identification, not for signalling legal protection) at all times.

How could a ‘digital emblem’ be developed?

As of 2022, no ‘digital emblem’ has been developed. It is the prerogative and responsibility of states to incorporate any additional distinctive emblems or signals in IHL. Thus the need for a ‘digital emblem’, the technical form it should take, and the framework of its deployment would need to be agreed upon by states.

CHAPTER 2

ASSESSING THE BENEFITS, RISKS, AND CHALLENGES ASSOCIATED WITH A ‘DIGITAL EMBLEM’

The objective of a ‘digital emblem’ is clear and simple: identify, and thereby protect, the assets, services and data of authorized medical and humanitarian actors in times of armed conflict. The ‘digital emblem’ signals legal protection; it does not otherwise contribute to defending the marked entities.

Therefore, a ‘digital emblem’ cannot be seen as a “technical silver bullet” for resolving the security challenges faced by protected entities in cyberspace. To protect itself against harmful cyber operations, every protected entity must implement its own cyber-security measures. A ‘digital emblem’ cannot replace such measures, but could supplement them by signalling that the marked entity enjoys specific protection under international law and must be spared from harm and protected against it. However, the use of a ‘digital emblem’, even if it is respected, would not necessarily provide protection against all kinds of harm: in times of armed conflict there is a risk of incidental damage to medical or humanitarian operators. For example, while parties to conflict must respect and protect hospitals and take constant care not to harm them, it is not necessarily an IHL violation if a clearly marked hospital were to suffer some collateral damage during an attack on a nearby military objective. Moreover, protected medical facilities depend on other infrastructure, such as water or electrical systems; and unlike medical facilities, such infrastructure cannot generally be marked with a distinctive emblem and may be at risk of being targeted.

A key takeaway from the research and consultation process is the conclusion reached by most experts that the idea of a ‘digital emblem’ is important and worthwhile. Based on the research and consultations, a number of key considerations were identified, regarding:

- the expected benefits of a ‘digital emblem’
- the potential risks associated with the use of a ‘digital emblem’
- the key challenges for operationalizing a ‘digital emblem’.

This chapter and Chapter 3 – which summarize the benefits, risks and challenges, and the technical and operational requirements, respectively – aim to present the main issues identified during research and raised by the experts during the consultation process. The objective is to provide a balanced account of the various views expressed on the concept and the necessary characteristics of a ‘digital emblem’, and on the benefits and risks associated with it. Inevitably, the experts and researchers did not agree on all points. Moreover, the list of considerations presented in the report is not exhaustive, and the operational and technical requirements set out here are not the only ways to implement a viable technical solution.

EXPECTED BENEFITS OF A 'DIGITAL EMBLEM'

For a majority of the experts consulted in this project, pursuing the development of a 'digital emblem' was worthwhile. A majority were of the view that the potential benefits of a 'digital emblem' to mark protected assets, services and data outweighed the potential risks.

A 'digital emblem' may strengthen protection

As they do in the physical world, protected entities in the ICT environment face the risk of being targeted or incidentally affected by disruptive or destructive operations: in the ICT environment, this threat originates in cyber operations. A 'digital emblem' aims to signal that medical and humanitarian entities must not be harmed; it has the potential to protect entities from harm caused by the effects of hostile cyber operations. If a 'digital emblem' can reduce the direct or incidental harm to medical and authorized humanitarian actors, even if only by a small proportion, the development and deployment of such an emblem would be a worthwhile initiative, especially in times of armed conflict. Whether or not a 'digital emblem' can provide a net-positive outcome will, however, be context-dependent (i.e. needs to be determined by each protected entity with regard to the context they operate in, the risks they face and their specific vulnerabilities); and any assessment in this connection will need to take into account the risk of the 'digital emblem' being misused (see further discussion below).

A 'digital emblem' may make it easier for cyber operators to avoid harming protected infrastructure

For cyber operators that aim to act in compliance with IHL, and avoid direct targeting or incidental harm to medical or humanitarian digital assets, services or data, a 'digital emblem' would clearly be of benefit, helping them to identify, and spare from attack, protected entities. For instance, it could enable cyber operators to program into malware safeguards aimed at avoiding direct or incidental harm to protected assets, services or data. While many cyber operators are already capable of identifying targets, and therefore generally know what sort of entity they are looking at in the ICT environment, or what type of ICT system the malware they employ will affect, a 'digital emblem' could provide additional help in identifying the digital components of medical and humanitarian entities that must not be attacked. It could help them avoid mistakes in reconnaissance (i.e. to verify that a system belongs to a medical or humanitarian facility) or to correct mistakes in reconnaissance. Moreover, it can be expected that in the future, cyber operations during armed conflict will be conducted at a fast pace and in the 'fog of war', where deceptive tactics may be one way to defend against such cyber operations. In that context, the risk of mistakes increases, and this additional signal can have real added value – just like the physical emblems.

Obviously, the benefit of identifying protected entities more easily, and taking active measure to spare them from harm, applies to parties to armed conflict that aim to operate within the confines of the law. In this respect, experts with a military background emphasized, if it can be expected that the adversary will respect the emblem, there is no reason why the benefits of a 'digital emblem' would be different from those of the physical emblem.[18]

[18] The news website BleepingComputer reached out in 2020 to different ransomware groups asking them if they would stop attacking health organizations during the Covid-19 pandemic. Some of them, like CLOP, DoppelPaymer, Netwalker, or Nefilim stated that they have never attacked certain types of facilities, including hospitals and charities, and will continue to not do so. See Lawrence Abrams, https://www.bleepingcomputer.com/news/security/ransomware-gangs-to-stop-attacking-health-orgs-during-pandemic/ 18 March 2020.

A ‘digital emblem’ would carry over into the ICT environment the signalling of IHL protections by the existing physical emblems

Today, there is consensus among states that international law applies in the ICT environment and that ‘international humanitarian law applies only in situations of armed conflict’.[19] A ‘digital emblem’ could – in step with the ongoing multilateral discussions on the applicability of IHL to cyber operations – be an effective means of carrying over into the ICT environment and making visible the protection that existing rules and principles of IHL provide for authorized medical and humanitarian entities. It could also play a role in adapting the existing rules of IHL to the challenges posed by cyber operations during armed conflict.

Practically speaking, in times of armed conflict, medical and humanitarian operations must be respected and protected. In the past, threats against these operations were exclusively kinetic in nature, such as the wrongful bombing of a hospital. Today, there is also, in addition to these kinetic threats, a growing risk of cyber operations against medical and humanitarian facilities. In light of this evolving threat landscape, signalling specific protection should no longer take place only in physical space (e.g. a red cross, red crescent or red crystal painted on the roofs of buildings), but should be complemented by a digital signal that operates in the ICT environment.

POTENTIAL RISKS ASSOCIATED WITH THE USE OF A ‘DIGITAL EMBLEM’

> Some experts saw greater risks than benefits in the development of a ‘digital emblem’, particularly the possibility of malicious actors intentionally targeting marked entities and misusing the emblem. These risks must be carefully considered in the development and possible use of any technical solution.

The use of the distinctive emblems to signal protected status in times of armed conflict has not only benefits, but, potentially, risks as well. A number of the identified risks in the ICT environment are similar to those that have existed for decades in the physical environment, such as the increase in exposure, misuse of the emblem, and creation of a false sense of safety. These risks could be aggravated by the particular speed, scale and reach that characterizes cyberspace. For instance, marked entities could be targeted from anywhere in the world irrespective of physical distance, or a large number of marked entities could be targeted simultaneously. Such cyber-specific risks are different from the risks in the physical environment.

A ‘digital emblem’ could increase the exposure of medical and humanitarian assets, services and data

One of the main risks associated with the use of a ‘digital emblem’ is the increased visibility, potentially, of medical and humanitarian assets, services and data. This increased visibility could further endanger these assets, services and data by facilitating the creation of lists of “soft targets” that could make targeting by malicious actors easier, or identify marked entities as especially ‘valuable’. The dangers may be even greater in the ICT environment, where the risk of harmful cyber operations against medical and humanitarian facilities has grown in recent years. In cyberspace, digital assets, services and data can be targeted by a variety of actors – including criminals – who are not in physical proximity of the protected objects; this is not the case in the physical world. A related cyber-specific risk is the possibility of attacking marked entities at scale: for example, when a malicious actor is capable of programming malware able or even designed to harm all entities marked with an emblem.

[19] See UN Group of Governmental Experts, *Final Report*, 2021, paras 69 and 71(f). For further discussion on how IHL applies to cyber operations, see ICRC, *International Humanitarian Law and Cyber Operations During Armed Conflict*, Position Paper, 2019.

Facilitating identification and targeting of protected entities is the most prominent risk that experts associated with a 'digital emblem'. Some experts added that the severity of this risk will likely vary, and should be considered in relation to the different threat actors. In the ICT environment, there are already many different ways to identify and classify digital assets, services and data. More sophisticated operators normally have the capabilities to identify medical and humanitarian digital assets, with or without the 'digital emblem'; a 'digital emblem' may not significantly facilitate their task, and therefore not significantly increase the risk if they have ill intent. In contrast, use of a 'digital emblem' might risk greater exposure to operations by less sophisticated actors.

