On the Digitization of Distinctive Emblems in International Humanitarian Law

Lei Zhang*
Hui Chen*

Abstract:
Currently, medical institutions and humanitarian organizations (MIHO) face severe digital threats in both peacetime and armed conflicts. To strengthen the identification and protection of MIHO's digital assets, data, and services, the ICRC is actively promoting the digitization of distinctive emblems (i.e., "digital emblems"). Compared to traditional distinctive emblems, "digital emblems" have unique advantages in medium, operability, scalability, time, and geographical constraints. At the practical level, "digital emblems" also bring certain transformative and uncertain factors. In terms of the formulation of rules related to "digital emblems", emphasis should be placed on shaping the legal protection of MIHO in peacetime and clarifying the international responsibilities of cyber militias and civilian hackers during armed conflicts.

---

* Lei Zhang is a PhD candidate at the Institute of International Law, Wuhan University. His main research focuses on international law issues related to cyberspace and artificial intelligence. Email:chrizzhang@foxmail.com.
* Hui Chen is an assistant researcher at the Institute of Cyber Governance and a postdoctoral fellow at the School of Mathematics and Statistics, Wuhan University. He is a member of the Sino-European Expert Working Group on the Application of International Law in Cyberspace (EWG-IL).
The authors would like to thank the editorial team of APJIHL and the anonymous reviewers for their insightful comments. Special thanks to Prof. Zhixiong HUANG, Jiayue LIN and Haokun YU from Wuhan University for providing constructive opinions and suggestions. The authors are also grateful for the funding provided by the Chinese Red Cross Society and the International Academy of the Red Cross of Soochow University. The views and remaining errors are the authors' own.

***Keywords**: digital emblem, distinctive emblem, international humanitarian law, international law in cyberspace, digital transformation*

I. Introduction

In recent years, especially during the COVID-19 pandemic, medical institutions and humanitarian organizations (MIHO) have been subjected to frequent cyberattacks, and the proper performance of their functions has been severely challenged.[1] In January 2022, the database of the International Committee of the Red Cross (ICRC) was hacked by an unknown source, stealing 515,000 pieces of personal information from at least 60 Red Cross and Red Crescent societies worldwide.[2] The incident accelerated the development and validation of the ICRC's "digital emblem" project to mitigate digital threats to MIHO from subsequent data theft, supply chain attacks and ransomware attacks.[3] In November 2022, the ICRC published the report Digitalizing the Red Cross, Red Crescent and Red Crystal Emblems: Benefits, Risks and Possible Resolutions (hereinafter referred to as "Digital Emblem" Report), which presents technical and legal options for the creation of "digital emblems" for the Red Cross, Red Crescent and Red Crystal.[4] The 34th International Conference of the Red Cross and Red Crescent in October 2024 adopted the resolution on "Protecting Civilians and other Protected Persons and Objects against the Potential Human Cost of ICT Activities during

---

[1] Ying He and Aliyu Aliyu et al., "Health Care Cybersecurity Challenges and Solutions Under the Climate of COVID-19: Scoping Review", *Journal of Medical Internet Research*, Vol. 23, No. 4, 2021, p. 1.

[2] ICRC, Cyber Attack on ICRC: What We Know, 16 February 2022, available at: https://www.icrc.org/en/document/cyber-attack-icrc-what-we-know.

[3] ICRC, Digitalizing the Red Cross, Red Crescent and Red Crystal Emblems: Benefits, Risks and Possible Resolutions, 3 November 2022, available at: https://www.icrc.org/sites/default/files/topic/file_plus_list/icrc_digitalizing_the_rcrc_emblem_1.pdf.

[4] *Ibid*.

Armed Conflict", and a preliminary international consensus was reached on the creation of "digital emblems", thus laying the foundation for the subsequent promotion of the relevant legal procedures.[5]

The "digital emblem" is an extension and digital representation of the Red Cross, Red Crescent, and Red Crystal emblems in cyberspace, aimed at providing identification and legal protection for MIHO's digital assets, data, and services during armed conflicts and peacetime. After MIHO uses the "digital emblem", enemy cyber forces or malicious cyber actors can clearly identify MIHO's digital assets, data, and services, thereby avoiding accidental damage and effectively alleviating the practical difficulties faced by MIHO. At the same time, the "digital emblem" is a major initiative of the Red Cross Movement to address new problems and challenges of the digital era and to respond effectively to the theoretical needs of IHL that are in urgent need of digital transformation to promote the clarification and development of IHL in cyberspace.

At present, most of the existing studies focus on the risks and challenges of "digital emblems" and the feasibility of technical and legal solutions, etc.[6] However, some scholars have prospectively

---

[5] ICRC, Protecting Civilians and other Protected Persons and Objects against the Potential Human Cost of ICT Activities during Armed Conflict, 28 October 2024, available at: https://rcrcconference.org/app/uploads/2024/09/34IC_9.2-Background-Doc-ICT-EN.pdf.

[6] For example, Tilman Rodenhäuser et al. pointed out the risks of "digital emblems" being vulnerable to misuse, of tagged entities being vulnerable to large-scale and rapid attacks, and of not providing substantial cybersecurity. Tilman Rodenhäuser and Mauro Vignati, "How Can a 'Digital Emblem' Help Protect Medical Facilities Against Cyber Operations?" *Lawfare*, 2023, available at: https://www.lawfaremedia.org/article/how-can-a-digital-emblem-help-protect-medical-facilities-against-cyber-operations. Felix Linker et al. proposed a technical solution based on the Authentic Digital EMblem (ADEM), emphasizing its attributes of authentication, accountability and covert verification. Felix Linker and David Basin, "ADEM: An Authentic Digital Emblem", *CCS'23: Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security*, 2023, pp. 2815-2829, available at: https://dl.acm.org/doi/10.1145/3576915.3616578.

explored how "digital emblems" can be applied to autonomous weapons.[7] There is still a lack of in-depth discussion about the potential practical changes that could be brought about by the "digital emblem" and how IHL could be refined and developed. To address this research gap in the field of international law, this paper aims to conduct an in-depth study from two perspectives: the transformative and uncertain nature of the "digital emblem" in practice and ways to improve international rules relating to it. This article seeks to provide doctrinal support for the process of establishing the "digital emblem".

II. Legal Basis and Legal Elements of the "Digital Emblem"

No international legal instrument on "digital emblems" has been adopted, and its legal basis is mainly derived from the existing rules on distinctive emblems in the Geneva Conventions and their Additional Protocols.[8] The legal assumptions expressed by the ICRC in its "Digital Emblem" Report, together with reference to the relevant rules on distinctive emblems, will help clarify the legal elements of the "digital emblem".

2.1 Legal Basis of the "Digital Emblem"

Chapter VII of the First Geneva Convention, Chapter VI of the Second Geneva Convention, Articles 18 to 22 of the Fourth Geneva Convention, Chapter II of Annex I to the First Additional Protocol and Article 12 of the Second Additional Protocol are the main legal bases for the deployment and application of distinctive emblems of IHL. The UN Group of Governmental Experts on Developments in the Field of

---

[7] Daniel C. Hinck et al. show that fully autonomous weapons may not be able to detect protective emblems due to long firing ranges, and point out that there are some advantages to "cross-frequency protective emblems". Daniel C. Hinck and Jonas J. Schottler et al, "A Next-generation Protective Emblem: Cross-frequency Protective Options for Non-combatants in the Context of (Fully) Autonomous Warfare", *International Review of the Red Cross*, Vol. 106, No. 926, 2023, pp. 1–29.

