Signaler la protection juridique dans le monde numérique : une nouvelle ère pour les emblèmes distinctifs ?

novembre 15, 2021, Droit et conflits / Générer le respect du DIH

14 minutes de lecture

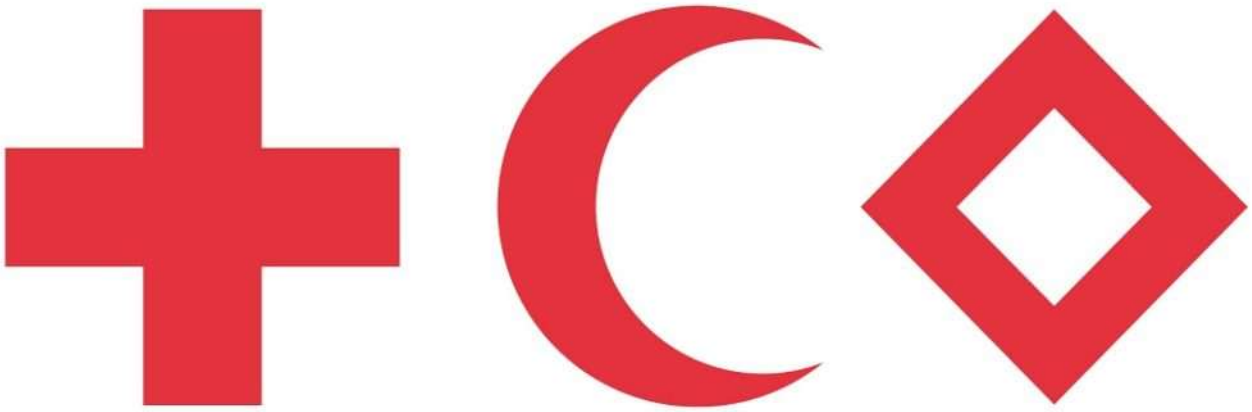

Tilman Rodenhäuser
Conseiller juridique thématique, CICR


Laurent Gisel
Chef de l'unité armes et conduite des hostilités, CICR


Larry Maybee
Conseiller juridique, Croix-Rouge australienne


Hollie Johnston
Conseillère principale, Croix-Rouge australienne


Fabrice Lauper
Conseiller en technologie, CICR



ICRC Humanitarian Law & Policy blog

Le recours à des technologies numériques dans les conflits armés s'est considérablement accru. Si cette évolution n'est pas sans inconvénients, elle peut aussi présenter des avantages. Par exemple, les nouvelles technologies pourraient-elles permettre la signalisation numérique de la protection dont jouissent certaines infrastructures et certains actifs en vertu du droit international humanitaire ? Depuis 150 ans, la croix rouge, le croissant rouge et, plus récemment, le cristal rouge, remplissent cette fonction dans le monde matériel. Serait-il possible – et souhaitable en termes de cybersécurité – de signaler les actifs numériques en période de conflit armé ?

Dans ce billet, Tilman Rodenhäuser, conseiller juridique au CICR, Laurent Gisel, chef de l'unité armes et conduite des hostilités du CICR ; Larry Maybee, conseiller juridique à la Croix-Rouge australienne ; Hollie Johnston, conseillère principale à la Croix-Rouge australienne ; et Fabrice Lauper, conseiller technique au CICR, exposent les principaux axes de réflexion du projet de recherche du CICR relatif à la numérisation des emblèmes de la croix rouge, du croissant rouge et du cristal rouge.

Cela fait trois ans qu'un conflit armé oppose la Boronie à la Banskie. Alors que le jour se lève, deux avions de chasse F-15 boroniens survolent une ville et se dirigent vers la cible qui a été déterminée lors de la planification de l'opération par les militaires. Cependant, ce que les pilotes ignorent, c'est que les planificateurs opérationnels se sont trompés de cible. Au lieu du hangar militaire qu'ils pensaient qu'ils allaient attaquer, les pilotes des avions de chasse se dirigent tout droit sur un hôpital de Banskie, un établissement qui dessert une population de plus de 55 000 personnes.