It should be recalled that the risk to protected entities, of being targeted, exists not only in the ICT environment but also in the physical world. To address this, states have made it a war crime to 'intentionally direct attacks against buildings, material, medical units and transport, and personnel using the distinctive emblems of the Geneva Conventions [of 1949] in conformity with international law'.[20] If a 'digital emblem' were to become part of the international legal framework, this rule would **afford protection against cyber attacks as well**.

Unauthorized actors could misuse the 'digital emblem' or appropriate it for perfidious purposes

For as long as the 'distinctive emblems' have existed, states, non-state actors and individuals have sporadically misused them to feign protected status under IHL. The risk of such unlawful conduct would also exist within the context of ICT operations. Anyone could misuse the 'digital emblem' to falsely claim protection under IHL, in the hope of being spared from attack (for instance, by storing military data on a server marked with the emblem or by operators routing operations through facilities showing the emblem, pretending that an operation originated in a medical or humanitarian entity). A 'digital emblem' could also be misused for perfidious operations (such as using the emblem to cover an offensive or criminal operation). Moreover, depending on the technical characteristics of the solution chosen to potentially develop a 'digital emblem', it may also be technically feasible to unlawfully deploy a 'digital emblem' in a broad range of unprotected digital assets, which would undermine the emblem's ability to signal any protection. These different kinds of misuse would not only undermine the credibility and protective value of the 'digital emblem', but would also put medical and humanitarian actors at risk of targeting.

In contexts in which medical facilities are the target of kinetic strikes in violation of IHL, or medical personnel unlawfully persecuted, the use of a 'digital emblem' in medical devices or data would risk facilitating the identification and tracking of medical facilities and personnel.

In fact, many of these risks have existed for decades and are addressed in existing rules of IHL and in the domestic law of many states. For example, under domestic and international law only specific entities (see section 1 above) are authorized to use the distinctive emblems: all other use is prohibited. Moreover, IHL prohibits the killing, injuring, or capturing of an adversary by resort to perfidy.[21] Misusing the emblem in a perfidious manner constitutes a war crime.[22] These legal frameworks would need to be built on and adapted to address potential misuse in the ICT environment.

[20] Articles 8(2)(b)(xxiv) and 8(2)(e)(ii) of the Rome Statute of the International Criminal Court.

[21] Under IHL, perfidy is defined as the misuse of a distinctive emblem to invite the confidence of an adversary to lead them to believe they are entitled to, or they are obliged to grant, protection under the rules of IHL, with intent to betray that confidence. See article 37(1) Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977.

[22] See article 8(2)(b) of the Rome Statute of the International Criminal Court.

A 'digital emblem' could create a false sense of safety and protection or give a false impression that unmarked entities are not protected

Protecting medical and humanitarian entities against hostile cyber operations first requires the taking of concrete cyber-security measures. A 'digital emblem' can only be an additional measure to signal legal protection; it cannot replace other cyber-security actions. This is also clear from the use of the distinctive emblems in the physical world: often, a medical facility or a building housing a humanitarian organization will be protected by sandbags or other means, while also being marked by a distinctive emblem.

Because ICT security requires investment and expertise, there is a risk that some entities might opt to rely entirely on a 'digital emblem' instead of taking other basic security measures. Thus the 'digital emblem' could create a false sense of protection or security. As the possibility cannot be excluded that malicious actors may use a digital emblem to target protected entities at scale, a 'digital emblem' cannot obviate the need to have adequate cyber-security measures in place.

Several measures can be taken to address and overcome this risk, such as clear communication that the 'digital emblem' has only an *added* value, concrete advice on the cyber-security measures that should be taken irrespective of whether an emblem is used, or offering to build capacities in cyber security for medical and humanitarian entities.

It is also essential to underline that the absence of a distinctive emblem does not necessarily indicate an absence of protection or suggest that an entity does not enjoy specific protection under IHL. There is a risk that cyber operators could become negligent in implementing their obligation to verify the lawfulness of a target: they might probe only for a 'digital emblem', and might wrongly equate the absence of such an emblem with an absence of legal protection. This, however, is not a cyber-specific risk or challenge. In fact, the distinctive emblems – including, potentially, their digital versions – can only be the *expression* or *signal* of a specific legal protection; they do not create the legal protection. The protection exists regardless of whether any emblem is displayed. In times of armed conflict it is prohibited – and is a war crime – to attack a hospital, irrespective of whether the hospital displays an emblem; and it is prohibited also to attack civilian buildings that are not hospitals and therefore may not display any emblem. Under IHL, operators have an obligation to 'do everything feasible to verify that the objectives to be attacked are neither civilians nor civilian objects and are not subject to specific protection but are military objectives'.[23]

KEY CHALLENGES FOR THE OPERATIONALIZATION OF A 'DIGITAL EMBLEM'

Digital components and data storage of protected entities are often intermingled with non-protected networks or data

In the ICT environment, networks and storage space are often shared, and many entities are increasingly moving to cloud-based options for applications and data storage. This may pose a number of challenges for the effective use of a 'digital emblem'.

First, an ideal solution should be able to mark the data of protected entities, and only those, in a shared storage space such as a cloud. This would enable an operator to spare the marked applications or data from attack, or malware to be programmed to that end. Conversely, a 'digital emblem' must not be used to mark an entire cloud or server as protected (as one or both may also host military data and may therefore be subject, potentially, to lawful attacks), unless it is used exclusively for medical or humanitarian purposes. Blanket use of the emblem, which does not allow for such differentiation, would risk undermining the protection it ought to signal.

[23] Article 57(2)(a)(i) of Additional Protocol I.

A 'digital emblem' would require measures to create trust and confidence around it

If the 'digital emblem' is misused – or the technology used to display it, compromised – that could undermine the trust on which the 'digital emblem' is based. To ensure trust, any 'digital emblem' would need to be developed in a neutral and transparent manner, possibly based on open-source technology that is safe and easy to verify. Moreover, use of the emblem should be regulated in law and misuse prosecuted.

The operating system of certain medical devices cannot be modified

The objective of a 'digital emblem' would be to mark a wide range of digital assets, services, and data belonging to protected entities. In this respect, medical devices present particular challenges. Some medical devices operate on closed-source software that cannot be accessed or modified, either for *physical* reasons (i.e. they cannot be accessed), *regulatory* reasons (i.e. there are compliance, certification or licensing restrictions that do not allow any modification), or *safety* reasons (it requires significant engineering effort to safely change such equipment). As a result, it would not be possible to directly mark existing devices having these characteristics with a 'digital emblem', which means that *certain* technical solutions may not, for now, be usable for medical devices that fall into these categories.

There are various possibilities for overcoming this challenge, such as: designing a 'digital emblem' that may not be needed to mark each medical device but could operate at the network level of a hospital (for example, a proxy server connecting these devices); or working with the manufacturers of medical devices, or standardization authorities, to facilitate the marking of these devices.

A 'digital emblem' must not only respond to the existing technological environment, but must also be capable of being used in, or adapted for, future infrastructure and development

Technology is developing fast; thus it is essential that a 'digital emblem' be capable of use in, or easy adaptation to, future internet infrastructure and development. It is generally recognized that devices with simple infrastructure, such as IoT devices, will be widely used by medical actors in the future, to such an extent that it might become difficult for medical or humanitarian entities to keep track of all devices in use. Thus a 'digital emblem' would have to be capable of identifying large numbers of devices or networks simultaneously, for instance, through installation at a proxy level to signal protection of all connected devices; in other words, it would need to be usable on a large scale.

Moreover, internet infrastructure is evolving. For instance, Internet Protocol (IP) addresses are moving from IPv4 to IPv6. Designing a 'digital emblem' would need to take into account foreseeable changes in internet infrastructure and be suitable for future use.

Ensuring the protective value of the digital emblem

Medical and humanitarian facilities have become the target of deliberately harmful operations (such as ransomware attacks and data breaches) or are incidentally affected by malware spreading indiscriminately. To prevent protected medical or humanitarian entities from incidental harm, a 'digital emblem' should be based on a technical solution that enables cyber operators to easily programme malware not to harm entities marked by the emblem.

CHAPTER 3

OPERATIONAL, TECHNICAL AND LEGAL REQUIREMENTS FOR THE DEVELOPMENT OF A ‘DIGITAL EMBLEM’

Experts and researchers emphasized that any ‘digital emblem’ should be developed with two things in mind: the users of such an emblem and the harm that is to be prevented. Moreover, due regard should be given to the types of cyber operation that are common in armed conflict, and the strategies and tools that operators normally use when identifying and attacking targets. Taking these points into account, as well as the benefits, risks and challenges presented in Chapter 2, a number of operational and technical requirements were identified as relevant to the development of a ‘digital emblem’. For this report, they have been categorized as:

- operational and technical requirements to enable use by protected entities
- operational and technical requirements to enable cyber operators to notice the ‘digital emblem’
- preparatory and legal requirements for a ‘digital emblem’.

As noted above, these operational and technical requirements are neither exhaustive nor mandatory for a viable technical solution. However, as these requirements were distilled from discussions with a diverse group of global experts, they should be taken into account in any evaluation of potential technical solutions.