[8] As a digital extension of distinctive emblems in physical space, "digital emblems" can reasonably be expected to largely follow the established rules on distinctive emblems in IHL, but also to make some innovations in the rules in light of their unique attributes.

Information and Telecommunications in the Context of International Security (UN GGE) and the UN Open-ended Working Group on Security of and in the Use of Information and Communications Technologies (OEWG) have reached a basic consensus on the applicability of IHL to cyberspace,[9] which is a natural extension of the physical world, and the rules related to distinctive emblems should be applied to cyberspace by analogy.[10] However, due to the virtual and interconnected nature of cyberspace, there is an urgent need for a legal response on how distinctive emblems can be visualized in the virtual world, how existing rules can deal with the frequent remote attacks and attacks by non-State actors in cyberspace, and how to address the difficulty of traceability and attribution.

To ensure a legal basis for the protective role of "digital emblems", existing international legal instruments should be amended, or new international treaties should be developed. In its "Digital Emblem" Report, the ICRC mentions three legal options: the development of a new Additional Protocol to the Geneva Conventions, the amendment of Annex I to Additional Protocol I, and the conclusion of a special agreement (*ad hoc* agreement) on "digital emblems".[11] *Ad hoc* agreements are not currently considered as a priority option, as they may be divorced from the existing IHL framework or simply duplicate existing international rules and may contribute to the fragmentation of international law.

A new protocol or an amendment to Annex I is the mainstream option currently being discussed by the international community. Amending Annex I would require the ICRC to initiate a meeting of

---

[9] UNGA, Report of the Group of Governmental Experts on Advancing Responsible State Behavior in Cyberspace in the Context of International Security, A/76/135, 14 July 2021, available at: https://dig.watch/wp-content/uploads/2022/08/UN-GGE-Report-2021.pdf.
[10] Major Thomas R. Burks, "Cyberspace, Electronic Warfare, and a Better *Jus Ad Bellum* Analogy", *Air Force Law Review*, Vol. 82, No. 1, 2022, p. 1.
[11] ICRC, above note 3, p. 26.

technical experts and propose amendments, which would then be considered for adoption by the Conference of the High Contracting Parties.[12] This option is quick and flexible, but its successful adoption and entry into force requires two rounds of large-scale consent by the Parties, which makes it more difficult to amend. The development of a new protocol, which consists of three steps (signature, incorporation into the Statutes and entry into force), requires more political will and diplomatic preparations before signature and is more difficult to initiate, but it is more in line with the ICRC's habit of creating new content.[13] At the same time, a new protocol would be more formal than an amendment to Annex I, with greater visibility and diffusion of the text, which would be more conducive to the creation and practice of "digital emblems".

2.2 Legal Elements of the "Digital Emblem"

2.2.1 Functions and Scope of Application of the "Digital Emblem"

The "digital emblem" inherits the indicative and protective functions of the traditional distinctive emblems, but it also has its own peculiarities.[14] The first one is on the function for identification. The use of "digital emblems" implies that the cyber entity is one that is respected and protected from cyberattacks. The "digital emblem" facilitates the clear and intuitive discovery of the digital assets, data and services of the protected entity. In times of armed conflict, the "digital emblem" facilitates the identification of the digital assets, data

---

[12] AP I, Art. 98.

[13] In December 2005, the States Parties to the Geneva Conventions adopted the AP III, which established the "Red Crystal" emblem. In the following year, the International Conference of the Red Cross and Red Crescent incorporated the new emblem into the provisions of the Statutes. The Additional Protocol entered into force in January 2007.

[14] Anita Nwotite, "The Last Question: Do the Distinctive Emblems of the Geneva Conventions 1949, Really Protect?", *Nnamdi Azikiwe University Journal of International Law and Jurisprudence* 1, Vol. 13, No. 1, 2022, p. 2.

and services of armed forces medical institutions, civilian medical institutions, and humanitarian organizations, preventing them from being the target of cyberattacks. In peacetime, the use of the "digital emblem" by armed forces medical services is a precautionary measure to indicate that they are in a position to provide medical care in the event of the outbreak of an armed conflict.[15] The use of the "digital emblem" by humanitarian organizations, such as members of the Red Cross Movement, demonstrates their neutrality, independence and impartiality in international humanitarian relief operations and identities. This type of use is also known as "indicative use".[16]

The difference between the identification function of "digital emblems" and that of traditional distinctive emblems is mainly reflected in four aspects. First, there is a difference between virtual and real carriers. The "digital emblems" identify virtual assets such as websites, databases, digital services, etc., while the traditional distinctive emblems identify physical assets such as hospital or clinic buildings, vehicles and medical equipment. However, "digital emblems" need to be visualized in the form of images on websites, databases and other carriers, which is also the unity of the two in the dialectic. Second, the operability of using and withdrawing the emblems is different. The use and withdrawal of "digital emblems" not only require authorization from the competent military authorities but also require technical management authority, which makes it difficult to operate and, to a certain extent, prevents abuse by malicious actors. The use and withdrawal of traditional distinctive emblems, while also requiring authorization by the competent military authority, do not have a technical threshold in practice, are less difficult to operate, and are susceptible to abuse. Third, there is the issue of time and geographical limitations of recognizability. Once a protected entity has marked a "digital emblem", states or regions

[15] ICRC, above note 3, p. 13.
[16] ICRC, above note 3, p. 13.

around the world with Internet access can identify and verify the "digital emblem" through digital channels at any time and in any place, whereas the identification of traditional distinctive emblems is usually limited to a specific time and place. This nature is rooted in the interconnectivity of the network, its trans-geographical nature, and the rapid mobility of data.[17] Fourth, there is a difference in the scalability of the identification function. The "digital emblem" has strong scalability, and the protected entity's first-level or second-level domain names, portals, etc., can usually be extended to the next level of domain names and websites after marking the "digital emblem", with the characteristics of "one to everything".[18] While traditional distinctive emblems do not have scalability, buildings, vehicles, equipment, etc., need to request authorization and mark distinctive emblems individually, which is a cumbersome procedure.

Second is the function of legal protection. In times of armed conflict, entities using "digital emblems" are explicitly protected by IHL, and violations of the relevant rules will be subject to accountability under international and domestic law.[19] Deliberate direct attacks on buildings, materials, medical units, means of transportation, and personnel using distinctive emblems of the Geneva Conventions in conformity with international law may constitute war crimes.[20] However, protected entities are not obliged to use "digital emblems", as such protection derives from IHL and does not depend on the use of "digital emblems".[21] In other words, even if

---

[17] Hakan Kayan and Matthew Nunes et al., "Cybersecurity of Industrial Cyber-Physical Systems: A Review", *ACM Computing Surveys,* Vol. 54, No. 11, 2022, p. 21.

[18] Shuai Hao and Haining Wang, "Exploring Domain Name Based Features on the Effectiveness of DNS Caching", *ACM SIGCOMM Computer Communication Review*, Vol. 47, No. 1, 2017, p. 37.