Les pilotes atteignent leur objectif, se tenant prêts à larguer leurs munitions à guidage de précision conformément à la liste des cibles qui a été établie lors de la planification des opérations. Juste au moment d'agir, un des pilotes constate sur le viseur tête-haute de son cockpit que quelque chose est peint sur le toit de la cible qui lui a été attribuée : une grande croix rouge sur fond blanc, d'environ dix mètres carrés. La pilote sait qu'en vertu du *droit international humanitaire* (DIH), les établissements sanitaires sont protégés contre les attaques et que la croix rouge est le signe de cette protection. Elle abandonne immédiatement l'opération.

Ce cas fictif montre l'importance *des emblèmes distinctifs de la croix rouge, du croissant rouge et du cristal rouge* pour identifier le personnel, les formations, les établissements, ainsi que les transports qui sont spécialement protégés par le DIH.

De nos jours, la guerre évolue. *Les cyberopérations pendant les conflits armés sont désormais une réalité* et les États ne cessent d'accroître leurs cybercapacités militaires. Cette évolution n'est pas sans inconvénients, mais elle peut aussi présenter des avantages. Par exemple, les nouvelles technologies pourraient-elles permettre la signalisation numérique de la protection dont jouissent certaines infrastructures et certains actifs en vertu du droit international humanitaire ? Que se serait-il passé si les Boroniens avaient eu l'intention de déployer un logiciel malveillant afin d'endommager des serveurs informatiques qui selon eux, étaient utilisés à des fins militaires ? Aurait-il pu y avoir un emblème, un signe ou un signal numériques indiquant que certains de ces serveurs jouissaient de la protection conférée par les emblèmes distinctifs ?

Le CICR étudie actuellement cette question avec plusieurs partenaires, dans le cadre d'un projet de recherche sur la numérisation des emblèmes de la croix rouge, du croissant rouge et du cristal rouge. Le projet a pour but de déterminer si les emblèmes distinctifs pourraient être utilisés dans les technologies de l'information et de la communication (TIC) et de quelle manière, en portant un regard critique sur la faisabilité technique et la valeur protectrice qu'aurait la signalisation des actifs numériques des structures protégées bénéficiant d'une protection en période de conflit armé.

Dans ce billet, nous présenterons les principaux axes de réflexion qui structurent ce projet. Dans les deux autres billets de cette série, le *Centre for Cyber Trust* de l'École polytechnique fédérale (EPF) de Zurich et le *Laboratoire en physiques appliquées de l'université de Johns Hopkin* exposeront le résultat de leurs recherches et les diverses options qui, d'un point de vue technique, permettraient de signaler les infrastructures et les données numériques des acteurs et établissements protégés.

Les emblèmes distinctifs : identification et protection pendant un conflit armé

La protection juridique conférée aux établissements sanitaires pendant un conflit armé est consacrée par le DIH. Le principe fondamental qui est au cœur de la toute première Convention de Genève de 1864 et qui aujourd'hui encore, demeure au centre du DIH, est que les blessés et les malades ainsi que ceux qui leur portent secours – personnel sanitaire, mais aussi établissements, unités et transports sanitaires – doivent être respectés et protégés en toutes circonstances pendant un conflit armé (voir, par exemple, les règles *25*, *28 et 29* de l'Étude du CICR sur le *DIH coutumier).[1]*

Depuis 150 ans, la croix rouge et le croissant rouge et plus récemment le cristal rouge rendent cette protection visible, en montrant que ceux qui les arborent, de même que les établissements et les biens qui sont marqués par ces signes, sont protégés contre les attaques (voir règle *30* de *l'Étude du CICR sur le DIH coutumier*). Les principaux instruments du DIH (voir article *44* de la Première Convention de Genève et article *18* du Protocole additionnel I) autorisent et réglementent l'usage des emblèmes par les services sanitaires et religieux des forces armées ainsi que par les unités et transports sanitaires civils autorisés pendant un conflit armé. Les emblèmes permettent aussi d'identifier et de protéger le CICR comme la *Fédération internationale* en période de conflit armé, ainsi que les autres membres du *Mouvement international de la Croix-Rouge et du Croissant-Rouge* (le Mouvement) lorsqu'ils remplissent des fonctions sanitaires en temps de guerre.*[2]*

Historiquement, le DIH conçoit les emblèmes sous une forme matérielle – une grande croix rouge, ou un grand croissant rouge ou cristal rouge sur fond blanc. Lorsqu'il est apposé sur des biens protégés ou arboré par des personnes, l'emblème constitue la manifestation visible de la protection juridique qui leur est conférée.

