DROIT & POLITIQUES
HUMANITAIRES

Vers un emblème numérique ? Cinq questions sur les enjeux juridiques, technologiques et politiques liés à une telle innovation

décembre 12, 2022, Action humanitaire / Droit et conflits / Nouvelles technologies

12 minutes de lecture

Tilman Rodenhäuser
Conseiller juridique thématique, CICR

Mauro Vignati
Conseiller sur les nouvelles technologies numériques de guerre, CICR

Les médecins qui soignent les blessés de guerre et les délégués du CICR qui œuvrent dans des régions affectées par un conflit armé s'en remettent à des symboles de protection uniques et universellement reconnus : les emblèmes de la croix rouge et du croissant rouge. Depuis plus de 150 ans, ces emblèmes communiquent un message simple : les installations, les véhicules et les personnes qui les arborent ne doivent pas être attaqués.

Aujourd'hui, les établissements médicaux et les acteurs humanitaires utilisent des technologies numériques qui leur permettent de répondre plus efficacement aux besoins des populations, mais les exposent aussi à de nouvelles menaces. À une époque où les conflits armés s'étendent au numérique, peut-on vraiment s'appuyer sur ces technologies pour renforcer la protection des structures médicales ? Est-il possible d'importer dans l'environnement numérique ce principe centenaire qui veut que « les hôpitaux, les ambulances et les évacuations (…) port[ent] croix rouge sur fond blanc » ? Techniquement, ceci est possible, mais quels en seraient les avantages et les risques ?

Afin d'étudier les solutions possibles, le CICR a entamé en 2020 un partenariat avec le Center for Cyber Trust et le laboratoire de physique appliquée de l'Université John Hopkins, et plus récemment avec l'Université ITMO de Saint-Pétersbourg. Il a également réuni un groupe d'experts internationaux (voir annexe 1 ici) chargé d'évaluer les avantages et les risques associés à un emblème numérique. Ce partenariat a donné lieu à un rapport publié aujourd'hui et intitulé « Digitalizing the Red Cross, Red Crescent and Red Crystal Emblems » (numériser les emblèmes de la croix rouge, du croissant rouge et du cristal rouge), où sont présentés différentes solutions techniques, le point de vue des experts sur les avantages et les risques qu'elles présentent ainsi que des solutions possibles pour avancer. Dans cet article, Tilman Rodenhäuser et Mauro Vignati, conseillers pour le CICR, répondent à cinq questions fondamentales que soulève l'idée d'un « emblème numérique ».

Qu'est-ce qu'un emblème numérique et que pourrait-il apporter ?

À l'instar de la numérisation qui s'opère au sein de nos sociétés, les cyberopérations deviennent une réalité dans les conflits armés contemporains. Les États considèrent que la probabilité croissante d'une « *utilisation des technologies de l'information et de la communication [TIC] dans les conflits futurs entre États* » constitue une menace pour la sécurité internationale. De son côté, le CICR met en garde contre le coût humain potentiel des cyberopérations et exprime son inquiétude quant à la vulnérabilité du secteur médical et des organisations humanitaires face à ces opérations, surtout lorsqu'elles sont relève de la cybercriminalité. En effet, depuis le début de la pandémie de Covid-19, plusieurs *hôpitaux ont été victimes de cyberattaques* qui ont perturbé la fourniture de soins vitaux et entravé le travail des médecins et du personnel infirmier, les obligeant à revenir au papier et au crayon en pleine situation d'urgence. Et en 2022, plusieurs membres du Mouvement international de la Croix-Rouge et du Croissant-Rouge, ainsi que d'autres organisations humanitaires, ont été la *cible de cyberopérations*. En période de conflit armé, celles-ci exposent les personnes déjà vulnérables – blessés, malades ou personnes en situation de précarité – à des risques encore plus élevés.

Ce projet d'emblème numérique vise à créer un signe numérique permettant d'identifier avant tout les structures médicales – et de signaler qu'elles sont protégées – et à l'intégrer dans le cadre juridique international existant. Un emblème numérique offrirait un niveau supplémentaire de protection contre les cyberopérations, tout comme la protection offerte par la croix rouge, le croissant rouge ou le cristal rouge dans le monde réel. Il enverrait un message clair : la structure qui l'arbore bénéficie d'une protection spéciale en vertu du droit international humanitaire et doit être protégée contre toute atteinte.