[19] For example, IHL prohibits acts such as improper use, perfidious use of distinctive emblems, etc. Art. 23, para.6 of the Hague Regulations, Art. 44 and 53 of the GC I, Art. 44 of the GC II, Art. 37, para.1 of AP I, Art. 12 of AP II, and Art. 2, para.3 of AP III.

[20] Art. 8(2)(xxiv) and 8(2)(vii) of the Rome Statute of the International Criminal Court.

[21] ICRC, above note 3, p. 13.

the protected entity does not display or withdraw the "digital emblems", it is still protected under IHL. This type of use is also known as "protective use".[22]

The scope of application of the identification function of the "digital emblem" covers both times of armed conflict and times of peace, while the scope of application of its legal protection function is limited to times of armed conflict. The functionalist division of the scope of application stems from the fact that IHL, as a *lex specialis* limited to times of armed conflict, can only legally regulate a specific period of time, specific objects, and specific behaviors.[23] In peacetime, there remains a lack of binding, specialized, and universally applicable international rules providing legal protection for MIHO. However, in peacetime, when cyberattacks occur more often than in times of armed conflict, the damage suffered by MIHO as a result of cyber activities can no longer be ignored. There is an urgent need to provide clear legal support for the respect and protection of MIHO in peacetime.[24]

---

[22] ICRC, above note 3, p. 13.

[23] Marko Milanovic, "The Lost Origins of Lex Specialis: Rethinking the Relationship between Human Rights and International Humanitarian Law", *Theoretical Boundaries of Armed Conflict and Human Rights*, in Jens David Ohlin (eds.), Cambridge University Press, 2014, pp. 1–10.

[24] Some scholars contend that the United Nations Charter, IHL, and ICL exhibit significant shortcomings in regulating military preparations during peacetime, particularly concerning military preparations involving disruptive emerging technologies such as cyber warfare and artificial intelligence. Consequently, a *Jus Ante Bellum* is required to provide a proactive legal framework for addressing the risks posed by the rapid advancement of such technologies. Asaf Lubin, "Technology and the Law of *Jus Ante Bellum*", *Chicago Journal of International Law*, Vol. 26, No. 1, 2025, p. 1.

2.2.2 Applicable Objects of the "Digital Emblem"

The "digital emblem" applies primarily to the digital assets, data and services of MIHO.[25] In times of armed conflict, digital assets, data and services of MIHO authorized by the competent military authorities may use the "digital emblem" and enjoy the legal protection provided by IHL. Beyond this, an increasing number of countries are advancing the digitization of historical sites and establishing "digital museums" to prevent these landmarks from being utterly destroyed by weather erosion, war damage, and other factors.[26] This effort holds profound significance for human civilization. Consequently, the digital assets, data, and services associated with religious and historical sites should also be protected by law to shield them from the ravages of war.[27] However, such digital cultural heritage should bear the "blue shield" emblem rather than the red cross, red crescent, or red crystal emblems. Article 16 of the 1954 Hague Convention[28] stipulates that cultural property may be marked with the "blue shield" emblem to facilitate its protection, identification, and reduction of unnecessary risks of destruction. Crucially, the use of the "blue shield" emblem must comply with the form, function, and placement requirements

---

[25] The digital assets, services, and data of protected entities can be specifically classified into four categories. The first category comprises digital assets, including servers, computers, smartphones, IoT devices, and so forth. The second category encompasses digital services, such as FTP servers for storing files and VPNs, as well as technical services for remotely managing electronic devices. The third category includes data stored in IT devices, servers, and clouds. The fourth category concerns communications and data transfers between protected devices and servers.

[26] Guohua Geng and Jian Gao et al., "Review of Research on Digital Protection and Application of Cultural Heritage", *Journal of Northwest University (Natural Science Edition)*, Vol. 55, No. 1, 2025, pp. 1–10.

[27] Presently, an increasing number of States are advocating for the digitization of historical sites and the construction of digital museums to prevent the complete destruction of historical sites due to natural disasters and the devastation caused by war. This is of paramount importance for the advancement of human civilization. The protection of places of cultural and religious significance is enshrined in Art.16 of AP II to the Geneva Conventions.

[28] Convention for the Protection of Cultural Property in the Event of Armed Conflict.

stipulated in the 1954 Hague Convention and its two Additional Protocols.[29] From this perspective, the International Committee of the Blue Shield (ICBS) should also explore the possibility of developing a digital version of the "blue shield" emblem and of integrating it into the international legal framework.

While the use of distinctive emblems in IHL is mainly concentrated in times of armed conflict, MIHO still enjoys the right to use distinctive emblems in peacetime as an exceptional measure. Such use is subject to two limitations: that it is permitted by national law and that it is authorized by the Red Cross at the highest level in the country (or by a similar body under IHL).[30] In peacetime, humanitarian organizations (members of the Red Cross Movement) use the "digital emblem" to indicate their international humanitarian relief purposes and identity.[31] Medical institutions use the "digital emblem" before the outbreak of an armed conflict as a preparatory step to protect themselves from the effects of an armed conflict and to indicate that they are able to undertake rescue missions immediately.[32] In peacetime, the use of "digital emblems" by medical institutions also helps patients quickly locate the digital facilities and services. For example, it enables patients to locate the official website of the hospital among a large number of webpages and register for appointments. However, such identification functions are for the sole purpose of identifying the entity concerned and do not provide legal protection. Against the backdrop of increasingly frequent and severe

[29] Mokhamad Gisa Vitrana and Anna Anindita Nur Pustika, "The Existence of the Blue Shield Emblem on Cultural Heritage Property in Armed Conflict", *Dialogia Iuridica*, Vol. 15, No. 1, 2023, p. 6.
[30] GC I, Art. 44.
[31] ICRC, above note 3, p. 15.
[32] ICRC, above note 3, p. 15.

peacetime cyberattacks on medical institutions, it is fully justified and necessary to provide MIHO with specific and clear legal protection.[33]

2.2.3 Autonomy in the Granting and Supervision of the "Digital Emblem"

The regulations pertaining to the distinctive emblems of the Geneva Conventions and the Additional Protocols thereto stipulate that the utilization of such emblems is contingent upon the direction, consent, or constraint of the competent military authority.[34] This serves to elucidate the autonomy of the military authorities in the granting and supervision of distinctive emblems. Furthermore, ICRC has reiterated in the "Digital Emblem" Report that civilian medical units and transports must be authorized by a competent authority (the State or, in times of armed conflict, possibly an "armed group").[35]

Military authorities must be guaranteed autonomy in the granting and supervision of "digital emblems", as this is a fundamental prerequisite for respecting cyber sovereignty. Cyber sovereignty represents the logical extension of state sovereignty in the digital domain.[36] It entails the internal supremacy and external independence of a State based on state sovereignty over network facilities, network subjects, network behaviors, and related network data and information within its own territory.[37] Competent military authorities thus enjoy legitimate autonomy over the establishment of their "digital emblem" infrastructure, the use and revocation of "digital

---

[33] Priya Urs, "Cross-Border Cyber Operations: Targeting Medical as Unlawful Intervention in the Affairs of States", *Vanderbilt Journal of Transnational Law*, Vol. 57, No. 1, 2024, p. 1175.