OPERATIONAL AND TECHNICAL REQUIREMENTS TO ENABLE USE BY PROTECTED ENTITIES

> The overwhelming view of experts was that a ‘digital emblem’ had to be easy to deploy, remove, and maintain at scale. This requirement is closely linked to the basic premise that a ‘digital emblem’ can offer protection only if it is used by authorized medical and humanitarian entities.

Ease of deployment, removal and maintenance by protected entities

Medical and humanitarian operations during armed conflict are complex, at times conducted rapidly with limited means, and in environments with only basic infrastructure. Moreover, ICT support during armed conflict is most often limited and with only minimal resources at its disposal. Infrastructure is usually ad hoc in nature and may be outdated, legacy hardware is generally the rule, and asset discovery and management are often difficult. In addition, as armed conflicts occur in all parts of the world, variations in ICT expertise – particularly in medical facilities and humanitarian organizations – must be expected. Thus a ‘digital emblem’ would need to be deployed and maintained at low cost to allow use by a variety of protected entities. For instance, if a ‘digital emblem’ requires complex software that is easy to deploy but requires significant hands-on maintenance, it may not be a workable solution. This challenge is aggravated by the expanded use of connected devices in medical and humanitarian operations, which makes it necessary that any solution be easily deployable at scale.

Therefore, the more complex a ‘digital emblem’ is, and the more difficult it is to deploy and to maintain, the less likely it is to be used. As usability is key to success, a ‘digital emblem’ must burden operational personnel as little as possible. Ideally, a ‘digital emblem’ should be deployable from a capital, main office or headquarters, or require minimal technical knowledge of personnel in operational environments. In addition, capacity building – and, potentially, substantial technical support – might be required to allow deployment throughout the world and by ICT experts from the medical and humanitarian sectors.

Moreover, a ‘digital emblem’ must be easily removable. This would enable a protected entity to choose – as with the physical emblem – whether to use the ‘digital emblem’, based on developments in the environment and circumstances in which they are operating. Ease of removability could be one way of addressing possible risks associated with use of the ‘digital emblem’. Protected entities must be aware, however, that past use of the emblem can be recorded and its removal may not eliminate all traces or record of that use, very much like the case in the physical domain.

To increase the likelihood of a ‘digital emblem’ being easy to deploy, maintain and remove, it may be advisable for a technical solution to leverage existing and commonly used technologies.

A ‘digital emblem’ should be able to protect a broad range of devices

Digital assets, data, and communication by protected entities can take different forms, rely on different types of infrastructure, and require different technical solutions for identification and protection. It is therefore unlikely that reliance on any one way of identifying protected entities, such as the use only of an ‘IP-based’ solution or a ‘file-based’ solution, will make it possible to identify the full range of assets belonging to protected entities.

To address this challenge, it may be necessary to employ a combination of techniques to identify protected entities. This, however, risks limiting the protective effect that an emblem might have. A ‘digital emblem’ would need to be easily identifiable and understood by operators and not impose undue burdens. If different solutions are used alternatively (sometimes one solution and sometimes another), the risk would be that cyber operators might not check all possible ‘digital emblems’ and therefore miss the protective signal.

Moreover, given the large – and in all likelihood, increasing – number of digital (or digitally connected) assets used in the health-care and humanitarian sectors, the deployment of a ‘digital emblem’ may not be viable if it has to be placed on each asset or piece of equipment. A ‘digital emblem’ might need to be deployable at the network level of a protected entity. This, however, would need to be done cautiously, to ensure that only devices that enjoy specific protection are connected to a network marked with a ‘digital emblem’.

A ‘digital emblem’ would need to be deployable under the direction of the competent authority of any party to an armed conflict

Both state and non-state parties are involved in many of the armed conflicts going on now. Both sides in a conflict may have medical facilities used by their fighters or armed forces, or exercise authority over medical facilities under their control. Under IHL, all parties to a conflict are, in principle, permitted to use or authorize the use of the distinctive emblem. Thus, a possible solution should not be one that is accessible only to states or that requires a state’s permission to use.

OPERATIONAL AND TECHNICAL REQUIREMENTS TO ENABLE CYBER OPERATORS TO NOTICE THE 'DIGITAL EMBLEM'

As the obligation to respect it rests – in practice, and of necessity – primarily with the cyber operators of parties to armed conflicts, experts with operational experience, in particular, emphasized that a 'digital emblem' needs to be easily identifiable by, 'visible' to and understood by them. Looking for a 'digital emblem' must not be a burden or identify an operator as a potential attacker.

A 'digital emblem' should be easily identifiable, 'visible' to and understood by cyber operators

The purpose of a 'digital emblem' is to signal to cyber operators – at times in the heat or the fog of war – that certain entities enjoy specific protection under IHL and must not be targeted. Such an emblem would therefore need to be clearly visible to enable easy identification by cyber operators or the malware they are using.

To this effect, and like in the 'physical emblem', a 'digital emblem' would need to be:

- obvious and easily visible, meaning that a cyber operator would not have to put a great deal of time and effort into identifying, or programming malware to identify and spare, a 'digital emblem'. Ideally, it should be found in a place or process that any operator (or malware) would routinely check, meaning that verifying the presence of a 'digital emblem' should not be a burden for the operator. One option might be to make the 'digital emblem' visible on the process list, meaning that when an operator is checking the active processes they will see the emblem.
- easily identifiable by cyber tools (malware, script) to allow programmers to exclude marked entities from the range of targets, for instance, by including a 'white list' of protected IP addresses or a specific process name.
- clearly identifiable, meaning that the 'digital emblem' should not get lost in the noise of internet traffic. Its design should be such as to prevent operators from claiming that they did not notice it.
- clearly understood, meaning that the operator who is confronted with the 'digital emblem' would be able to understand what the signal is, irrespective of the language the operator speaks or their geographic or cultural background.

A 'digital emblem' must be trustworthy. It should be possible for cyber operators and authorities to verify the authenticity of a 'digital emblem'

In light of the risk that a 'digital emblem' might be misused to falsely mark entities that are military in nature or otherwise not authorized to display the distinctive emblem, and to ensure that trust in the emblem is not undermined, it is important that cyber operators are able to verify the validity of a 'digital emblem'. There are a number of different technological solutions to help ensure authenticity and trustworthiness, such as:

- an *a priori* authorization for the use of an emblem by a relevant authority. This would be the case, for example, if an IP-based solution is used, under which a protected actor would have to request and obtain from an authority an IP number that signals protection (see domain-name-system (DNS)- and IP-based emblems, Chapter 4 and Annex 2).
- a system of certification and endorsement under which protected entities would signal their protection by means of certificates endorsed by a trustworthy authority, such as a national or international authority (see ADEM, Chapter 4 and Annex 3). A number of technical solutions may be considered to address the risk of forged certificates or the leaking of private keys, such as short-lived certificates or a revocation system.

As emphasized below, such verification must be simple and must not identify an operator to a protected entity as a potential threat actor.

Probing for a 'digital emblem' must not identify a cyber operator as a potential threat actor

Cyber operators will check for a 'digital emblem' during reconnaissance operations only if that will not identify them as potential threat actors. In other words, if cyber operators are concerned that probing for a 'digital emblem' will identify them, they will not probe for it. This risk of 'discovery' will become particularly acute if the operator has to send a request for a specific file to verify the presence of a 'digital emblem'. In addition, a 'digital emblem' cannot function as a honeypot:[24] probing for an emblem must not be disadvantageous to a law-abiding actor.

One possibility for overcoming this challenge might be to include a 'digital emblem' in standard information that is checked so frequently that probing for a 'digital emblem' will not excite suspicion in the protected entity. Moreover, if a DNS- or IP-based solution is used, it might be possible to verify whether a domain name or IP address belongs to a protected entity by means of a list provided by a neutral third party, which anyone could access and verify.

In this connection, it must be recalled that a distinctive emblem or signal, including a digital one, is a humanitarian sign aimed at strengthening protection for inherently medical and humanitarian missions. While identification of attackers, attribution of operations, and accountability for wrongful acts may all help increase compliance with IHL, it is not the object and purpose of the distinctive emblem to facilitate this.

A 'digital emblem' should be placed at the perimeter or end points and throughout the internal network

The purpose of a 'digital emblem' would be to prevent cyber operations against marked entities. Cyber operations can take place solely at the network level on the victim's perimeter, such as a distributed denial-of-service attack, where the operation consists in saturating the resources or bandwidth of a server so that it is no longer available. To prevent such operations, a 'digital emblem' would need to signal the protection of assets even when the victim's computer network has not been penetrated. It would need to inform the operator or malware that a specific network is protected, even before that network is penetrated.

Cyber operations may also involve penetrating a network. When an operator penetrates the victim's network, it often needs to move laterally within that network to increase its privileges (become an administrator and thus be able to operate with greater 'depth') or reach specific assets within a given network (get access to the active directory or the domain controller). In these cases, the 'digital emblem' must be installed on and distributed directly from the end points of a system (i.e. laptops, desktops, virtual machines, servers, etc.) to signal their protection.

