DROIT & POLITIQUES
HUMANITAIRES

8 règles destinées aux « hackers civils » en temps de guerre et quatre obligations des États pour limiter leur action

janvier 12, 2024, Droit et conflits / Nouvelles technologies

16 minutes de lecture

Tilman Rodenhäuser
Conseiller juridique thématique, CICR

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

La technologie numérique fait évoluer la manière dont les armées conduisent leurs opérations en temps de guerre, ce qui s'accompagne d'un nouveau *phénomène préoccupant* : l'augmentation du nombre de civils qui participent à des conflits armés à travers des outils numériques. Se tenant à une certaine distance de la zone de combat, voire à l'extérieur des pays en guerre, ces civils peuvent être des « hacktivistes », des professionnels de la cybersécurité ou des « chapeaux blancs », des « chapeaux noirs » ou des hackers « patriotiques », qui mènent toutes sortes de cyberopérations dirigées contre leur « ennemi ». Certains spécialistes *considèrent* que les civils sont les « cybercombattants par excellence », car « c'est dans le secteur privé (ou civil) que l'on trouve la grande majorité des compétences en matière de cyberdéfense ».

Les exemples de hackers civils opérant dans des situations de conflit armé sont aussi divers que nombreux (voir *ici*, *ici* et *ici*). Ainsi, dans le conflit armé international entre la Russie et l'Ukraine, certains groupes *se présentent* comme une « communauté mondiale d'informaticiens », dont la mission consiste, pour reprendre leurs propres termes, à « contribuer à la victoire de l'Ukraine en paralysant l'économie de l'agresseur, en bloquant des services financiers, des services d'infrastructure et des services publics essentiels, et en harcelant les contribuables les plus importants ». D'autres personnes *auraient* « incité à attaquer ou attaqué directement des sites internet d'hôpitaux en Ukraine et dans des pays alliés pour les déstabiliser, bien que temporairement » et on recense bien d'autres opérations de ce type. Comme de nombreux groupes mènent des actions dans ce domaine et que certains d'entre eux coordonnent, par leurs canaux, des milliers de pirates informatiques et fournissent à leurs membres des outils automatisés, la participation de civils à des opérations numériques lors de conflits armés a pris des proportions sans précédent.

Ce n'est pas la première fois (et sans doute pas la dernière) que des hackers civils opèrent dans des situations de conflit armé. Dans cet article, notre objectif est d'expliquer pourquoi ce phénomène devrait alerter les États comme les sociétés. Nous présentons ainsi 8 règles fondées sur le droit international humanitaire que doivent respecter tous les pirates informatiques menant des opérations en temps de guerre, en rappelant qu'il relève de la responsabilité de l'État de limiter leur action.

Un phénomène préoccupant : quand des civils prennent part à la guerre numérique

Le phénomène des hackers civils qui conduisent des cyberopérations pendant un conflit armé est préoccupant et ce pour au moins 3 raisons.

Premièrement, les hackers civils portent atteinte aux populations civiles, que ce soit en prenant directement pour cible des biens de caractère civil ou en leur causant incidemment des dommages. Certains *experts* considèrent avant tout les hackers civils et leurs réseaux comme des collectifs de « cyberautodéfense » (*cyber vigilantism*) et soulignent que leurs opérations ne sont guère élaborées sur le plan technique et présentent peu de risques d'entraîner des conséquences graves. Pourtant, il est également vrai que des hackers civils et des « armées » de ce type ont perturbé le fonctionnement de divers biens de caractère civil, y compris des banques, des entreprises, des pharmacies, des hôpitaux, des réseaux ferroviaires et des services publics.

Deuxièmement, les hackers civils courent le risque d'être affectés, ainsi que leur entourage, par des opérations militaires. Une partie à un conflit armé pourrait en effet considérer, selon le type d'opération qu'ils mènent, qu'ils participent directement aux hostilités (voir *ici* et *ici* pour des analyses concernant en particulier les cyberopérations). En d'autres termes, les ordinateurs et les infrastructures numériques qu'ils utilisent pourraient devenir des objectifs militaires, susceptibles d'être attaqués. De la même manière, aux yeux de l'adversaire et selon l'endroit où se trouve le pirate informatique, il pourrait lui-même être visé par des attaques, par arme à feu, au moyen d'un missile ou d'une cyberopération.