Exemple de l'usage de l'emblème distinctif par les services sanitaires des forces armées

Toutefois, l'obligation de respecter et de protéger ces personnes et ces biens ne se limite pas seulement à la guerre cinétique ; elle s'applique aussi *dans le cadre de cyberopérations conduites lors d'un conflit armé.* Et il est absolument nécessaire que cette protection soit signalée aux opérateurs cyber : les cyberopérations menées contre des établissements médicaux sont une réalité et risquent de nuire à des êtres humains, notamment en période de conflit armé, au moment même où il est vital de préserver le fonctionnement des établissements médicaux et des systèmes de santé. De même, dès lors que le CICR – et les autres composantes du Mouvement – numérisent de plus en plus leurs services et leurs opérations, le risque qu'ils soient eux-mêmes victimes de cyberopérations hostiles est bien réel.

La question d'un « emblème numérique »

Dans la quête de mesures concrètes permettant de renforcer la protection des services de santé des forces armées ainsi que des activités des autres acteurs médicaux et humanitaires autorisés à intervenir pendant un conflit armé, l'idée de concevoir un nouveau signe, une signalisation numérique ou d'autres moyens d'identification dans le cyberespace (c'est-à-dire un « emblème numérique ») est apparue comme une voie possible. Un des atouts majeurs de cette proposition est que ce nouveau signe pourrait figurer parmi les « emblèmes distinctifs » ou « signaux distinctifs » internationalement reconnus sur le plan juridique et politique (à l'instar du *signal lumineux*, du *signal radio* et de *l'identification par moyens électroniques*, voir l'*Annexe I* du Protocole additionnel I).

Ces dernières années, le CICR a évoqué l'idée d'un « emblème numérique » lors de discussions avec des experts en cybersécurité et des spécialistes opérationnels, qui ont fait ressortir les avantages d'un tel projet, mais aussi un certain nombre d'inconvénients (voir *ici* [pp. 9 ; 39-42] et *ici* [pp. 27-31]). D'un côté, un « emblème numérique » pourrait signaler les infrastructures et les données des acteurs protégés afin de faciliter leur identification et d'éviter qu'ils ne soient pris pour cible par erreur ou qu'ils ne soient victimes de dommages incidents causés par des cyberopérations. D'un autre côté, un signe numérique présente le risque que des acteurs malveillants identifient certaines « cibles faciles » (*soft target*), qui pourraient donc être attaquées plus facilement et plus systématiquement. De plus, des acteurs malveillants pourraient faire un emploi abusif d'un « emblème numérique » en faisant croire que leurs opérations bénéficient du statut protecteur conféré par le DIH. Toutefois, ces inconvénients et ces avantages ne sont pas nouveaux et ils sont aussi présents dans le monde matériel ; toute la question est de savoir s'ils sont différents dans un environnement numérique et en quoi ils le sont.

Un processus de recherche et de consultation pour examiner la faisabilité d'un « emblème numérique » et sa valeur protectrice

En 2020, le CICR a lancé un projet afin d'examiner les moyens techniques qui permettraient d'identifier des infrastructures et des données numériques appartenant à des acteurs ayant le droit d'utiliser les emblèmes distinctifs.

Le CICR a d'abord travaillé avec deux instituts de recherche : le *Centre for Cyber Trust* de l'EPF de Zurich et le *Laboratoire en physiques appliquées de l'université de Johns Hopkin*, afin de trouver des moyens techniques permettant de signaler les infrastructures et les données numériques des acteurs protégés. Le CICR travaille désormais en partenariat avec la Croix-Rouge australienne (CRA) afin de consulter des experts en cybernétique issus de divers pays, pour examiner les solutions proposées par les chercheurs et analyser leurs avantages et inconvénients, mais aussi les les défis liés à la création d'un emblème ou d'un signe distinctif dans le cyberespace. Cette consultation d'experts en cybersécurité et de spécialistes opérationnels de divers horizons débutera prochainement.