[34] Chapter VII of GC I, Chapter VI of GC II, Chapter II of Annex I to AP I, and Art.12 of AP II.

[35] ICRC, above note 3, p. 13.

[36] Xu Wenhong, "Challenges to Cyber Sovereignty and Response Measures", *Mirovaya Ekonomika I Mezhdunarodnye Otnosheniya*, Vol. 64, No. 2, 2020, pp. 89–99.

[37] Cyber Sovereignty: Theory and Practice (Version 4.0), World Internet Conference, 2023, available at: https://cn.wicinternet.org/2023-11/09/content_36955448.htm.

emblems", and the granting and supervision of such emblems.[38] Developed countries and cyber powers should fully adhere to the Principles of Sovereignty and Non-interference, and should not interfere in the internal affairs of developing countries for any reason or through any means, such as acquiring and coordinating digital infrastructure resources, providing technical assistance, economic assistance, or coercion.[39] When providing cyber capacity building assistance (such as assistance in building "digital emblem" infrastructures) to some developing countries or least developed countries, the Principles of Fairness and Non-discrimination should be followed.[40] It should be noted that, according to the functional positioning of the ICRC, it is more likely to play a mediating and coordinating role in the development and operation of the "digital emblem", but it does not have the right to manage the "digital emblem", and it does not involve a situation in which a country cedes sovereignty to an international organization.[41]

III. The Transformative and Uncertain Nature of "Digital Emblem" in Practice

International law in the digital era has become more uncertain in terms of value orientation, normative system, attribution of behavior, identification of responsible subjects, etc., and the evolution of

[38] It can be reasonably inferred that the deployment and use of "digital emblems" will adhere to the existing rules for the deployment and use of distinctive emblems under IHL.
[39] Marko Milanovic, "Revisiting Coercion as an Element of Prohibited Intervention in International Law", *American Journal of International Law*, Vol. 117, No. 4, 2023, p. 604.
[40] Francesca Bosco and Elise Vermeersch et al., "Non-discrimination and Protection of Fundamental Rights in Cybercrime and Cyberterrorism Research", *Combatting Cybercrime and Cyberterrorism*, in Babak Akhgar and Ben Brewster (eds.), Springer Press, 2016, pp. 97–115.
[41] If an international organization holds the right to administer "digital emblems" and is responsible for allocating, granting and withdrawing them, the internal supremacy and external independence of sovereign States may be undermined.

specific rules has accelerated.[42] How to deal with the risks and challenges in the digital transformation of international law has become a proposition of the times. As an exploratory attempt at how IHL can be applied to cyberspace, the creation and implementation of "digital emblems" have naturally given rise to some practical changes and uncertainties that are different from their physical counterparts. Specifically, these practical changes are reflected in the plurality of actors of "digital emblems", the perpetrator bias in identifying and attributing them, and the complexity of determining international responsibility.

3.1 Plurality of Actors of the "Digital Emblem"

International law is a set of principles, rules, and institutions that regulate relations between states. For a long time, the thesis that "the State is the subject of international law" prevailed.[43] Its proponents were convinced that the state was the end of the evolution of social systems. If international law existed, it could only be applied between states.[44] With the organization of international society and the complexity of international relations, international organizations, individuals, and other non-State actors are gradually participating in the international legal order, providing a realistic basis for the openness of the subject of international law.[45] As far as IHL is concerned, it contains a set of international rules for the protection of

---

[42] 黄志雄，促进数字时代国际法的"良法善治"，中国社会科学报，2023 年 10 月 17 日 05 版 (Zhixiong Huang, "Promoting Good Law and Good Governance in International Law in the Digital Era", *Chinese Journal of Social Sciences*, 17 October 2023, version 5, only available in Chinese).

[43] 王铁崖，国际法，北京：法律出版社，2005：105(Tieya Wang, *International Law*, Law Press, Beijing, 2005, p. 105).

[44] Astrid Kjeldgaard - Pedersen, "The International Legal Personality of the Individual", Oxford University Press, 2018, p. 17.

[45] 王立君，国际法基本范畴的再认识——基于系统论的反思，江西社会科学，2023，43(11) (Lijun Wang, "Re-conceptualization of the Basic Categories of International Law - A Reflection Based on Systematics", *Jiangxi Social Science*, Vol. 43, No. 11, 2023).

wounded soldiers and civilians in times of armed conflict and for the restriction of the ways and means of combat, and the subject of its application is the State or armed groups. Thus, distinctive emblems in the physical domain are used to protect wounded soldiers, civilians, MIHO from military damage by states or armed groups. This reflects the functional state-centrism of distinctive emblems.

However, as the actors in cyberspace tend to diversify, the creation of "digital emblems" will inevitably accelerate the transformation of IHL from state-centrism to pluralism. With the rapid development of the internet, non-state actors, such as hackers, have increasingly gained influence by using information and communication technologies (ICTs) as tools.[46] In times of armed conflict, cyber militia[47] and civilian hackers[48] are deeply involved in cyber warfare between states. Such entities may find it difficult to comply with the rules on "digital emblems" to help their home

---

[46] Ashley Broin, "Cyber Mercenaries: The State, Hackers, and Power", *Journal of Information Technology & Politics*, Vol. 15, No. 4, 2018, pp. 400–401.

[47] A cyber militia can be defined as a group of volunteers engaged in defense-related activities in cyberspace on behalf of a State. These individuals are officially recognized by the States in question and receive a degree of coordination or guidance from the State, yet they remain distinct from the State's regular armed forces or national security structures. Jerker B. Svantesson, "Regulating a 'Cyber Militia' - Some Lessons from Ukraine, and Thoughts about the Future", *Scandinavian Journal of Military Studies*, Vol. 6, No. 7, 2023, p. 86.

[48] "Civilian hackers" include hacktivists, cybersecurity professionals, white-hat hackers, black-hat hackers, and patriotic hackers who help their home country or other countries to conduct a range of cyber operations against enemy countries. White-hat hackers are programmers who stand in for hackers attacking their own systems for security vulnerability troubleshooting. Black-hat hackers are often referred to as "hackers" who utilize their own skills to steal other people's resources or crack paid software on the network to make a profit. A patriotic hacker is a hacker who defends the interests of his country and does not use network technology to invade his country's computers but rather defends justice and fights for his country's honor. Tilman Rodenhäuser and Mauro Vignati, "8 Rules for 'Civilian Hackers' during War, and 4 Obligations for States to Restraint Them", *Humanitarian Law & Policy*, 2023, available at: https://blogs.icrc.org/law-and-policy/2023/10/04/8-rules-civilian-hackers-war-4-obligations-states-restrain-them/.

countries or sympathetic countries win.[49] However, there are currently no clear, specific rules governing such entities, which can only be regulated through general rules such as cybercrime conventions.[50] It remains to be seen whether the use of "digital emblems" can mitigate non-State-sponsored hacking attacks against MIHO in peacetime, where hackers frequently steal the private data of protected entities and launch ransom attacks. As such, given the large number and scale of non-State actors in cyberspace, their low willingness to comply with international law, and their much higher risk than that of sovereign states, "digital emblems" will be used primarily to protect the digital assets, data and services of MIHO from damage caused by a multiplicity of non-State actors.