Troisièmement, plus des civils participent activement à la conduite des hostilités, plus la frontière qui permet de distinguer les civils des combattants s'estompe, ce qui accroit le risque de causer des dommages au sein de la population civile. Des *juristes* ont soulevé la question de savoir si le principe de distinction, principe fondamental du droit international humanitaire, résistera à ces changements.

8 règles destinées aux hackers civils menant des opérations dans le cadre d'un conflit armé

Le cyberespace n'est pas une zone de non droit : même la guerre a des limites.

Il va sans dire que les hackers civils sont tenus de respecter la législation des pays dans lesquels ils opèrent. Lorsque la législation nationale est faible ou qu'elle n'est pas appliquée, ou si un hacker civil décide de ne pas la respecter, le droit international humanitaire (DIH) fournit, en temps de conflit armé, un ensemble de règles universellement acceptées, destinées à protéger la population civile ainsi que les soldats hors de combat contre certaines des horreurs de la guerre. Les pires violations de ces règles constituent des *crimes de guerre*, passibles de poursuites nationales ou *internationales*.

En situation de conflit armé, le DIH n'interdit pas le « piratage informatique » en tant que tel, pas plus qu'il n'interdit aux civils de mener des cyberopérations contre des objectifs militaires. En revanche, le DIH formule des considérations élémentaires d'humanité relatives à la protection des civils, c'est-à-dire des obligations que chacun doit respecter dans la conduite d'opérations en temps de guerre, quelles que soient les raisons du conflit, même si l'on considère que les objectifs de telle ou telle partie sont légitimes, et qu'il s'agisse d'une opération défensive ou offensive.

Le DIH comporte des centaines de règles ; on trouvera ci-après un avertissement et 8 règles qui doivent être au minimum connues et respectées par toute personne menant une cyberopération dans le cadre d'un conflit armé (y compris les groupes armés non étatiques et les hackers civils). Les groupes ou les collectifs devraient veiller à ce que leurs membres respectent ces limites.

Avertissement : les hackers civils risquent de perdre leur protection contre les attaques, qu'il s'agisse de cyberopérations ou d'opérations cinétiques, et peuvent faire l'objet de poursuites pénales s'ils participent directement aux hostilités par des moyens cybernétiques.

Conformément au DIH, les civils ne doivent pas être attaqués, à moins qu'ils ne participent directement aux hostilités et pendant toute la durée de cette participation. Le fait de mener des cyberattaques contre des objectifs militaires ou civils peut constituer une « participation aux hostilités », ainsi, les hackers civils peuvent être attaqués. En outre, si les membres des forces armées d'un État (y compris les cyberopérateurs) ne peuvent pas être poursuivis pour avoir commis des actes de guerre licites (attaquer une installation militaire, par exemple) et ont le statut de « prisonniers de guerre » en cas de capture, ces règles ne s'appliquent pas aux hackers civils (voir *ici*, par. 3634 sur l'article 85 de la CG III). En cas de capture, il se peut qu'ils soient considérés comme des criminels ou des « terroristes » et poursuivis en conséquence.

1. Ne pas conduire de cyberattaques* contre des biens de caractère civil.

On entend par « biens de caractère civil » tous les biens qui ne sont pas des objectifs militaires, notamment les infrastructures civiles, les services publics, les entreprises, les biens privés, voire les données civiles. Les objectifs militaires ne bénéficient pas de la même protection. Les « objectifs militaires » comprennent principalement les infrastructures matérielles et numériques de l'armée d'un belligérant, mais peuvent aussi inclure des biens de caractère civil, s'ils sont utilisés par des forces armées et selon la manière dont ils sont employés.

2. Ne pas utiliser de logiciels malveillants ni d'autres outils ou techniques qui se propagent automatiquement et qui causent des dommages indiscriminés à des objectifs militaires et à des biens de caractère civil.

À titre d'exemple, les logiciels malveillants qui se propagent automatiquement, dont les effets se répandent et qui causent des dommages, sans distinction, aux objectifs militaires et aux biens de caractère civil, ne doivent pas être employés.

3. Faire tout ce qui est pratiquement possible pour éviter ou réduire les effets qu'une l'opération pourrait avoir sur les populations civiles au moment de la planification d'une cyberattaque.