Ces consultations ont pour but d'examiner si un « emblème numérique » serait de nature à renforcer la protection de ceux ayant le droit de l'utiliser, contre des cyberopérations qui leur seraient préjudiciables. Si cet examen permet de trouver une solution pérenne et protectrice, cela ne résoudra pas la question de savoir si et comment les emblèmes distinctifs pourraient être utilisés dans les TIC, mais marquera au contraire le début d'un nouveau processus ou d'une nouvelle étape du projet d'« emblème numérique ».

D'un point de vue technique, il faudrait développer et tester des prototypes d'un « emblème numérique ». Plus important encore, le CICR – conformément à *son mandat* de « travailler à la compréhension et à la diffusion du droit international humanitaire applicable dans les conflits armés et d'en préparer les développements éventuels » – devrait soumettre aux États les solutions envisageables et discuter des moyens de les incorporer dans le cadre juridique existant. Des discussions plus approfondies devraient aussi être organisées avec d'autres parties prenantes concernées, notamment le Mouvement de la Croix-Rouge et du Croissant-Rouge dans son ensemble.

* * *

Quelle qu'en soit l'issue, le projet propose une importante réflexion sur la manière dont le cadre actuel du DIH peut répondre aux défis posés par les progrès technologiques et s'y adapter. Les résultats de ce projet de recherche pourraient avoir une influence sur la nature des opérations conduites par les belligérants dans le cyberespace. Il suffit de repenser au cas présenté en introduction de cet article…

Le conflit armé dure maintenant depuis quatre ans.

La Banksie a commencé à mettre au point un logiciel malveillant qui se diffuse automatiquement et qui affecte un logiciel basé dans le cloud et utilisé par la Boronie pour la logistique de ses équipements militaires. Alors qu'il effectue une mission de reconnaissance, le cybercommandement de la Banksie se rend compte que le logiciel ciblé est plus souvent utilisé qu'il ne s'y attendait, notamment sur des systèmes qui sont signalisés par un tout nouvel « emblème numérique ». Après une enquête plus poussée, les opérateurs découvrent que ces systèmes appartiennent à un hôpital.

Le cybercommandement de la Banksie sait que les emblèmes et les signes distinctifs sont un symbole de protection. Le commandant ordonne à son équipe de reprogrammer leur logiciel malveillant afin de veiller à ce qu'il n'affecte pas l'infrastructure numérique de l'hôpital. Informés, grâce à l'emblème numérique et au fait qu'il soit facilement reconnaissable, de l'utilisation du logiciel par des services médicaux, le commandant ordonne aux programmeurs de revoir les procédures et de programmer les capacités cyber de façon à ce qu'elles ne nuisent pas aux systèmes signalés par un emblème numérique.

[1] Ils perdent leur protection s'ils sont utilisés pour commettre, en dehors de leurs fonctions humanitaires, des actes nuisibles à l'ennemi.

[2] En tout temps, les composantes du Mouvement peuvent utiliser l'emblème pour signaler leurs unités, leurs transports, leur personnel et leurs volontaires. On dit alors que l'emblème est « utilisé à titre indicatif » . Lorsque l'emblème est utilisé à titre indicatif, il doit toujours être arboré avec le nom et les initiales de la composante du Mouvement qui l'utilise et être de petites dimensions.

La version originale de cet article a été publiée en anglais le 16 septembre 2021.

Voir aussi

- Helen Durham, *Les cyberopérations en période de conflit armé : 7 questions juridiques et politiques essentielles*, 26 mars 2020.

Tags: CICR, cristal rouge, croissant rouge, croix rouge, Croix-Rouge australienne, DIH, DIH coutumier, emblème distinctif, EPF Zurich, Johns Hopkins, Mouvement de la Croix-Rouge et du Croissant-Rouge

Ceci pourrait vous intéresser

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

Droit et conflits / Générer le respect du DIH Émilie Charpentier

Les conflits armés ont des conséquences à long terme sur les populations, même bien longtemps après la fin du conflt. Les organisations humanitaires ...

Le DIH et les territoires occupés

17 minutes de lecture

Droit et conflits / Générer le respect du DIH Tristan Ferraro & Mikhail Orkin

Alors que le conflit armé en Ukraine s'installe, les civils pris au piège de ce conflit subissent de plein fouet les effets des ...