Il est important de comprendre que l'emblème numérique n'aurait pas vocation à protéger les systèmes informatiques contre les intrusions et les dommages ; sa fonction serait de signaler l'existence d'une protection juridique. Par conséquent, les établissements médicaux arborant l'emblème numérique devraient veiller à prendre également des mesures de cybersécurité, de la même façon qu'un hôpital situé dans une zone de guerre recourt généralement à diverses mesures physiques pour se prémunir contre les dommages causés incidemment.

À quoi pourrait ressembler un emblème numérique et quelles devraient être ses caractéristiques ?

Pour résumer, nos *partenaires de recherche* ont élaboré trois solutions techniques possibles pour la création d'un emblème numérique.

La première option consiste en un *emblème fondé sur le système DNS (Domain Name System)* qui utiliserait un marqueur spécial pour lier l'emblème numérique à un nom de domaine (par ex. : www.hopital.*emblème*). Cet emblème numérique simple et directement lisible par les internautes identifierait le système protégé.

La deuxième option est un emblème fondé sur les adresses IP. Cela consisterait à intégrer des métadonnées sémantiques dans les adresses IP pour identifier à la fois les ressources numériques protégées et les messages protégés transitant par un réseau.

La troisième option, *un système d'emblème numérique authentifié (ou ADEM)*, consisterait à utiliser des chaînes de certificats pour signaler la protection. Dans ce cas, les certificats (comparables au petit verrou figurant dans la barre d'adresse du navigateur, par exemple) pourraient être authentifiés par diverses instances et communiqués *via* différents protocoles Internet.

Nous sommes en train d'affiner et de tester ces différentes options avec nos partenaires en tenant compte, comme nous l'avons fait jusqu'ici, de plusieurs critères considérés comme importants par des experts des secteurs médical, humanitaire et militaire.

Tout d'abord, pour pouvoir être utilisé par des structures médicales, l'emblème numérique doit être facile à déployer et à maintenir, à moindres frais et partout dans le monde, en dépit des différences linguistiques, technologiques, culturelles et matérielles. Il doit pouvoir s'intégrer dans l'environnement technologique existant (y compris le cloud) et s'adapter aux évolutions à venir tant au niveau des technologies que des infrastructures. Point crucial pour parer à d'éventuels risques en matière de sécurité, l'emblème numérique doit également pouvoir être retiré facilement. De plus, il faut qu'il puisse être déployé sous le contrôle de l'autorité compétente de chacune des parties à un conflit armé.

Ensuite, pour un signalement effectif de la protection, l'emblème doit pouvoir être vu et aisément identifié et compris des personnes menant des cyberopérations (les « cyberopérateurs »). Ceux-ci doivent également pouvoir détecter la présence d'un emblème numérique sans être automatiquement identifiés comme des menaces potentielles. Idéalement, l'emblème numérique devrait faire partie des informations recherchées par tout cyberopérateur qui s'introduirait dans un système informatique. Enfin, il doit être possible d'en vérifier facilement l'authenticité.

Quels sont les principaux avantages et risques associés à l'emblème numérique ?

Le principal avantage est qu'il serait plus facile pour les cyberopérateurs d'identifier et de respecter les structures protégées, tant que les protections juridiques sont visibles et appliquées dans l'environnement numérique. Dans le chaos de la guerre, ce signal supplémentaire pourrait présenter une réelle

utilité, car il permettrait aux structures concernées de mieux se protéger contre le risque de dommages causés incidemment par des opérateurs respectueux du droit. Il pourrait en outre avoir un effet dissuasif sur les opérateurs malveillants.

Dans le même temps, le fait de signaler et d'identifier numériquement les structures médicales et humanitaires pourrait accroître le risque qu'elles deviennent la cible d'opérations hostiles. L'importance de ce risque serait toutefois variable. En effet, nombre d'opérateurs sont déjà en mesure d'identifier sans problème ces structures dans le cyberespace ; dans ce cas, le risque supplémentaire lié à la facilité d'identification serait donc relativement faible. Quant aux opérateurs technologiquement moins avancés, l'utilisation d'un emblème numérique pourrait certes leur faciliter la tâche, mais leurs capacités de nuisance seraient plus limitées.

L'emblème numérique présente un autre risque : celui d'une utilisation inappropriée pour signaler des infrastructures militaires ou d'autres infrastructures non protégées. Ce risque existe également dans le monde physique, où l'utilisation abusive des emblèmes est strictement interdite tant par le droit international que par les législations nationales.

Qui peut utiliser un emblème numérique et dans quelles circonstances ?