Si, par exemple, votre objectif est de perturber les réseaux électriques ou ferroviaires utilisés par des forces armées, vous devez éviter ou réduire les effets que votre opération pourrait avoir sur la population civile. Il est essentiel, avant de lancer une opération, d'analyser et de comprendre ses conséquences, sans oublier ses effets involontaires. Durant la planification d'une cyberattaque contre un objectif militaire, vous devez faire tout ce qui est pratiquement possible pour éviter ou réduire au minimum les effets que votre opération pourrait produire sur les civils, et interrompre l'attaque si les dommages causés aux civils risquent d'être excessifs. Si vous avez réussi à pénétrer un système d'exploitation, mais que vous ne saisissez pas les conséquences possibles de votre opération, ou si vous comprenez que les dommages causés aux civils risquent d'être excessifs, abandonnez l'opération.

4. Ne pas conduire de cyberopération contre des infrastructures médicales ou humanitaires.

Les hôpitaux et les organisations de secours humanitaires ne doivent jamais être pris pour cible.

5. Ne pas conduire de cyberattaque contre des biens indispensables à la survie de la population civile ou qui pourraient libérer des forces dangereuses.

Le droit international humanitaire définit les ouvrages ou installations contenant des forces dangereuses comme « les barrages, les digues et les centrales nucléaires de production d'énergie électrique » ; en réalité, toutefois, les industries chimiques ou toute autre installation de ce type contiennent aussi des forces dangereuses. Les biens indispensables à la survie de la population civile comprennent, entre autres, les réseaux d'eau potable ou les systèmes d'irrigation.

6. Ne pas diffuser de menaces de violence dont le but est de répandre la terreur parmi la population civile.

Il est interdit, par exemple, de pirater des systèmes de communication pour publier des informations dont le but principal est de répandre la terreur parmi les populations civiles. De la même manière, le droit interdit de concevoir et de diffuser des contenus explicites destinés à répandre la terreur parmi la population afin de l'inciter à fuir.

7. Ne pas inciter à commettre des violations du droit international humanitaire.

N'encouragez pas ou ne donnez à d'autres pas les moyens de mener des cyberopérations ou d'autres types d'opérations dirigés contre des civils ou des biens de caractère civil. Par exemple, ne partagez pas d'informations techniques sur des canaux dans l'objectif de faciliter des attaques contre des infrastructures civiles.

8. Respecter ces règles même si l'ennemi ne les respecte pas.

La vengeance ou la réciprocité ne sauraient justifier des violations du droit international humanitaire.

* Aux termes du DIH et dans le cadre des cyberopérations, la *notion d'attaque* recouvre des cyberopérations dont on peut raisonnablement attendre qu'elles causent — directement ou indirectement — des dommages, la mise hors service ou la destruction de biens (tels que des infrastructures, voire des données), ou des blessés ou des morts. Elle n'inclut pas, par exemple, les cyberopérations destinées à obtenir un accès à des informations sans autorisation.

Pour en savoir plus sur la position du Comité international de la Croix-Rouge relative au DIH et aux cyberopérations, voir *ici* et *ici*. Pour plus d'informations sur la manière dont le droit international s'applique dans le cyberespace, consultez-le « *Cyber Law Toolkit* ».

Les pirates informatiques ne vivent pas dans le cyberespace ; les États doivent fixer des limites

Les États ne devraient pas encourager ni tolérer que des cyberopérations soient menées par des hackers civils dans le cadre de conflits armés.

La multiplication des cyberopérations conduites par des hackers civils accroît le risque que des opérations constituent des violations du droit applicable et brouillent la frontière permettant de distinguer les civils des combattants. Le CICR a donc appelé les États à « *réfléchir au danger qu'ils font courir aux civils avant de les encourager à participer à des cyberopérations militaires [...] ou d'exiger d'eux une telle participation* ».

D'un point de vue juridique, la totalité des États se sont engagés à ne pas permettre sciemment que leur territoire soit « utilisé pour commettre des faits internationalement illicites à l'aide des technologies de l'information et des communications » (*voir ici*, par. 13, c)). Bien qu'elle prenne la forme d'un

engagement politique, cette norme reflète l'obligation de « diligence raisonnable » qui incombe aux États en vertu du droit international, y compris à l'égard des hackers civils opérant à partir de leur territoire (voir *ici*). Un État qui s'engage à respecter l'État de droit ou un « ordre international fondé sur des règles » ne saurait fermer les yeux lorsque des personnes mènent, sur son territoire, des cyberopérations qui enfreignent le droit national ou international, même si elles sont dirigées contre un adversaire.