3.2 Perpetrator Bias in the Identification and Attribution of the "Digital Emblem"

The distinctive emblems were created to protect the wounded and sick, the personnel, facilities, and means of transport of MIHO in times of armed conflict, and are essentially focused on protecting the rights and interests of victims.[51] However, owing to the characteristics of cyberspace, such as its virtual nature, interconnectedness and the multiplicity of actors,[52] "digital emblems" may in practice run counter to the original intent and appear to be biased in favor of the interests

---

[49] Tilman Rodenhäuser, "Civilian Hackers in War: The Limits that International Humanitarian Law Imposes on Volunteer IT Armies, Hacktivists, and other Civilian Hackers", *International Review of the Red Cross*, Vol. 107, No. 935, 2025, pp. 1270–1272.

[50] Danrui Luo, "Progress, Prospects, and Outlook of Global Convention on Combating Cybercrime from the Perspective of International Law", *International Journal of Cyber Criminology*, Vol. 16, No. 2, 2022, pp. 175–176.

[51] Francois Bugnion, "Adoption of the Additional Protocols of 8 June 1977: A milestone in the Development of International Humanitarian Law", *International Review of the Red Cross*, Vol. 99, No. 905, 2017, pp. 785–786.

[52] Sampath Kumar Venkatachary and Jagdish Prasad et al., "Cybersecurity Infrastructure Challenges in IoT-Based Virtual Power Plants", *Journal of Statistics & Management Systems*, Vol. 23, No. 2, 2020, pp. 263–264.

of the perpetrators, especially in terms of identification and attribution.

First, the core component of the "digital emblem" is the authentication mechanism, which is designed to facilitate potential cyber-attackers in verifying the true identity of the protected entity. In short, there is a state of "darkness" between the defender and the attacker.[53] "Digital emblems" are mainly used by attackers to verify the authenticity of the legal identity of a protected entity and are used more frequently by potential attackers; defenders do not know who has verified and who has attempted to attack, and the frequency of defenders' risk response and maintenance is lower. As one of the members of the "digital emblem" project technology demonstration of the expert group - the University of Bonn, Germany- Professor Matthew Smith said, "'digital emblems' should be easy to use by the attacker to ensure that the attacker can easily find the emblem, but the defender cannot see it. So, in effect, the system is being built that is useful to the attacker rather than the defender, and that is what is unique."[54]

Second, intentional attacks against entities using "digital emblems" are difficult to technically trace and attribute to the state,

---

[53] The state of "darkness" between the defender and the attacker can also exist when traditional distinctive emblems are used, such as when armed groups hiding their identities attack hospitals marked with the "Red Cross, Red Crescent and Red Crystal" emblems. In the case of hospitals, the armed group is detectable, and the hospital can mount a timely and appropriate defense. This type of "darkness" is usually limited to the difficulty of identifying the attacker. However, protected entities using "digital emblems" face a very different situation: cyberattacks are transient, often unknown, and cannot be detected and defended against promptly; the traces of the attack are easily erased, making traceability and attribution after the fact more difficult. In the cyber environment, the characteristics of "darkness" are more complex.

[54] Alexander Martin, "Could a 'Digital Red Cross Emblem' Protect Hospitals from Cyber Warfare?", *The Record*, 2022, available at: https://therecord.media/could-a-digital-red-cross-emblem-protect-hospitals-from-cyber-warfare.

and ultimately, perpetrators may not be held legally accountable.[55] In the physical world, deliberate attacks on entities wearing distinctive emblems are easier to identify (e.g., military or civilian, nationality, whether state-controlled or funded, etc.). In cyberspace, there has not yet been a fundamental breakthrough in the technology of tracing cyberattacks, which remains a threshold barrier to accountability. Even if the IP address and organizational affiliation of the perpetrator are found, it is difficult to determine whether the IP address and identity are suspected of being forged, or whether the perpetrator is funded or controlled by the state.[56] This has led to limitations on accountability to perpetrators, indirectly contributing to the expansion of malicious cyberattacks.

It is important to note that some states may be subject to false and unfounded accusations as a result. While the legal attribution of distinctive emblems usually exists in the state directly concerned, cyberattacks targeting "digital emblems" may still be subject to false accusations full of prejudice and arrogance, due to their invisibility, difficulty of traceability, and the disparity of traceability among states. This is especially so in view of the fact that some countries emphasize in their position statements on the application of international law to cyberspace that the political attribution of cyber operations is a matter within the sovereignty of each country, and that sufficient evidence of attribution is required only for the initiation of legal proceedings.[57] If

---

[55] Marcus Schulzke, "The Politics of Attributing Blame for Cyberattacks and the Costs of Uncertainty", *Perspectives on Politics*, Vol.16, No. 4, 2018, pp. 954–955.

[56] Chaoqin Zhang and Guangwu Hu et al., "Towards a SDN-Based Integrated Architecture for Mitigating IP Spoofing Attack", *IEEE Access*, Vol. 6, 2018, p. 22764.

[57] For example, Estonia states in its position paper that attribution is a national policy decision based on technical and legal considerations of a cyber incident or action. And the Netherlands states in its position paper that attribution of any cyber action is based on a government decision. Attribution of cyber actions does not require a state to disclose the underlying evidence. Evidence in the legal sense is only relevant when legal proceedings are initiated. UNGA, Official Compendium of Voluntary National Contributions on the Subject of How International Law Applies to the Use of Information and Communications Technologies by States Submitted by Participating Governmental

states make political attribution and so-called "legal attribution" of cyberattacks based on their political considerations alone, it may further expand the room for false accusations.[58] This is not conducive to the maintenance of the purposes of the Charter of the United Nations of international peace and security[59] and would constitute a serious interference in international humanitarian activities.

As a result, the perpetrator bias in the identification and attribution of "digital emblems" is twofold. On the one hand, it is beneficial for cyber attackers with certain legal awareness and moral bottom lines to verify and identify the true identity of the "digital emblem" user, thereby avoiding protected entities promptly and preventing accidental damage. At the same time, it also helps to reduce the network risk response and maintenance costs for defenders (i.e., users of "digital emblem"). On the other hand, the difficulty in tracing cyberattacks and accountability will also exacerbate the disregard (or even intentional challenge) by malicious actors of the international rules related to "digital emblems", making it difficult to bring into play the expected effect of legal protection.

3.3 The Uncertainty in Determining War Crimes Related to the "Digital Emblem"

There are two uncertainties regarding the determination of war crimes related to "digital emblems": one is whether it is necessary to examine the effects of cyberattacks, and the other is the structural contradiction between IHL and ICL. Article 8 (2) (xxiv) of the Rome Statute stipulates that intentionally attacking entities using distinctive

---

Experts in the Group of Governmental Experts on Advancing Responsible State Behavior in Cyberspace in the Context of International Security Established Pursuant to General Assembly Resolution 73/266, A/76/136, 13 July 2021.

[58] Florian J. Egloff, "Contested Public Attributions of Cyber Incidents and the Role of Academia", *Contemporary Security Policy*, Vol. 41, No. 1, 2020, pp. 55–56.