In order to prevent misidentification or incidental harm, and to have a deterrent effect, a 'digital emblem' must be identifiable to a cyber operator at an early stage – ideally, at the perimeter, meaning the external-facing part of a network. This is particularly important because most cyber operations start with a reconnaissance phase, which includes, for example, active scanning or identification of network information, websites, or potential targets. The 'digital emblem' should be identified during this phase. Placing a 'digital emblem' on the external facing part of a network is, however, a double-edged sword: the risk of making protected entities more easily visible to malicious actors in cyberspace is associated primarily with a 'digital emblem' deployed at the perimeter, not inside a network.

[24] A 'honeypot' is a computer security mechanism to detect, deflect, or, in some manner, counteract attempts at unauthorized use of information systems. Generally, a honeypot consists of data (for example, in a network site) that appears to be a legitimate part of the site and contain information or resources of value to attackers but is set up to isolate, monito, and analyse the attacker. (Wikipedia: https://en.wikipedia.org/wiki/Honeypot_(computing). In this case, this refers to the illegitimate use of the 'digital emblem' to identify possible cyber operations.

PREPARATORY AND LEGAL REQUIREMENTS FOR A 'DIGITAL EMBLEM'

Any technical solution for a 'digital emblem' must be tested before it is implemented

A 'digital emblem' does not yet exist and, as shown by this report, technical solutions will have to meet various requirements. There is probably no single solution that meets all the requirements equally well; for example, a solution that is very hard to misuse might also be less easy to deploy. It is therefore important to research, develop, test, and refine possible solutions. It will be important to assess the results of such testing with respect to the viability of any option presented, and the potential benefits and risks associated with it (as identified in Chapter 2).

In addition, and depending on the technical solution, it will be necessary to have discussions with specific authorities: for instance, with the Internet Assigned Numbers Authority (IANA), about the use of dedicated IP numbers; and with the Internet Corporation for Assigned Names and Numbers(ICANN), about the use of dedicated top-level domains (such as '.emblem').

A 'digital emblem' needs to be part of an international legal framework to ensure that it is widely accepted, known, and the rules on its use enforced

An important characteristic and strength of the existing distinctive emblems is that their form, function, use, and protection are regulated under IHL and domestic law. Their misuse is prohibited and in certain circumstances, criminalized, both at the national and the international level. It may be expected that without a regulatory and enforcement system, a 'digital emblem' will be less widely known and rules on its use less likely to be respected. Thus, if a 'digital emblem' is to be introduced, it should become part of the existing international and domestic legal frameworks regulating the use of the distinctive emblems and signals. Such matters as the entities that are permitted to display the emblem and for what purposes, and how to prevent and stop misuse, must be clearly regulated and understood. There are a number of different avenues for adapting the international legal framework, such as:

- **a new Protocol additional to the Geneva Conventions**, which could, like the existing legal framework for the distinctive emblems, recognize a 'digital emblem', define its form and technical details, provide which entities are permitted to use it and for what purpose, and proscribe misuse. This approach was taken to establish the red crystal emblem in 2005;[25] as a new Protocol additional to the Geneva Conventions would be a new international treaty, its development, adoption and worldwide ratification would require significant diplomatic effort.
- **a revision of Annex I of Additional Protocol I**, which includes 'regulations concerning identification', for instance, on the use of 'distinctive signals' (light and radio signals, electronic identification) or communication (radio communication, codes) by protected entities. States developed Annex I of Additional Protocol I specifically in the expectation that technological developments might allow, or necessitate, new means of identifying personnel, material, units, transports and installations protected under the Geneva Conventions and Additional Protocol I. Changes to this Annex can be made under a procedure defined in Additional Protocol I (see Article 98), which is simpler than the development of a new Protocol additional to the Geneva Conventions. States last pursued this avenue in 1993.
- **ad hoc agreements on a 'digital emblem'**, meaning that states, and possibly other parties to armed conflict, may at any time 'agree upon additional or other signals, means or systems which enhance the possibility of identification and take full advantage of technological developments in this field'.[26] This approach might be the most agile and flexible, but it also comes with the challenge of warring parties having to agree on a 'digital emblem' after the onset of armed conflict, and to implement such an emblem while fighting is in progress.

After it has been agreed upon, the success of a 'digital emblem' will require broad dissemination of knowledge and capacity building among protected entities, who are entitled to use the 'digital emblem', and among operators, who must respect it. A 'digital emblem' cannot be expected to function properly if these actors do not have an adequate understanding of it.

[25] Additional Protocol III to the Geneva Conventions, 2005.

[26] Article 1(4) of Annex I to Additional Protocol I.

CHAPTER 4

INITIAL ASSESSMENT OF POSSIBLE TECHNICAL SOLUTIONS

In the first stage of the 'digital emblem' project, the ICRC partnered with researchers at the CECYT and the APL to identify technical means to mark and identify the digital assets, services and data of protected entities (see Annex 2 and 3 for further details).

During the second stage of the project, the various technical solutions proposed by the CECYT and the APL were shared with the experts participating in the consultation process, to facilitate their consideration of the concept of a 'digital emblem'. The experts raised a number of points with respect to each solution: each technical solution was found to have advantages and disadvantages, and to require further study and testing. There was, however, broad agreement among the experts that a combination of technical solutions would be most likely to satisfy all preferred requirements (see Chapter 3) or apply to all relevant digital assets, services and data used by medical and humanitarian entities in times of armed conflict.

Based on the research undertaken so far and the expert consultations, the following points seem pertinent to the technical solutions proposed.

A file-based emblem

This would be an end-point-based 'digital emblem', such as a well-known file, made visible to processes running on the protected system. It would signal protection either simply through the existence of the file or by directives contained within the file.

A file-based emblem is generally easy to deploy by cyber-security personnel on a system-by-system basis. Implementation of a query protocol by cyber operators to notice the file-based emblem is considered easy.

There are, however, disadvantages, such as the necessity of placing such an emblem on individual assets and devices (which can be numerous); in addition, a file-based emblem would be difficult to place on certain restricted medical devices, and its placement could lead to the invalidation of the certification and the licences of such devices. The simplest version of a file-based emblem could also be misused rather easily to mark infrastructure that does not enjoy specific protection. Moreover, a file-based emblem would become visible only after an operator is inside a network (i.e. it would not be visible at the perimeter), and it would not be visible to intermediate networks (i.e. it cannot protect data in transit). The main problem with a file-based emblem is accessibility: cyber operators would need to query each host for the existence of the emblem. If operators have to actively search for the emblem (within a specific file or folder), and run the risk of being discovered while within a network, they may be less likely to check for a 'digital emblem'. The file-based emblem should, therefore, make itself visible.

An example of such a solution would be a file-based emblem that takes the form of a specific process, which is then listed among active processes and can thus be easily identified without impeding an operation.[27]

A DNS-based emblem

A DNS-based emblem would use a special label to associate the ‘digital emblem’ with the domain name (e.g., www.icrc.*emblem*). As long as the domain name is associated only with systems that are eligible for protection by the ‘digital emblem’, it represents a straightforward, human-readable ‘digital emblem’ identifying the protected system.

One advantage of a DNS-based emblem is that domain names are easily understood by both humans and software, and could be easily integrated into the readily accessible global internet infrastructure. A DNS-based emblem would also be of great practical convenience to IT staff of protected entities because it would cover an entire domain and would not need to be placed on each individual asset. Identifying an entity via DNS does not require access to the entity for set-up or the deployment of additional software. Moreover, as an obvious and human-readable sign, such an emblem would be easy to recognize, and early on, by any operator. Given that the distribution of domain names is globally regulated, that global infrastructure could also be leveraged to prevent misuse through *a priori* authorization for those wishing to use it.

Obtaining a DNS-based emblem would, however, require those wanting to employ the ‘digital emblem’ to follow a certain process; it would also involve authorization by entities other than the medical or humanitarian entity that is entitled to use it. The use of a DNS-based emblem would require the establishment of a new top-level domain by ICANN, with IANA’s approval. To operationalize a DNS-based emblem, it would also be necessary to establish an entity in charge of the protected top-level domain and responsible for permitting the protected entity to use the emblem in a timely, impartial and a non-political manner. In addition, it would also have to be possible for a protected entity to use a new DNS signaling protection while still being reachable at the previously used address.

One potential shortcoming of a DNS-based emblem is that its revocation might not be immediately effective. Because of DNS caching, domains can be resolved locally or through intermediate resolvers; a request does not have to be sent to an authoritative name server every time. These local resolutions have a time frame for expiration (‘time to live’). Thus when an emblem (a specific domain name) is revoked, a local resolution will be updated only at the end of the update cycle and not immediately, resolving domains that should in fact no longer be resolved. Another consideration is the security of the DNS, which is, in many quarters, thought to be weak. The DNS did not include security features in the past, but Domain Name System Security Extensions (DNSSEC) signing capabilities using public-key cryptography were developed by the Internet Engineering Task Force. While not used universally, over the last ten years, major DNS service providers including Google, AWS, and Deutsche Telekom have adopted DNSSEC. DNSSEC helps to protect against forged or manipulated DNS data, and therefore against harmful operations like DNS spoofing or DNS-cache poisoning. Thus, the DNS-based emblem could rely on a newly developed multi-party signing capability. There is also this disadvantage associated with the use of a DNS-based emblem: domain names are not transported in data exchanges across the internet and intermediate systems do not query DNS while forwarding traffic.