Il convient donc, avant tout, d'adopter et de faire respecter les législations nationales qui réglementent le piratage informatique civil.

En outre et eu égard en particulier au comportement de personnes privées en temps de guerre, les États se sont engagés à respecter et à faire respecter le DIH. Cet engagement juridique implique au moins quatre éléments :

Premièrement, si des hackers civils agissent sur instruction, sous la direction ou sous l'autorité d'un État, ce dernier est responsable, au regard du droit international, de tout comportement de ces personnes qui ne serait pas conforme aux obligations juridiques internationales lui incombant, y compris au titre du droit international humanitaire (voir *ici*, article 8, et *ici*). À titre d'exemple, si un État utilise des personnes privées ou des groupes comme « volontaires » et les charge de mener des cyberopérations particulières constituant des violations du droit international, l'État est juridiquement responsable de ces violations (voir *ici*, article 8, par. 2, cette responsabilité s'ajoute à l'éventuelle responsabilité pénale du pirate informatique privé).

Deuxièmement, les États ont l'obligation de ne pas encourager des personnes ou des groupes à agir en violation du droit international humanitaire (voir *ici*, par. 220). Concrètement, cela signifie que les agents de l'État — qu'il s'agisse de membres de l'armée, des services de renseignement ou de toute autre institution de l'État — ont l'interdiction d'encourager des personnes ou des groupes, par exemple, à diriger des cyberattaques contre des biens de caractère civil, quels que soient les canaux ou les applications utilisés à cette fin.

Troisièmement, les États ont une obligation de diligence raisonnable en matière de prévention des violations du droit international humanitaire qui pourraient être commises par des hackers civils se trouvant sur leur territoire (voir *ici*, par. 183). Certes, un État ne peut pas prévenir toutes les infractions, mais il doit prendre toutes les mesures pratiquement possibles (par exemple *prendre publiquement position* pour exiger des hackers civils qu'ils ne conduisent pas de cyberopérations en lien avec des conflits armés ou qu'ils respectent le DIH le cas échéant) et réprimer les violations conformément à la législation nationale (voir ci-après).

Quatrièmement, les États sont tenus de poursuivre les crimes de guerre et de prendre les mesures nécessaires pour réprimer les autres violations du DIH (articles *49*/*50*/*129*/*146* des CG I-IV ; article *85* du Protocole additionnel I). À cette fin, ils doivent en premier lieu adopter et appliquer les lois nécessaires pour que les cyberopérations qui constituent des crimes de guerre soient érigées en infractions pénales et, dans un deuxième temps, prendre des mesures efficaces pour faire cesser toutes les autres violations du DIH, qu'il s'agisse de mesures juridiques, disciplinaires ou administratives. De toute évidence, aussi longtemps que la question des cyberopérations conduites par des hackers civils et dirigées contre « l'ennemi » ne sera pas sérieusement prise en compte dans les législations ou les politiques adoptées par les États, cette obligation ne sera pas respectée.

***

Le DIH fixe des règles fondamentales pour limiter les effets des conflits armés sur les populations civiles. Ces règles s'imposent à tous ceux qui participent au conflit et, en particulier, à tout pirate informatique menant des opérations dans le cadre d'un conflit armé. Les États doivent veiller à ce que ces règles soient bien respectées, pour protéger les populations civiles et éviter qu'on leur porte atteinte.

Cet article a été initialement publié en anglais le 4 octobre 2023 et est également disponible sur le site *EJIL:Talk!* *ici*.

Voir aussi

- Joelle Rizk, Sean Cordey, *Les menaces numériques dans les conflits armés : ce qui nous échappe et comment y remédier*, 2 octobre 2023.

Tags: Conventions de Genève, cyberguerre, hackers civils, technologies numériques

Ceci pourrait vous intéresser

Les menaces numériques dans les conflits armés : ce qui nous échappe et comment y remédier

22 minutes de lecture

Droit et conflits / Nouvelles technologies Joelle Rizk & Sean Cordey

Le développement et le recours à de nouvelles technologies numériques dans les conflits contemporains – des technologies de l'information aux cyberopérations, créent de …

Un filet de protection pour les prisonniers de guerre : cinq principes fondamentaux de la Troisième Convention de Genève

14 minutes de lecture

Droit et conflits / Nouvelles technologies Yvette Issar

Après la Seconde Guerre mondiale, les États ont œuvré ensemble afin d'améliorer la protection juridique accordée à certaines catégories de personnes, en particulier …