[59] UN Charter, Art. 1.

emblems constitutes a war crime. This means that launching cyberattacks against entities using "digital emblems" constitutes a war crime. However, Article 8 (2) (vii) stipulates that the improper use of distinctive emblems resulting in the death or serious injury of personnel from another State constitutes a war crime. This means that launching a cyberattack against a legitimate entity in country B using a "digital emblem" by an entity in country A that improperly uses it does not directly constitute a war crime but must result in death or serious injury to personnel.[60] There is a clear asymmetry between the two clauses, with the latter increasing the assessment of the effect of the cyberattack. In the determination of war crimes related to "digital emblems", there is still uncertainty about whether the effect of cyberattacks needs to be examined. If the effect of cyberattacks needs to be examined, considering the virtual nature of cyberspace and other characteristics, the determination of the effect of cyberattacks is also complex.[61]

In cyberspace, there is particular uncertainty in determining the scale and effect of damage and its forms, for example, what degree of damage can constitute a war crime, and whether non-physical damage (e.g., data leakage from medical institutions, economic loss, etc.) should be considered in addition to casualties and physical damage (e.g., computer system malfunction). National standards for determining the use of force and armed attack in cyberspace may provide an important reference for the determination of war crimes involving "digital emblems".

First, there is no doubt that an intentional attack on a medical institution using "digital emblems" that results in heavy casualties and

---

[60] Anita Nwotite, above note 14, p. 6.

[61] Kosmas Pipyros and Christos Thraskias et al., "A New Strategy for Improving Cyberattacks Evaluation in the Context of Tallinn Manual", *Computers & Security*, Vol. 74, 2018, pp. 371–372.

damage to medical facilities constitutes a war crime. As most States have stated in their position statements on the application of international law to cyberspace, cyberattacks resulting in serious injury or death to persons or damage to or destruction of objects may be considered a use of force or an armed attack.[62]

Second, it is debatable whether the theft of large amounts of data from medical institutions or humanitarian organizations using "digital emblems" or the causing of significant financial damage to medical institutions meets the threshold for war crimes. A few States, such as France, the Netherlands, Norway, and Denmark, consider that cyberattacks causing serious economic or financial damage constitute the use of force or an armed attack. In addition, Italy considers that a cyberattack may be considered a use of force even if it does not cause physical damage but results in the disruption of essential network services.[63] Fewer States have taken a position on the characterization of non-physical damage caused by cyberattacks. Consensus on this issue is far from being reached. This is mainly because, at present, cyberattacks are frequent and most of them cause non-physical damage with minor consequences,[64] so that the formation of relevant rules will inevitably exacerbate political conflicts and public opinion disputes among States, which is not conducive to the maintenance of harmony and tranquility in the international community.

Furthermore, the structural tension between IHL and ICL exacerbates the uncertainty surrounding war crimes involving "digital emblems". This tension is an inherent contradiction stemming from

---

[62] Estonia, Australia, Poland, Germany, France, Finland, the Netherlands, the United States, Norway, Switzerland, Singapore, New Zealand, Iran, Israel, and Italy consider that cyberattacks resulting in serious injury or death to persons or damage to or destruction of objects may be regarded as a use of force or armed attacks. UNGA, above note 57.

[63] UNGA, above note 9.

[64] Sorin Ducaru and Mihail Caradaica et al., "Can a Cyberattack Become an Act of War? European and Trans-Atlantic Perspectives", *Romanian Journal of European Affairs*, Vol. 24, No. 1, 2024, pp. 21–22.

the irrational or incomplete systemic structure formed by the two bodies of law. Unlike superficial or temporary conflicts, this tension is deep-seated and enduring, profoundly affecting the stability and development of the entire system. This is particularly evident in functional conflicts between the two systems, in tensions over the interpretation of rules, and in the paradoxes of enforcement mechanisms.[65] Regarding the creation of the "digital emblem", this structural contradiction manifests in the following way: as digital threats escalate daily, there is a need and impetus for IHL to undergo digital transformation and be interpreted expansively.[66] However, the

[65] This structural tension manifests itself in three main ways: Firstly, functional conflict. IHL aims to minimize harm in armed conflicts by permitting violence under the Principles of Military Necessity and Proportionality. However, ICL aims to prosecute individual crimes, characterizing similar acts as war crimes through a strict interpretation of prohibitive rules. The same conduct in an armed conflict may be evaluated as either a legitimate tactic or a criminal offence, depending on the applicable framework. Secondly, there is tension in rule interpretation. Regarding proportionality, IHL allows for the balancing of military advantage against civilian harm in real time, whereas ICL employs "harsh *ex post facto* scrutiny", which makes it more likely to find it disproportionate. Regarding command responsibility, IHL requires superiors to exercise feasible control over the actions of their subordinates, whereas ICL holds commanders criminally liable under Article 28 of the Rome Statute for intentionally acquiescing in or failing to prevent violations, thereby holding them accountable for errors in battlefield decision-making. Thirdly, there is the paradox of enforcement mechanisms. In terms of sovereignty, IHL relies on state self-enforcement, whereas the ICC requires the overcoming of sovereign immunity to enforce accountability. Regarding evidentiary thresholds, IHL focuses on compliance with conduct standards, whereas the ICC requires proof of individual subjective intent. These structural contradictions fundamentally stem from the fragmentation of international law and the realities of power politics. While technological innovation and rule harmonization may mitigate some conflicts, the logic of tolerance in IHL and the logic of punishment in the ICC will coexist dynamically for the foreseeable future.

[66] The Russia-Ukraine conflict shows that cyber warfare is now a key part of hybrid armed conflicts. Given the rapid advancement of artificial intelligence (AI), particularly in the form of lethal autonomous weapons (LAWS), AI is set to dominate future armed conflicts. IHL is actively adapting to the changes brought about by digitalization. In 2021, the UN GGE and OEWG reached a consensus on the applicability of IHL to cyberspace; however, further clarification on its implementation is required. In May 2023, some States respectively proposed draft Additional Protocols to the Convention on Certain Conventional Weapons to regulate LAWS. This marked significant progress in the Expert Group on LAWS' negotiation process. United Nations Office of Disarmament Affairs, *Draft Protocol on Autonomous Weapon Systems (Protocol VI)*, CCW/GGE.1/2023/WP.6, 11 May

principle of restraint in criminal law limits the extent to which the Rome Statute can be interpreted expansively. According to Article 22 (2) of the Rome Statute, the constituent elements of war crimes are to be interpreted strictly, and expansive application by analogy is prohibited. The principle of *nullum crimen sine lege*, one of the fundamental principles of criminal law, strictly limits the specificity of war crimes and does not support an expansive interpretation.[67] This means that even if a new treaty on "digital emblems" is developed or Annex I of Additional Protocol I is amended, the International Criminal Court (ICC) may not necessarily be consistent with IHL when faced with a specific case.