[27] As normal computer users are using Windows Task Manager as a quick and easy method of viewing what programs, background processes, and apps are running on a computer, cyber operators similarly apply tools to identify what processes are running on a computer.

An IP address-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. That would allow systems anywhere in the Internet to determine whether the systems they probe, or messages traversing the network, are associated with a specifically protected entity. An address-based emblem can be based on IPv4, IPv6, a specific port, or other elements.

The IP address-based emblem provides significant visibility, both at the host level (by software) and at the network level (by router). It could identify assets and data in transit (i.e. communication). As IP addresses are obtained through a global system, that system could also be leveraged to protect an IP address-based emblem against misuse. An IP address-based emblem would also be easy to query for cyber operators, who already implement IP checks. Thus, dedicated subnets could be an option to facilitate implementation and respect by operators.

An IP address-based emblem would build on an existing system that assigns IP addresses; this is comparable to what was said above about a DNS-based emblem. After a dedicated range of IP numbers has been established, the next requirement would be the establishment of an organization to take responsibility for allocating IP numbers to protected entities in a timely, impartial and non-political manner. Once the responsible organization learns that a protected entity no longer enjoys specific protection or identifies misuse, the protected entity's traffic would no longer be routed through the dedicated range of IP numbers. Usually, such changes take effect within 24 hours.

There is, however, concern about how IP addresses are mapped in an environment where they may not be reflective of the end point (i.e. where multiple devices have the same IP address, as in a Network Address Translation (NAT) or in a mobile-phone network). Another disadvantage is that a single network address could potentially host both protected and unprotected services. Thus, it would be mandatory for IP spaces dedicated to signalling legal protection (i.e. a 'digital emblem') to be used only for protected entities. The process for embedding semantics in IP addresses for global use can be expected to be complex and contentious.

An 'Authenticated Digital Emblem' (ADEM)

This solution is based on a distributed approach that leverages certificate chains. To support diverse deployment scenarios, ADEM's scheme has three tiers:

- 'self-signed emblems' that are linked to public keys and can be generated by anyone
- an 'organizational emblem', meaning that self-signed emblems are linked to real-world organizations identified by a domain name
- an 'endorsed emblem', meaning an additional layer of authentication in which such emblems are endorsed by third authorities.

This solution foresees the distribution of the 'digital emblem' in three ways, covering a wide range of use cases and allowing easy identification: the DNS for labeling public and named network entities; the Transport Layer Security (TLS) protocol for confidential network connections; the Internet Control Message Protocol (ICMP) for unnamed network entities, assets, and passive observers of network connections.

Many experts considered the ADEM framework to be considered and elaborate for a 'digital emblem'. It would allow wide distribution by users and easy identification by operators. Moreover, the different layers of authenticity would constitute a system in which at least organizational and endorsed emblems could be trustworthy.

The various ways of distributing an ADEM (DNS, TLS and ICMP) have strengths and weaknesses. Those relating to the use of a DNS-based emblem are discussed above. Distributing the ADEM via TLS might prove effective because many application-level protocols, such as Hypertext Transfer Protocol Secure (HTTPS), are typically served over TLS and could communicate an emblem. A solution using TLS is, however, relatively difficult to implement. Custom TLS extensions might be a possibility for distributing the emblem. Operators would need to adapt their TLS servers in order to distribute emblems. However, to inspect these emblems, TLS clients must also be adapted, which is more challenging than for DNS- or ICMP-based distribution, where independent software clients can be used. Another challenge associated with TLS is the injection of extensions if the protected entity is not the owner of the TLS server. ADEM may also be communicated via other protocols, such as ICMP. Information transmitted over ICMP is, by definition, non-essential; therefore ICMP does not guarantee reliability. Thus an entity should not be labelled only via ICMP when delivery guarantees are required. However, if delivered via ICMP, the certificate would still provide authenticity and could reduce or prevent harmful operations. Distribution via files has the advantages and disadvantages mentioned above in connection with a file-based emblem. In light of the advantages and disadvantages associated with the different modes of distribution, one solution might be to distribute the emblem through a combination of modes.

The ADEM framework also foresees different levels of authenticity through different levels of certificates, which provide different levels of trust. In practice, even small organizations with limited capacities can generate self-signed certificates and thus signal that they are protected parties. The authenticity of such self-signed emblems would, however, be difficult to verify. Those who are required to verify an emblem will be able to choose the authority to which they wish to give credit (i.e. a self-signed emblem, an organizational emblem, or only emblems endorsed by an authority they trust). As 'endorsed emblems' provide the greatest level of trust, a medical facility or Movement-affiliated actor in a context affected by armed conflict should obtain endorsement from the relevant (sometimes *de facto*) authority in that country (which could also be territory under the effective control of a non-state armed group), other belligerent parties, or other trusted authorities (i.e. an international entity recognized by all parties). Where authorities would not endorse valid certificates of protected entities for political reasons, endorsement by other trusted actors could increase trust in the status of the protected party, even without the endorsement of a state.

As the ADEM framework can involve endorsements, one form of abuse, potentially, could be the issuance of fraudulent certificates. To create the – false – impression that such endorsements are issued by national authorities or international entities, an attacker would have to hack such authorities and issue certificates in the name of that authority. Such cyber operations are known to have taken place, including against certificate authorities.[28] A decentralized system of revocation should therefore be considered in order to invalidate fraudulently issued certificates.

There may also be concerns about the possibility of malicious operators hacking the ADEM framework and misusing it. Such an operation would, however, be complex, and there are solutions for an ADEM to limit the scope of such a hack. Consider an operation against a protected entity where the attacker's aim is to steal the protected party's private key and use it to issue an emblem for an entity that would not have the right to use the 'digital emblem', such as a military objective. In this case, one could limit the use of certain keys by tying them to specific IP addresses: thus even if a malicious actor managed to steal a key, they would be able to use it only in combination with the IP addresses of the protected entity.

[28] Examples of such operations are the hack against the Certificate Authority DigiNotar, Comodo.

CHAPTER 5

MAIN FINDINGS AND POSSIBLE NEXT STEPS

The obligation to respect and protect medical personnel and facilities is one of the oldest codified rules of IHL. As cyber operations have become increasingly common in contemporary armed conflicts, and as their use is likely to increase, the need to protect medical and humanitarian entities against cyber operations is becoming more urgent by the day.

There is no 'silver bullet' to ensure effective protection in the ICT environment, but research and consultation have shown that the idea of a 'digital emblem' is worth further study.

Based on the research conducted by the APL and the CECYT, and the series of consultation with a diverse group of multidisciplinary experts, the ICRC has identified the following main takeaways:

In the view of a majority of experts consulted, the expected benefits tend to outweigh the risks.

- A 'digital emblem' would make it easier for cyber operators to identify and spare protected entities in cyberspace by visualizing and operationalizing legal protections in the ICT environment and in the heat of armed conflict (the 'fog of war'). This will primarily enhance protection for marked entities against the risk of harm caused by law-abiding operators; however, 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 sophisticated operators, and even for those with less advanced capabilities, it is already easy to identify medical or humanitarian organizations in cyberspace; the additional risk of facilitating their targeting of 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 who would otherwise not be able to easily identify these targets.
- 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 domestic laws. A cyber-specific risk that may pose new challenges is the speed, scale and reach that characterizes the ICT environment and might enable new types or a greater magnitude of harmful operations.
- To ensure proper use, and prevent and prosecute misuse, a 'digital emblem' must be anchored in law and this law enforced by relevant authorities.

Experts were overwhelmingly of the view that a 'digital emblem' needs to be easy to deploy, remove, and maintain at scale.

- A 'digital emblem' would need to be easy to deploy and maintain at low cost. It will have to be suitable for use and maintenance with minimal resources, in places affected by armed conflict throughout the world, bridging linguistic, technological, resource and cultural differences.
- To be a viable option, it should be capable of integrating into the existing technological environment, and capable also of marking different types of assets, services and data. A 'digital emblem' should also be easily removable, as that is crucial for addressing possible security risks. Moreover, it should be adaptable to future technological and infrastructure developments. For example, it would be important to identify a technological solution for marking protected data in a cloud.
- A 'digital emblem' would need to be deployable under the direction of the competent authority of any party to an armed conflict.

A 'digital emblem' needs to be 'visible' to and easily identifiable and understood by cyber operators.

- It must be possible for a cyber operator to easily identify the presence of a 'digital emblem'. Looking for and understanding a 'digital emblem' must not be a burden for a cyber operator.
- Ideally, a 'digital emblem' should be part of the information that any cyber operator asks of a system. It needs to be seen early on in an operation and must signal protection unambiguously.
- It should be possible to easily verify the authenticity of a 'digital emblem'; this is essential for such an emblem to be trusted and respected.

Ultimately, the litmus test for any 'digital emblem' or other signal of protection will be whether it is used in practice by protected entities to identify their assets, services and data, based on the expectation that it is respected by parties to armed conflicts and will increase protection. As such use is voluntary, it will be the choice of protected entities whether or not to use a 'digital emblem'. This decision will depend, among other things, on the assessment of each actor on whether in a specific environment and context the anticipated protection benefits from using the 'digital emblem' are expected to outweigh the possible risks that its use may entail.

