LE RUBICON

La protection des civils dans un contexte de numérisation et de « civilianisation » des conflits armés : un continuum d'obligations internationales

Aude Géry, Marie-Gabrielle Bertran | 9 novembre 2023 | ARTICLES |

Le 4 octobre 2023, deux conseillers du Comité international de la Croix-Rouge (CICR) ont publié un article intitulé « *8 rules for "civilian hackers" during war, and 4 obligations for states to restrain them* ». La publication est loin d'être passée inaperçue. Elle a suscité des réactions de la part de groupes de hackers et a fait l'objet de plusieurs articles dans la presse généraliste et spécialisée. Or, tant la publication que les réactions sont intéressantes au regard de ce qui est écrit et dit et de ce qui ne l'est pas : l'espace numérique n'est pas une zone de non droit, et seule une réflexion globale sur le continuum des responsabilités et obligations entre les différents acteurs prenant part, directement ou non, aux hostilités dans le cyberespace, peut conduire à une meilleure protection des civils et biens civils en temps de conflit armé.

Le contexte : un phénomène de numérisation et « civilianisation » des conflits armés

L'invasion de l'Ukraine par la Fédération de Russie le 24 février 2022 a donné lieu à un intérêt renouvelé pour l'utilisation des capacités numériques dans le cadre d'un conflit armé. Cet usage du numérique à des fins militaires ne s'est pas cantonné à la conduite d'attaques informatiques. Il a pris d'autres dimensions, parmi lesquelles la mise en œuvre de campagnes de désinformation, la collecte d'informations en sources ouvertes, la fourniture de services ou technologies ou encore la manipulation de la connectivité dans des territoires occupés. La présence croissante du numérique dans ce conflit a surtout contribué à un phénomène de « civilianisation » de la guerre, en faisant augmenter le nombre de civils impliqués dans les hostilités.

Parmi les manifestations de ce phénomène, l'implication de civils (pirates informatiques, cybercriminels, *etc.*) dans la conduite d'attaques informatiques contre les systèmes d'information de parties au conflit est l'une des plus visibles. D'après un décompte publié le 27 février 2022 par le chercheur en cybersécurité connu sous le pseudonyme de Cyberknow, on comptait environ neuf groupes ayant perpétré des cyber-attaques en faveur de l'Ukraine et neuf autres en faveur de la Russie, auxquels s'ajoute un

groupe aux revendications qui étaient inconnues. D'après son dernier décompte publié le 20 juillet 2023, on compterait environ cent-vingt-huit groupes engagés sur le plan cyber du conflit, dont soixante-douze engagés en faveur de la Russie, cinquante-et-un engagés en faveur de l'Ukraine et cinq groupes aux revendications inconnues. En juillet dernier, l'augmentation du nombre de groupes de cyberattaquants engagés dans le conflit russo-ukrainien s'élevait donc à plus de 600%, auxquels il faut rajouter les individus qui agissent de manière autonome et ponctuelle en participant à telle ou telle attaque informatique. L'engagement des « hackers civils » dans le volet cyber des conflits n'est pas nouveau. Leur implication a déjà été observée dans la guerre du Haut-Karabagh ou face à l'organisation État islamique. Les mêmes tendances reparaissent dans le cadre du conflit israélo-palestinien. Les affrontements de grande ampleur initiés par la Russie en Ukraine depuis 2022 ont toutefois constitué une véritable rupture au regard du nombre sans précédent de « hackers civils » impliqués.

Les données disponibles sur ces groupes et leurs activités ne sont pas sans laisser le juriste songeur. L'existence d'un conflit armé, international ou non-international, déclenche l'application d'un corps spécifique de règles, le droit international humanitaire (DIH). Or l'implication croissante des civils dans les conflits armés a des conséquences directes sur la mise en œuvre du DIH, notamment dans la conduite des hostilités, qui, en son cœur, pose la règle de la distinction entre civils et combattants et biens de caractère civil et objectifs militaires. En se rapprochant des hostilités, les civils sont plus susceptibles d'être pris pour cibles et de perdre la protection qui leur est accordée. Ces risques sont une préoccupation croissante du CICR.

La publication de l'article des conseillers du CICR intervient donc dans un contexte où la sensibilisation au DIH et au respect de ses règles, y compris auprès de nouveaux acteurs, est plus que jamais nécessaire. L'applicabilité du droit international aux activités cyber fait consensus. Il existe toutefois de nombreux débats sur les modalités de son application. De plus, la question de l'application du DIH reste contestée par certains États. Leur article s'inscrit donc dans un effort de diffusion du DIH, y compris auprès de nouveaux acteurs de la conflictualité. Les réactions qu'ont suscité l'article montrent toutefois que le chemin est encore long en matière d'application du droit dans l'espace numérique.