IV. Improving International Rules Related to the "Digital Emblem"

Cyberspace is different from the physical world. There are certain incompatibilities or deficiencies in the application of the existing rules on distinctive emblems to cyberspace. As mentioned earlier, there are at least two major issues that need to be addressed in the implementation of "digital emblems": one is the lack of specialized international legal rules to protect MIHO during peacetime; another issue is that most of the cyberattacks against MIHO are carried out by cyber militias and civilian hackers, and these actors also lack specialized rules to regulate them. This article advocates the development of specialized international legal rules to address these two issues. For rules that are not suitable for inclusion in IHL (such as

---

(2023); and United Nations Office of Disarmament Affairs, *Draft Articles on Autonomous Weapon Systems–Prohibitions and other Regulatory Measures on the Basis of International Humanitarian Law("IHL")*, CCW/GGE.1/2023/WP.4/Rev.2, 15 May 2023.

[67] The principle of *Nullum Crimen Sine Lege* is one of the fundamental principles of criminal law. No one can be held responsible for an unlawful act unless it has been established that, at the time of its commission, the act was subject to a clear rule making it a *de facto* crime. This principle applies both to the domestic legal order and to international law. *International Covenant on Civil and Political Rights*, Art. 14 and 15; and Luigi Condorelli, "La définition des infractions internationales, Présentation de la IIème Partie', in Hervé Ascensio, Emmanuel Decaux and Alain Pellet (eds.), *Droit International Pénal*, Paris Pedone, 2000, p. 241.

"Shaping the Obligation to Legally Protect MIHO in Peacetime"), the relevant soft law rules can be gradually developed through resolutions of the International Conference of the Red Cross and Red Crescent, etc., with a view to shaping universal *opinio juris* and State practice, and ultimately forming rules of general customary international law.[68] IHL rules that should be supplemented (e.g., "Clarifying the International Responsibility of Cyber Militias and Civilian Hackers in Times of Armed Conflict") could be fully utilized to form legally binding rules of the law of treaties by means of a compact for a new additional protocol.

4.1 Shaping the Obligation to Legally Protect MIHO in Peacetime

The use of distinctive emblems in IHL is mainly concentrated in times of armed conflict. However, as an exceptional measure, MIHO still enjoys the right to use distinctive emblems in peacetime. It should be noted that distinctive emblems in peacetime can only provide an identification function for MIHO, but cannot provide legal protection. This is due to the inherent nature of IHL as a special law in times of armed conflict.

However, against the backdrop of the deepening information technology revolution and the accelerated digital transformation of various industries, MIHO has been subjected to frequent and severe

---

[68] With regard to shaping the obligation to legally protect entities using "digital emblems" in peacetime, although it is closely related to IHL, it is inconsistent with its purpose and orientation, and it is therefore recommended that international humanitarian organizations or conferences be used as a platform, and that resolutions and other forms be used as a means of shaping international practice and forming rules of customary international law of a general nature. In emerging technological fields such as outer space, cyberspace, and AI, which are facing imminent threats, instant customary international law can be developed to make up for the long period of time and lag in the development of customary international law rules. Cheng Bin, "United Nations Resolutions on Outer Space: 'Instant' International Customary Law?", *Studies in International Space Law,* Oxford University Press, 1997, pp. 125–149.

cyberattacks in peacetime, and the cumulative damage has become too great to be ignored.[69] In contrast, protected entities in the physical world are less likely to be physically attacked by armed groups from other states, terrorist organizations, etc., which is inextricably linked to the simplicity, speed, anonymity, and low cost of cyberattacks. In light of this, there is an urgent need to provide MIHO using distinctive emblems with clear peacetime legal protection, especially in the cyber environment. The identification function does not deter potential attackers from launching cyber operations; clear and binding international legal protection is the only way to deter malicious actors. It should be noted, however, that it would be inappropriate to develop the rules in the context of IHL, as this would be inconsistent with its orientation and purpose of protecting the wounded, sick, and injured, civilians, and limiting the ways and means of warfare during armed conflict.

Consideration could be given to the development of new rules of general customary international law, such as the "Prohibition of Peacetime Cyberattacks on MIHO", to promote the formation of relevant international obligations. In the absence of a rule of international law directly regulating peacetime cyberattacks on MIHO, the international community often treats the digital assets, data, and services of medical institutions as critical civilian infrastructure[70] and invokes the general Principle of Sovereignty or the soft law "Norms for Responsible State Behavior in Cyberspace", which were adopted by UN GGE in 2015, to regulate such behavior.[71]

---

[69] Niki O'Brien and Saira Ghafur et al., "Cybersecurity in Health is an Urgent Patient Safety Concern: We can Learn from Existing Patient Safety Improvement Strategies to Address it", *Journal of Patient Safety and Risk Management*, Vol.26, No. 1, 2021, pp. 5–10.

[70] Priya Urs, above note 33, p. 1206.

[71] Most States have stated in their published position papers on the application of international law to cyberspace that attacks on critical infrastructure are considered a violation of sovereignty. The UN GGE "Norms for Responsible International Behavior in Cyberspace" 13(f) and 13(g) also address the protection of critical infrastructure. UNODA, The UN Norms of Responsible State Behavior in Cyberspace, March 2022, available at:

The ICRC has also made it clear that medical facilities are part of the critical infrastructure protected by the Norms for Responsible State Behavior in Cyberspace.[72] The consensus that medical facilities should be considered "critical infrastructure" of sovereign states has already been reached in the reports of the UN GGE and the OEWG, and this is also an important reason why the ICRC, the Oxford Process and other processes have explored in recent years the development of a new international rule "Prohibiting Cyberattacks on Medical Institutions in Peacetime".[73]

However, it has yet to be determined whether humanitarian organizations can be regarded as "critical infrastructures", and there is no specific international legal basis for the protection of humanitarian organizations in peacetime. In view of the important value and irreplaceable role played by the Red Cross Movement in international humanitarian relief, relevant rules of protection should be formulated to provide some legal support for the protection of humanitarian organizations in peacetime.

---

https://documents.unoda.org/wp-content/uploads/2022/03/The-UN-norms-of-responsible-state-behaviour-in-cyberspace.pdf.

[72] ICRC, Norms for Responsible State Behavior on Cyber Operations Should Build on International Law, 2020, https://www.icrc.org/en/document/norms-responsible-state-behavior-cyber-operations-should-build-international-law.

[73] ICRC and the Oxford Process have published more research on the protection of the medical sector in peacetime. ICRC, Call by Global Leaders: Work Together now to Stop Cyberattacks on the Medical Sector, 2020, available at: https://blogs.icrc.org/law-and-policy/2020/05/26/call-global-leaders-stop-cyberattacks-medical/; The Oxford Process, The Oxford Statement on the international Law Protections Against Cyber Operations Targeting the Health Care Sector, 2020, available at: https://www.elac.ox.ac.uk/the-oxford-process/the-statements-overview/he-oxford-statement-on-cyber-operations-targeting-the-health-care-sector/.

4.2 Clarifying the International Responsibility of Cyber Militias and Civilian Hackers in Times of Armed Conflict

In times of armed conflict, cyber militias under the command or control of states and independent civilian hackers have become increasingly involved in cyberwarfare between states, which, to a certain extent, affects the application of the Principle of Distinction in IHL in cyberspace, and consequently complicates the pursuit of the international responsibility of the relevant entities.[74] Such entities are closely related to the so-called "cyber combatants". Cyber combatants, by virtue of their direct participation in hostilities, lose the status of protected civilians. Some scholars also refer to them as "unlawful combatants".[75] The definition of a cyber-combatant is controversial. This concerns not only whether such entities can be lawfully targeted, but also whether they can enjoy prisoner-of-war status if captured and how they can be held internationally accountable.