THE WAY FORWARD

Based on the research and consultations conducted as part of this project, the generally positive feedback received from the international group of experts, and the unanimous encouragement of the Red Cross and Red Crescent Movement "to continue researching the technical feasibility of a digital emblem … and assess the benefits of such an emblem',[29] the ICRC will continue research and consultation on a possible 'digital emblem'. This will require further work on the technical development, validation and verification of possible solutions (notably those proposed by the APL and the CECYT) and consultations with all relevant stakeholders, in particular states, National Red Cross and Red Crescent Societies, and internet organizations.

[29] See Council of Delegates of the International Red Cross and Red Crescent Movement, Safeguarding Humanitarian Data (resolution), CD/22/R12.

ANNEX 1

LIST OF EXPERTS CONSULTED FOR THE PROJECT

GLOBAL GROUP OF EXPERTS

EXPERTS PARTICIPATED IN THEIR PRIVATE CAPACITY. PROFESSIONAL AFFILIATIONS AT THE TIME OF THE CONSULTATIONS ARE MENTIONED FOR IDENTIFICATION PURPOSES ONLY AND DO NOT SIGNIFY ENDORSEMENT BY THE INSTITUTIONS FOR WHICH EXPERTS WORK

- **Abdul-Hakeem Ajijola**, Chair, African Union Cyber Experts Group, Nigeria
- **Raphaël Arrouas**, Security Researcher, Switzerland
- **Mark Barwinski**, Global Head of Cyber Operations, UBS, Switzerland
- **Major Gordon Boom**, Previously assigned to U.S Cyber Command, U.S. Air Force, United States
- **Jonathan Bouman**, Medical Doctor and Security Researcher, Netherlands
- **Mr Franck Calcavecchia**, Information Security Officer, Hopitaux Universitaires de Genève, Switzerland
- **Nick Carr**, Lead, Cyber Crime Intelligence, Microsoft, United States
- **Jasmin Craufurd-Hill**, Future Technology Fellow, 3Ai/CDR; Australian Defence College, Australia
- **Oleg Demidov**, Global Internet Governance and Cyber Security Consultant, PIR Centre, Russia
- **Tamas Földesi**, Senior Officer, Information Security, Policies, Quality, International Federation of Red Cross and Red Crescent Societies, Switzerland
- **Thomas Graindorge**, Cyber Legal Adviser, French Cyber Command, France
- **Anastasiya Kazakova**, Senior Public Affairs Manager, Kaspersky, Russia
- **Elizabeth Kolade**, Security Analyst, Defence Space Administration, Nigeria
- **Viktoriia Korzhuk**, Associate Professor, ITMO University, Russia
- **Marina Krotofil**, Cyber Security Product Owner, IoT platform: Connected Vessels, Terminals and Warehouses, A.P. Moller, Maersk, United Kingdom
- **Vineet Kumar**, Global President, Cyber Peace Foundation, India
- **Prof Kwok-Yan Lam**, Professor, School of Computer Science and Engineering; Associate Vice- President (Strategy and Partnerships), Nanyang Technological University, Singapore
- **Vikas Mahajan**, Chief Information Security Officer, American Red Cross
- **Muslim Medzhlumov**, Head of Managed Security Services, BI.ZONE, Russia
- **Jelena Milosevic**, Nurse and Affiliate, I am the Cavalry, Netherlands
- **Viktor Minin**, Chairman, Association of Chief Information Security Officers, Russia
- **Dr Dai Mochinaga**, Senior Researcher, Keio Research Institute; Analyst, JPCERT Coordination Centre; and Lecturer, Chuo University, Japan
- **Adrien Ogee**, Chief Operating Officer, Cyber Peace Institute, Switzerland
- **Dr Kenneth Okereafor**, Deputy General Manager, ICT, Head Database and App Security, National Health Insurance Scheme, Nigeria
- **Folake Olagunju**, Programme Officer, Internet and Cybersecurity, Economic Community of West African States, Nigeria
- **Arina Pazushko**, Head of Brand Development and External Affairs, BI.ZONE, Russia
- **Mr Zhang Peng**, Senior Fellow, Centre for International Rule of Law in Cyberspace, Beijing Normal University, China
- **Nigel Phair**, Director, Enterprise, UNSW Institute for Cyber Security, Australia

- **Professor Paul Pilyugin**, Senior Research Fellow, Information Security Centre, Faculty of Computational Mathematics and Cybernetics, Lomonosov Moscow State University, Russia
- **Costin Raiu**, Director, Global Research and Analysis, Kaspersky, Romania
- **Timo Schless**, Whiteflag Foundation; Lieutenant Colonel, Royal Netherlands Air Force; International Fellow, College of Information and Cyberspace, National Defense University, United States
- **Oleg Shakirov**, Senior Expert, Centre for Advanced Governance, Russia
- **Ellie Shami**, Automation Leader and Cybersecurity Project Manager, Konfidas, Israel
- **Ron Shamir**, The Federmann Cyber Security Research Center – Cyber Law Program, The Hebrew University of Jerusalem, Israel
- **Chelsey Slack**, Deputy Head of Cyber Defence, Emerging Security Challenges Division, NATO, Belgium
- **Timo Steffens**, Author of Attribution of Advanced Persistent Threats, Germany
- **Vikram Thakur**, Technical Director, Symantec, United States
- **Antti Tikkanen**, Security Engineer, Snap Inc., Switzerland
- **Dr Fitri Bintang Timur**, Researcher, Centre for Strategic and International Studies, Indonesia
- **Anne Tricaud**, Head of International Affairs, Agence nationale de la sécurité des systèmes d’information, France
- **Taariq Twaha**, Head of Information, Communication and Technology, Kenya Red Cross Society, Kenya
- **Phil Whittaker**, Head of Information Security, British Red Cross, United Kingdom
- **Marcus Willett**, Senior Adviser for Cyber, International Institute for Strategic Studies, United Kingdom
- **Dr Danil A. Zakoldaev**, Dean of the Faculty of Secure Information Systems, ITMO University, Russia

EXPERTS FROM RESEARCH PARTNERS

CENTRE FOR CYBER TRUST (ETH ZURICH AND UNIVERSITY OF BONN)

- **Professor Dr David Basin**, Department of Computer Science, ETH Zurich
- **Lisa Geierhaas**, Institute of Computer Science, University of Bonn
- **Maximilian Häring**, Institute of Computer Science, University of Bonn
- **Dr Dennis Jackson**, Independent
- **Felix E. Linker**, Department of Computer Science, ETH Zurich
- **Mihael Liskij**, Department of Computer Science, ETH Zurich
- **Professor Dr Adrian Perrig**, Department of Computer Science, ETH Zurich
- **Professor Dr Matthew Smith**, Institute of Computer Science, University of Bonn, and Fraunhofer FKIE

JOHNS HOPKINS UNIVERSITY APPLIED PHYSICS LABORATORY

- **Erin Hahn**, Principal Professional Staff, Johns Hopkins University Applied Physics Laboratory
- **Dr Antonio De Simone**, Principal Professional Staff, Johns Hopkins University Applied Physics Laboratory
- **Dr Brian Haberman**, Principal Professional Research Scientist, Johns Hopkins University Applied Physics Laboratory

EXPERTS FROM THE ICRC AND THE AUSTRALIAN RED CROSS

- **Laurent Gisel**, Head of the Arms and Conduct of Hostilities Unit, ICRC Headquarters
- **Vincent Graf Narbel**, Strategic Technology Adviser, ICRC Headquarters
- **Stephane Hankins**, Legal Adviser, ICRC Headquarters
- **Jonathan Horowitz**, Legal Adviser, ICRC Delegation in Washington, D.C., United States
- **Hollie Johnston**, Legal Adviser, Australian Red Cross
- **Fabrice Lauper**, Technical Adviser, ICRC Headquarters
- **Cedric Maire**, Digital Adviser, ICRC Headquarters
- **Larry Maybee**, Legal Adviser, Australian Red Cross
- **Tilman Rodenhäuser**, Legal Adviser, ICRC Headquarters
- **Lorenzo Redalie**, Head of the Humanitarian Affairs Department, ICRC Delegation in Moscow, Russia
- **Vitaly Savenkov**, Humanitarian Affairs Adviser, ICRC Delegation in Moscow
- **Bertrand Stivalet**, ICT Security Expert, ICRC Headquarters
- **Mauro Vignati**, Digital Technologies of Warfare Adviser, ICRC Headquarters
- **Delphine Van Solinge**, Digital Threats Adviser, ICRC Headquarters

ANNEX 2

TECHNICAL SOLUTIONS PRESENTED BY THE JOHNS HOPKINS UNIVERSITY APPLIED PHYSICS LABORATORY

TECHNICAL APPROACHES TO PROTECTING DIGITAL ASSETS AND INTERNET COMMUNICATIONS DURING CONFLICT

There are numerous examples of cyber operations being used to disrupt communications and digital assets. The cyber actors range from pranksters to criminals to nations. Some disruptions are undertaken in pursuit of a government's objectives – including in situations below the threshold of an armed conflict, as in Egypt[30] and Tunisia[31] during the Arab Spring – or within the context of an armed conflict, as in Syria[32]. Malware such as WannaCry, NotPetya, or Teardrop[33] has spread throughout the world indiscriminately, affecting various industries, and in a number of states, medical services.