L'article de Tilman Rodenhäuser et Mauro Vignati se décompose en deux parties. Dans une première partie, les deux auteurs listent et explicitent huit règles que, selon eux, les « hackers civils » doivent suivre lorsqu'ils s'impliquent dans un conflit armé. Dans une seconde partie, ils s'attachent à identifier quatre obligations opposables aux États parties et non parties à un conflit et relatives aux activités susmentionnées. En revanche, ils passent sous silence ce qui constitue le troisième aspect des activités décrites, à savoir l'implication passive ou active de sociétés dans ces activités. Or chacune de ces dimensions mérite d'être analysée distinctement, tant du point de vue des réactions et des silences que des obligations elles-mêmes.

Une posture de défiance des « hackers civils » face à des règles pourtant garantes de leur protection

L'article porte sur des activités menées par une grande diversité d'acteurs. L'expression de « hackers civils » est utilisée pour désigner l'ensemble des groupes ou individus qui exécutent des attaques informatiques en lien avec un conflit, sans nécessairement se trouver sur le territoire de ce conflit et sans faire partie d'une institution militaire ou étatique. Ils rangent parmi cette catégorie d'acteurs les hacktivistes (des militants politiques qui utilisent les cyberattaques comme un outil de protestation ou de contestation), les professionnels de la cybersécurité et divers pirates informatiques (« hackers éthiques », cybercriminels et « hackers patriotes » qui s'engageraient dans le champ cyber d'un conflit pour soutenir l'entreprise de guerre ou de défense de leur gouvernement).

Pour les deux auteurs, le rôle non négligeable de ces acteurs dans le volet cyber des conflits actuels induit un effort de diffusion du DIH auprès d'eux pour deux raisons :

1. assurer une meilleure protection des populations et biens de caractère civil, conformément au principe de distinction ;
2. assurer la protection même de ces acteurs dont le rôle actif dans le champ cyber de la guerre peut leur faire perdre leur protection en tant que civils et en faire des cibles potentielles au cours des hostilités, sans qu'ils bénéficient nécessairement des protections offertes aux membres des forces armées des belligérants.

Pour ce faire, les auteurs listent un ensemble de huit règles qui doivent être respectées et appliquées par les « hackers civils » eux-mêmes. Ils y énoncent explicitement les pratiques à adopter ou à proscrire, en comparant les pratiques mises en œuvre avec celles qui seraient acceptables conformément au DIH.

Les huit règles basées sur le DIH que les « hackers civils » doivent suivre :

1. Ne pas conduire de cyberattaques contre des objets civils.

Par « cyberattaques », ils entendent les « opérations cyber qui peuvent raisonnablement être considérées comme pouvant résulter, directement ou indirectement, en des dommages, mises horsservice ou destructions d'objets (tels que des

infrastructures [ou des] données) », voire provoquer des blessures ou la mort d'individus. Cette définition ne prend pas en compte les « opérations cyber qui visent à obtenir illégalement accès à des informations. ».

2. Ne pas utiliser de programmes malveillants ou autres outils et techniques qui se propagent de manière automatique et portent atteinte à des objectifs militaires et des objets civils de façon indiscriminée.
3. Faire en sorte d'éviter ou de minimiser les effets qu'une opération pourrait avoir sur les civils au moment de la planification d'une cyberattaque contre un objectif militaire.
4. Ne conduire aucune opération cyber contre des bâtiments médicaux et humanitaires.
5. Ne conduire aucune cyberattaque contre des objets indispensables à la survie de la population ou pouvant libérer des « forces dangereuses ». Suivant le DIH, ces objets comprennent les « barrages, digues et centrales nucléaires ». Les auteurs ajoutent à cette liste les usines industrielles et chimiques qui peuvent contenir et libérer de telles « forces dangereuses ».
6. Ne pas diffuser de menaces de violence ou répandre la terreur parmi les populations civiles.
7. Ne pas inciter à des violations du DIH.
8. Respecter ces règles même si l'ennemi ne le fait pas.

Malgré l'objectif annoncé de protection de ces acteurs des conflits, la publication de ces huit règles a suscité de vives réactions parmi les groupes engagés dans la guerre russo-ukrainienne. Le jour même de la publication, KillMilk, le dirigeant officiel du groupe russe et prorusse KILLNET connu pour ses attaques de déni de service distribué (DDoS), déclarait dans un entretien à la BBC « pourquoi devrais-je écouter la Croix-Rouge ? ». Un autre groupe d'attaquants prorusse interrogé par la BBC, Anonymous Sudan, déclarait dans le même temps que les règles n'étaient « pas viables » et que les enfreindre était « inévitable ».