L'utilisation des emblèmes et des signes distinctifs est réglementée par le droit international humanitaire (voir, entre autres, l'article *44* de la Première Convention de Genève ; les articles *18* et *38* du Protocole additionnel I ; et l'*Annexe 1* au Protocole additionnel I), ainsi que par les lois et réglementations nationales correspondantes. Conformément à ces traités, les emblèmes distinctifs peuvent être utilisés pour deux raisons.

Tout d'abord pour signaler la présence d'une protection juridique. Dans ce cadre, les emblèmes distinctifs ne peuvent être utilisés qu'en période de conflit armé, et non en temps de paix (sauf comme mesure de préparation en vue d'assurer la protection lorsqu'un conflit vient à éclater). De plus, leur utilisation est essentiellement limitée au personnel médical autorisé (services médicaux des forces armées, établissements médicaux civils autorisés) ainsi qu'au CICR et à la Fédération internationale des Sociétés de la Croix-Rouge et du Croissant-Rouge.

Ensuite, en temps de paix et de conflit armé, les membres du Mouvement international de la Croix-Rouge et du Croissant-Rouge (le Mouvement) peuvent utiliser l'emblème à titre indicatif, autrement dit pour marquer leur appartenance au Mouvement.

Le droit international humanitaire limite l'utilisation des emblèmes distinctifs aux entités médicales et aux opérations humanitaires menées par le Mouvement, mais il existe d'autres emblèmes ou signes, par exemple pour identifier les Nations Unies ou les biens culturels.

Les voies possibles vers un emblème numérique

Les études et les consultations menées, les avis globalement positifs du groupe d'experts internationaux et le *soutien sans faille du Mouvement* pour « poursuivre [les] recherches sur la faisabilité technique d'un emblème numérique (…) et à évaluer les avantages d'un tel emblème » incitent le CICR à persévérer dans cette voie. Sur le plan technique, des efforts de développement supplémentaires seront nécessaires, et les solutions possibles devront être validées et vérifiées. Ce volet sera assuré par le CICR en coopération avec ses partenaires de recherche. Sur le plan diplomatique, il revient désormais aux États d'examiner cette idée et de définir les prochaines étapes. Le CICR souhaite mener des consultations à cette fin avec toutes les parties prenantes concernées, en particulier les États et le Mouvement.

L'un des atouts majeurs des emblèmes et signes distinctifs réside dans le fait que leur forme, leur fonction et leur utilisation sont réglementées par le droit international humanitaire, qui en interdit tout usage inapproprié. Si les États estiment que la création d'un emblème numérique est souhaitable, il existe différentes voies possibles pour l'intégrer dans le cadre juridique international existant, notamment les suivantes :

- L'adoption d'un nouveau protocole additionnel aux Conventions de Genève. C'est l'approche qui a été adoptée en 2005 pour adopter l'emblème du *cristal rouge*.
- La révision de l'*Annexe I au Protocole additionnel I*, qui réglemente l'utilisation des signaux distinctifs (signaux lumineux et radio, identification électronique) et des moyens de communication (communication radio, codes). Une procédure de mise à jour régulière de cette annexe est prévue dans le Protocole additionnel I (voir *article 98*).

Alors que les cybermenaces contre les établissements médicaux et les organisations humanitaires impartiales se multiplient, l'heure est venue pour la communauté internationale de s'unir pour faire face à ces risques nouveaux en modernisant les mesures de protection pratiques mises en place de longue date et en faisant preuve d'innovation dans ce domaine.

Cet article a été initialement publié en anglais le 3 novembre 2022.

Voir aussi :

- Tilman Rodenhäuser, Laurent Gisel, Larry Maybee, Hollie Johnston & Fabrice Lauper, « *Signaler la protection juridique dans le monde numérique : une nouvelle ère pour les emblèmes distinctifs ?* », 15 novembre 2021

Tags: action humanitaire, Conventions de Genève, DIH, droit international humanitaire, emblème numérique

Lorsque les hostilités prennent fin mais que les souffrances demeurent : la nécessité de poursuivre des activités humanitaires au lendemain d'un conflit armé

15 minutes de lecture

Action humanitaire / Droit et conflits / Nouvelles technologies

Émilie Charpentier

Les conflits armés ont des conséquences à long terme sur les populations, même bien longtemps ...

Le DIH et les territoires occupés

17 minutes de lecture

Action humanitaire / Droit et conflits / Nouvelles technologies

Tristan Ferraro & Mikhail Orkin

Alors que le conflit armé en Ukraine s'installe, les civils pris au piège de ce ...