A technical solution for marking communications and digital assets—a 'digital emblem'—would provide cyber actors with a means to avoid disrupting protected missions. This note recommends criteria to evaluate technical solutions, and lays out three approaches to creating a 'digital emblem' for designating protected status that can be recognized and respected by conflict participants carrying out offensive cyber operations and by third parties.

CONSIDERATIONS FOR DESIGNING AN EMBLEM

A technical solution can be evaluated based on a set of technical criteria for a desirable emblem. We propose to evaluate choices for a 'digital emblem' based on these criteria:

- logistical and operational burden on the ICRC and competent authorities controlling use of the emblem
- logistical and operational burden on the protected organization
- visibility of the emblem to third parties to identify violations and misuse
- potential for unauthorized use, including perfidious use

[30] B. Woodcock, "Overview of the Egyptian Internet Shutdown," February 2011. [Online]. Available: https://www.privacywonk.net/download/Egypt-PCH-Overview.pdf; M. Richtel, "Egypt Cuts Off Most Internet and Cell Service," The New York Times, 28 January 2011. [Online]. Available: https://www.nytimes.com/2011/01/29/technology/internet/29cutoff.html.

[31] Renesys, "77 networks out in Tunisia," [Online]. Available: http://b2b.renesys.com/eventsbulletin/2016/11/TN-1479438870.html; M. Elkin, "Tunisia Internet Chief Gives Inside Look at Cyber Uprising," 28 January 2011. [Online]. Available: https://www.wired.com/2011/01/as-egypt-tightens-its-internet-grip-tunisia-seeks-to-open-up/

[32] Renesys, "77 networks out in Syria," 29 November 2012. [Online]. Available: http://b2b.renesys.com/eventsbulletin/2012/11/SY-1354184790.html; Akamai, "State of the Internet @ akamai_soti," 29 November 2012. [Online]. Available: https://twitter.com/akamai_soti/status/274163048263057408

[33] Teardrop is one of the malware tools used to compromise the Orion product in the SolarWinds hack. [12]

- alignment with existing cyber operations and security approaches, including traceability of hostile cyber activity.

Threats to protected operations

A 'digital emblem' identifies operations entitled to protection. The risk-benefit trade-off depends on both the capabilities and the motivation of cyber actors. A 'digital emblem' provides a benefit for cyber actors who want to avoid disrupting protected operations for various reasons, such as not wishing to draw undesirable attention to themselves and wanting to comply with IHL. On the other side of the risk-benefit equation, exposing identifying information, in theory, could make the operations a target of cyber attackers.

A sophisticated cyber attacker will have many mechanisms to disrupt operations relying on digital processing and internet connectivity. For example, a gang of cybercriminals recently targeted hospitals in the United States, relying only on existing information to identify their targets.[34] Regardless of the presence of an emblem, a sophisticated cyber attacker would be able to disrupt all but the most technically sophisticated operations on the internet. The emblem is unlikely to materially affect the actions of a sophisticated attacker intent on disrupting medical operations or the ICRC's activities. A state targeting protected operations in violation of IHL has intelligence resources at its disposal and, in many cases, it also has direct control of internet resources.

A 'digital emblem' might create new threats by providing new opportunities for less sophisticated malicious actors to target protected medical facilities, transports and personnel. Marking with a 'digital emblem' could allow a belligerent to more easily identify the resources protected by that emblem. That could, for example, give a cyber actor the opportunity to use the 'digital' emblem to identify targets for harmful operations (e.g. ransomware operation against a hospital). The threat depends on the degree to which identifying those targets furthers the objectives of cyber actors.

Efficacy for the protective function

An easily visible emblem allows cooperating cyber actors to take protected entities into account in their targeting decisions, and prosecute their missions against legitimate targets without disrupting the operations entitled to protection.

The problem of misrepresentation is widespread in the digital domain. Robust techniques for preventing misrepresentation are well developed for other information in the digital domain similar to the digital emblem, typically depending on attestation of the information by a third party. Similar techniques can be applied to the digital emblem, albeit at a cost in complexity. The trade-off between the risk of misuse and the complexity of implementation is an important consideration in selecting a digital emblem.

TECHNICAL APPROACHES

The Johns Hopkins University Applied Physics Laboratory has considered three technical approaches to designing a 'digital emblem', with different implications for the considerations identified above: threats to protected operations and efficacy for the protective function. The approaches will also differ in their effects on the different categories of cyber threat actors.

Distinguished file-based emblem

A file-based 'digital emblem' signals active use of the emblem, either simply by the existence of the file or by well-known directives contained within the file. When such a file is placed in a well-known location on a system, the 'digital-emblem' file can be easily located by any software operating on that system. Additionally, a simple query/response protocol could be developed to enable external systems to query a target system about the existence/use of the 'digital emblem'.

[34] R. Hattersley-Gray, "Pro-Russia Hackers Targeted More than 400 U.S. Hospitals in 2020," 30 March 2022. [Online]. Available: https://www.campussafetymagazine.com/hospital/pro-russia-hackers-targeted-400-us-hospitals/. [Accessed 7 April 2022]

DNS-based emblem

The DNS is a key part of the globally distributed Internet infrastructure. Domain names provide a human-understandable label for identifying systems; and the DNS provides information of several kinds that is mapped to the label associated with a system.

Domain names consist of a series of labels aligned hierarchically (e.g. www.icrc.org contains three labels). A special label could be defined that would incorporate the 'digital emblem' as a part of the domain name. As long as the domain name is associated only with systems eligible for protection by the digital emblem, it will provide a straightforward, human-readable 'digital emblem' identifying the protected system.

The DNS can also map fresh information (i.e. a 'digital emblem' record) to the domain name. When querying the DNS for the network address of a domain name, software could also 'digital emblem' information associated with that name or network address. If such a record exists, the enquirer will know that the target system is protected by the 'digital emblem'.

Address-based emblem

Network addresses, for the most part, uniquely identify systems connected to the internet. These network addresses allow internet infrastructure to determine which path to use to reach the target system during message exchanges. A network address only supports the technical function of establishing a path; it does not carry any global semantics regarding the purpose associated with the system using the address.

One way to deploy a 'digital emblem' might be to develop a framework for introducing semantics into network addresses. Embedding semantics within a portion of the network address would mean that both protected digital assets and protected messages traversing the network would have addresses associated with the 'digital emblem'. This would allow systems anywhere within the internet to determine whether systems they are probing, or messages traversing the network, are associated with a protected entity (i.e. a 'digital emblem').

ENFORCEMENT

Proper use of certain critical resources within the internet's infrastructure can be enforced through an *a priori* approval process combined with public attestation (the formal certification by a neutral party) of proper use. For example, a Regional Internet Registry (RIR) allocates network addresses to an Internet Service Provider (ISP). The ISP will advertise the addresses allocated to it as an indication of that allocation. At the same time, the RIR will attest to that allocation through an independent channel. This will allow an unrelated third party to verify the advertisements made by an ISP. A party wishing to use the 'digital emblem' would make a formal request to an allocating entity, such as a member of the International Federation of Red Cross and Red Crescent Societies. If the member approves, it would publicly attest to that approval through publicly accessible means. If a third party were to question the use of the 'digital emblem', that use could be verified against the public statements of attestation.

Alternatively, passive monitoring or crowdsourcing could be leveraged to detect misuse of the 'digital emblem'. Rather than making a formal request to use the 'digital emblem', an organization could declare its intent to use the emblem in a certain way (e.g. global, distributed ledger). When a third party detects the use of the 'digital emblem', that use could be looked up in the ledger to determine if it was recorded. If it was not recorded, or if the third party believes the use was illegal, that could be reported to the entity managing the ledger, who would then be responsible for investigating the complaint. In addition, entities could scan networks for organizations using the 'digital emblem' without prior declaration of its use.

ANNEX 3

TECHNICAL SOLUTIONS PRESENTED BY THE CENTRE FOR CYBER TRUST

AN AUTHENTIC DIGITAL EMBLEM (ADEM)

In response to the ICRC's call to develop technical solutions for a 'digital emblem', the Centre for Cyber Trust (CECYT), a joint effort of ETH Zürich and the University of Bonn, designed an *Authentic Digital Emblem (ADEM)*. ADEM allows protected parties to mark their digital assets as protected by distributing cryptographically verifiable claims of protection, and to back these claims by independent, third-party endorsements.

ADEM was designed after rigorously analysing the 'digital emblem's' design space. Before implementing a 'digital emblem', three sub-problems must be solved:

1. A 'digital emblem' must be able to protect vastly different types of entities. How can a 'digital emblem' identify those entities that are protected?
2. How are 'digital emblems' distributed? The heterogeneity of protected entities necessitates different means of transmission. Additionally, we must identify channels that support the active distribution of 'digital emblems'.
3. (Why should a 'digital emblem' be trusted? The challenge here is to design a 'digital emblem' such that verifiers are convinced of an entity's protection whenever they see one, even when threat actors try to interfere with the system.