Cyber combatants are different from physical-world combatants, and the criteria for their identification should be adjusted. Combatants are members of the armed forces of the opposing side, including regular and irregular forces, such as standing armies, reserve forces, paramilitary militias *de facto* integrated into the armed forces, and so on.[76] Articles 43 and 44 of Additional Protocol I to the Geneva Conventions regulate armed forces, combatants, and prisoners of war, but in contrast, article 4, paragraph 2, of the Third Geneva Convention (relating to militia and volunteer forces) is more clearly organized and complete in its provisions on combatants and

---

[74] Nori Katagiri, "Between Cyber Retaliation and Escalation: Explaining the Variations in State Compliance with the Principle of Proportionality", *Politics & Policy*, Vol. 52, No. 4, 2024, pp. 712–727.

[75] Yoram Dinstein, The Conduct of Hostilities under the Law of International Armed Conflict, Cambridge University Press, 2016, p. 44.

[76] Yoram Dinstein, above note 79, p. 41.

prisoners of war. Article 4 (2) of the Third Geneva Convention contains four criteria:

> (a) that of being commanded by a person responsible for his subordinates;
> (b) that of having a fixed distinctive sign recognizable at a distance;
> (c) that of carrying arms openly;
> (d) that of conducting their operations in accordance with the laws and customs of war.

There is also an implicit criterion: (e) belonging to a party to the conflict. It has been argued that these five criteria are the conditions for lawful combatants.[77] However, (d) "conducting their operations in accordance with the laws and customs of war" is only an obligation attached to the status of combatant and is not a necessary condition for constituting combatant status. Moreover, article 44, paragraph 2, of Additional Protocol I to the Geneva Conventions emphasizes that all combatants must abide by the rules of international law applicable in armed conflict, and that violations of these rules shall not deprive combatants of their rights as combatants or as prisoners of war. Thus, the essential conditions for being a lawful combatant include the following four: (a) that of being commanded by a person responsible for his subordinates; (b) that of having a fixed distinctive sign recognizable at a distance; (c) that of carrying arms openly; (d) that of belonging to a party to the conflict.

However, due to the virtual and hidden nature of cyberspace, the two formal elements of "displaying distinctive signs" and "openly carrying weapons" cannot be effectively adapted to the unique

---

[77] Zhixiong Huang and Yaohui Ying, "The Application of the Principle of Distinction in the Cyber Context: A Chinese Perspective", *International Review of the Red Cross*, Vol.102, No. 913, 2020, p. 347.

attributes of cyberspace and should be adjusted. In judging cyber combatants, only two criteria need to be recognized: (a) that of being commanded by a person responsible for his subordinates; (b) that of belonging to a party to the conflict. Accordingly, a cyber militia that has a clear commander-in-chief, is strongly organized and is under the command or control of a party to an armed conflict is a cyber combatant, and intentionally attacking an entity that uses "digital emblems" may constitute a war crime. Civilian hackers are not under the command of the armed forces and are more loosely organized. Even if they directly attack protected entities using "digital emblems", it is difficult for them to resort to IHL and the Rome Statute for malicious cyber operations, and they can only be regulated by global or regional rules in the field of cybercrime such as the United Nations Convention on Cybercrime, the Budapest Convention on Cybercrime, and domestic laws.

In recent years, the ICRC has been active in advocating for international rules against civilian hackers. In October 2023, against the backdrop of the intensifying Russian-Ukrainian cyberconflict, the ICRC proposed 8 rules against civilian hacking and reaffirmed the responsibility of governments to restrict such entities.[78] Rule 4, "Prohibition of Cyberattacks on Medical and Humanitarian Facilities", is consistent with the aims and objectives of the "digital emblem". However, these rules still face the dilemmas of low awareness, weak enforcement, and a lack of binding mechanisms in reality.[79] These

[78] Tilman Rodenhäuser & Mauro Vignati, above note 48.

[79] Many hacker communities are unaware of their legal obligations and even actively refuse to be bound by the rules. Even if they are aware of the relevant content (a few hacker organizations, such as KillNet, have stated that they comply with the rules), it is often difficult to enforce the consequences due to the ambiguity and anonymity of the responsibility. The most urgent task now is to enhance the hacker community's awareness and acceptance of the rules and to promote cooperation between the States and technology companies to strengthen ethical awareness of cyber warfare through education and incentives. The lack of effective legal constraints in the field of cyber warfare will make it difficult for IHL to adapt to the new form of warfare, and the ICRC's

rules should not remain at the initiative level but should be made legally binding through special agreements or new treaties to regulate the uncontrolled development of civilian hackers in cyberspace. Respect for distinctive emblems (including "digital emblems") must be more than just theoretical or superficial; it must be upheld in practice. Therefore, more proactive measures are needed to promote the protection and respect of MIHO and distinctive emblems in contemporary armed conflicts.[80]

V. Conclusion

The "digital emblem" is a significant initiative by the International Red Cross Movement in response to new issues and challenges emerging in the digital age. During the preparatory phase preceding its establishment, it is important to conduct in-depth research into its legal basis and elements, its transformative potential, and the practical uncertainties, as well as how to advance the refinement and development of related international rules. This research will contribute to the clarification and development of IHL in cyberspace, as well as the digital transformation of international law.

Governments should actively support the ICRC in researching and implementing the "digital emblem" project and participate in negotiations on relevant international legal instruments. At the same time, attention must be given to safeguarding the collective interests of developing countries and those with underdeveloped cyber capabilities. In addition, governments should actively oppose the

---

initiative, although not mandatory, is a necessary but insufficient first step to lay the moral and legal foundation for the future development of cyber warfare rules, which will need to be upgraded through inter-state cooperation and legal mechanisms to transform the soft guidance into substantive and binding rules in the future. Samuel White, "One Year On: Are the ICRC's Principles for Civilian Hackers Shaping the Laws of War?", *Lieber Institute*, 2025, https://lieber.westpoint.edu/one-year-are-icrcs-principles-civilian-hackers-shaping-laws-war/.

[80] See Anita Nwotite, above note 14, p. 3.

misuse of cyber weapons and LAWS and advocate capacity-building assistance from developed countries and cyber powers for developing countries. Guided by the Principles of Non-interference and Non-discrimination, they should assist these States in establishing the "digital emblem" infrastructure, bridging the digital divide and contributing to the sustainable development of the international community.

As a landmark humanitarian initiative that benefits the international community, non-State actors—including members of the International Red Cross and Red Crescent Movement, as well as relevant internet entities [81] —should collaborate to advance the implementation and practice of the "digital emblem", thereby jointly building a more inclusive, equitable and resilient community with a shared future in cyberspace.

[81] Relevant internet entities include internet technology standards organizations such as the Internet Engineering Task Force (IETF), cybersecurity companies, and laboratories. These entities played a significant role in the demonstration and testing of the "digital emblem" project. IETF, "Problem Statement for Digitized Emblems", May 2024, available at: https://datatracker.ietf.org/doc/draft-haberman-digital-emblem-ps/01/.