ADEM answers these questions as follows:

1. Entities are identified either by their network addresses or domain names, which identify networked processes and machines.
2. Emblems are distributed via three different protocols that offer strong security guarantees where possible, and enable lightweight distribution with fewer security guarantees in all other cases. At the same time, at least one of these protocols should be available to any kind of entity one may want to protect.
3. ADEM allows authorities to cryptographically endorse protected parties who issue 'digital emblems'. We expect nation states or supranational organizations usually to take the role of authorities. However, independent organizations can also act as authorities. It is up to verifiers to choose which authorities they trust. In times of conflict, we expect verifiers that are bound by IHL to be associated with states. In these cases, endorsements by authorities allows those verifiers to check if their own state has endorsed an emblem, minimizing trust requirements.

ADEM has many desirable properties stemming from these design decisions:

1. As the name ADEM suggests, 'digital emblems' can be *authenticated*. Cryptographic endorsements allow verifiers to authenticate a protected party's status as such.
2. ADEM allows protected parties to *actively* distribute 'digital emblems'. This ensures that observers of 'digital emblems' can remain undetectable. Hence, verifiers can use ADEM safely, without being detected as a potential threat.

3. ADEM is *distributed*. Authorities independently endorse protected parties and need not collaborate with or trust one another. This fits with the realities of international diplomacy where consensus is notoriously difficult to reach. Even parties engaged in armed conflict with each other can use ADEM.
4. ADEM is *flexible*. It was designed with many forms of digital assets, services, data, and various kinds of organizations in mind. Additionally, protected parties can tailor ADEM's deployment to their needs.
5. ADEM is *simple* and self-contained. 'Digital emblems' are presented uniformly across interfaces. Also, ADEM does not require updates to the internet's infrastructure. The modes of distribution are backwards compatible with current clients, and no updates to specifications or support from independent parties, such as certifying authorities or internet providers, is required. Finally, ADEM relies on well-tested and well-known principles and technologies, facilitating easy development and deployment.

DESIGN

We will introduce the design of ADEM with an example. Consider the protected party 'Emergency Doctors' (ED) running a group of emergency hospitals in a region at war. Each of these hospitals is linked to numerous digital entities:

- The hospitals' staff use personal devices such as tablets or laptops, connected to IT infrastructure such as databases maintaining patient records.
- The hospitals run many small devices, for example, routing infrastructure or medical devices.
- ED run an HTTPS-enabled website that informs the public about their services.

ADEM supports the protection of each of these kinds of entities and more. To configure an entity to distribute emblems, a system administrator needs only to install and configure a software client on it. Should some entities not be capable of running the client, or should there be simply too many clients, ADEM can also be configured on, for example, routers to claim protection for all nodes in their network.

To enable cryptographic verification of claims of protection, ED must take three more steps:

1. They must configure their central website to identify themselves. They are identified both in a human-readable sense – by providing information about the organization – and in a technical sense, by distributing cryptographic public keys. These public keys will enable verifiers to associate claims of protection with a protected party – in this case, ED.
2. They must individually reach out to the two parties engaged in conflict: call them Alicetan and Bobania. They ask for cryptographic endorsements, which allow the militaries of both countries to determine if the public keys hosted on their website do in fact belong to ED, a party eligible to issue claims of protection.
3. ED must connect the digital emblems issued by their entities with one of the public keys hosted on their website.

To connect digital emblems with a public key, ED must issue intermediate secret keys, to their staff, for example. The public keys are cryptographically endorsed by a public key hosted on ED's website, and in turn endorse the protected entities' public keys. This technique closely resembles certificate chains in the ecosystem of web certificates. All cryptographic endorsements are transferred to the entities and distributed alongside the emblems, so that verifiers are provided with all the information they need to decide on whether to trust the emblem they see.

Whenever a verifier – for example, a military unit belonging to either Alicetan or Bobania – receives a 'digital emblem', they can verify that: (a) it was issued by ED, and that the party claiming to be ED has been verified by both (b) Alicetan and (c) Bobania. In all likelihood, they will not trust their adversary's endorsements, but only their own.

VARIATIONS

In the previous section, we set out our recommendation of how ADEM could be deployed. However, in times of war, compromises might need to be made. ADEM supports less involved ways of deployment as well: endorsements by third parties, a central website for protected parties, and even signatures are all options and also highly recommended.

Without third-party endorsements, the public keys of a protected party can be authenticated only via the party's identifying website. This might be necessitated by a lack of time, or of connectivity, to reach out to authorities. We should, however, point out that protected parties can gather endorsements later.

Sometimes, even setting up a central website might not be within reach. In these cases, 'digital emblems' might root in a public key alone. This would require the protected party to reach out to the parties to the conflict, in order to communicate their root public key independently.

Finally, it might not even be possible for a protected party to connect their assets to a central public key. In these scenarios, entities can be configured to distribute unauthenticated claims of protection. While such unauthenticated claims should be given the closest scrutiny possible, they might be useful as a temporary measure when the conflict is unexpected and its onset abrupt. They are intended to ensure that a protected party is not left without a sign of protection while it is setting up the more involved deployment of ADEM.

TECHNICAL DETAILS

So far, we have laid out ADEM's core idea. In this section, we give more details of its technical realization. This section is intended for more technically adept readers.

We mentioned two sorts of cryptographic messages: 'digital emblems' and endorsements. We call both tokens. Tokens are encoded as JSON Web Signatures (JWS), a well-known and widely adopted standard for signing machine-readable, structured data. At its core, each token bears an issuer, encoded as a domain name that must point to an HTTPS-enabled website. This website hosts public keys, as mentioned earlier. We call all such keys *root public keys*.

Root public keys are the subject of endorsements by authorities. Endorsements encode the statement: "Public key K belongs to party P, and P is eligible to issue claims of protection." Additionally, endorsements can include constraints, for example, limiting the IP range for which emblems may be issued. These constraints are intended to limit the effects of secret-key compromise and to enhance trust in endorsements. Using constraints, authorities need not blindly trust protected parties in issuing *cartes blanches*, which would allow those protected parties to claim protection for unprotected entities.

Third-party endorsements need to be hosted alongside the root public keys on a party's identifying domain. Endorsements can also be used to manage complexity within a protected party. A protected party can distribute key material, endorsed by one of their root public keys, to their staff, for example. These intermediate keys can in turn endorse other keys, establishing a chain of endorsements that reaches the key material stored on the protected entities themselves. Any endorsements that connect a root public key to an entity public key must be sent alongside 'digital emblems'.

The distribution of 'digital emblems' happens by means of one of three protocols: TLS, ICMP, and DNS. We recommend using TLS whenever possible. The use of TLS assures a verifier that no emblem or endorsement has been intercepted by an adversary. ICMP serves as an alternative wherever TLS cannot be deployed. It comes with no guarantees that an emblem will be delivered to a potential verifier, but it is supported by almost every entity that can run the IP stack. Finally, DNS complements the options for distribution channels: it does not require entities to be modified or reachable, but is not available for all digital entities.

ADOPTION

Having sketched out the technical details of ADEM, we will now briefly discuss what would be required by protected parties to adopt ADEM. As mentioned earlier, ADEM does not require updates to the internet's architecture. Consequently, protected parties can set it up independently. However, we do not expect protected parties to have the expertise necessary to develop and deploy ADEM from scratch.

ADEM requires four kinds of software components – to manage keys and sign endorsements, distribute emblems, receive emblems and finally, verify emblems. Software for distribution and reception needs to be implemented for TLS, ICMP, and DNS each. We plan to implement and test these components in a prototyping phase.

Luckily, these components can be developed independently from protected parties. We envision them to be maintained as free and open-source software. Protected parties could then freely access and utilize them within their organization, minimizing the burden of adoption.

POSSIBLE EXTENSIONS

Besides ADEM's core design as laid out in the previous sections, we are also looking into two extensions.

First, the distribution of emblems locally on machines to processes running on these machines, which can include malware. Local distribution of emblems would make ADEM even more versatile. However, the local distribution of emblems comes with challenges that have been studied in detail, but remain generally unsolved. Therefore, work on this part is still ongoing.

Second, the support of independently operated logs maintaining a history of central public keys and their respective endorsements. This would strengthen ADEM's transparency and accountability. Logs would, for example, deter states from setting up false protected parties, endorsed only by that state, while they are used to conduct malicious operations.

In general, ADEM's core design is future-proof. ADEM's trust model can be adapted to new means of identification of protected entities, or distribution of 'digital emblems', with little additional overhead, should this ever be required in future.

MISSION
The International Committee of the Red Cross (ICRC) is an impartial, neutral and independent organization whose exclusively humanitarian mission is to protect the lives and dignity of victims of armed conflict and other situations of violence and to provide them with assistance. The ICRC also endeavours to prevent suffering by promoting and strengthening humanitarian law and universal humanitarian principles. Established in 1863, the ICRC is at the origin of the Geneva Conventions and the International Red Cross and Red Crescent Movement. It directs and coordinates the international activities conducted by the Movement in armed conflicts and other situations of violence.

facebook.com/icrc
twitter.com/icrc
instagram.com/icrc

International Committee of the Red Cross
19, avenue de la Paix
1202 Geneva, Switzerland
T +41 22 734 60 01
shop.icrc.org

4649/002 08.2022 100 Cover photo: R.Banerjee/ICRC