Du côté des acteurs engagés en faveur de l'Ukraine, l'un des principaux membres d'Anonymous International déclarait à son tour à la chaîne britannique que son groupe avait « toujours mené ses opérations en respectant certains principes, dont les règles citées par le CICR ». Il ajoutait néanmoins avoir « perdu foi en l'organisation » humanitaire et ne pas avoir l'intention de « suivre ses nouvelles règles ». Plus grave, un pirate informatique ukrainien connu sous le pseudonyme de Hdr0 a attaqué et défacé le site *web* de la Croix-Rouge russe dans la matinée du 4 octobre, pour protester contre des actes malveillants qu'il attribuait à des représentants de l'organisation humanitaire en Russie. D'après le témoignage d'un infirmier cité par l'attaquant, certains représentants de la branche russe du CICR avaient humilié des prisonniers et des blessés ukrainiens. Hdr0 affirmait également dans un message posté sur Telegram : « [i]l n'y a pas de règles dans la guerre. Et la Croix-Rouge, couverte du sang de nos soldats captifs et des larmes de nos enfants, n'a aucune autorité pour suggérer ou établir quoi que ce soit », avant d'ajouter « [n]ous profiterons de chaque opportunité pour causer le plus de dommages possibles à notre ennemi en utilisant tous les moyens à notre disposition ».

Les règles énoncées dans l'article ont donc d'abord été rejetées dans un contexte où les belligérants sont apparus comme ne respectant pas eux-mêmes le DIH en matière d'attaques informatiques. Nombre d'infrastructures civiles ont en effet été ciblées au moyen d'attaques informatiques par les deux camps, telles que des centrales électriques et nucléaires en Ukraine et en Russie, ou des systèmes de transport ferroviaire en Biélorussie. Ces attaques informatiques, dont la licéité peut faire l'objet de nombreux débats, ont sans doute incité les acteurs à augmenter la fréquence et l'impact de leurs attaques par rapport aux opérations cyber qu'ils auraient pu mener en temps de paix.

Les propos tenus dans un premier temps par les membres de l'IT Army of Ukraine sur leur canal Telegram témoignent de leur crainte de perdre en puissance de frappe sur le plan cyber en appliquant les règles énumérées dans l'article. Dans un message posté le 4 octobre, un membre de cette organisation affirmait notamment : « [t]ant que les Russes ne suivront pas ces règles, nous ne le ferons pas non plus. Cela nous mettrait dans une position délicate : ils peuvent, nous ne pouvons pas. Étrange logique ». Cette position en contradiction avec la huitième règle de l'article était largement partagée d'après les discussions engagées sur les canaux Telegram de différents groupes. Sur son canal Telegram personnel (@ruheight), le porte-parole de la *Ukrainian Cyber Alliance* (UCA), Sean Townsend, avait affiché une position similaire quelques heures auparavant : « [s]ur leurs huit règles, il peut en rester deux : ne pas tuer de civils en grand nombre, même si l'ennemi est constitué de cannibales et de meurtriers. […] Évidemment, les hôpitaux, chemins de fer, centrales électriques, communications et autres infrastructures "civiles" et "critiques" sont les cibles principales et légitimes des pirates informatiques, tant civils que militaires. Elles doivent être détruites. *Le cyber est l'un des moyens les plus humains pour y parvenir* ». Il affirmait en outre ne pas avoir « besoin de la "protection" que les conventions accordent aux civils ».

Ces positions hostiles ou sceptiques de l'ensemble des acteurs ont évolué dans les jours qui ont suivi. Le dirigeant du groupe KILLNET a publié une traduction en russe des huit règles de l'article sur son canal Telegram le matin du 6 octobre, indiquant : « [a]ujourd'hui, KILLNET fait le premier pas vers la paix ! C'est pourquoi nous écoutons la Croix-Rouge et nous engageons à respecter ces règles ! ». Le porte-parole de l'IT Army a contacté la BBC dans la journée, affirmant que le groupe ferait également

de son mieux pour respecter les règles. D'abord encourageantes, ces déclarations ont rapidement été démenties par différents piratages menés par les deux groupes. Une semaine seulement après ses déclarations, KILLNET publiait sur son canal Telegram une photographie indiquant qu'il avait piraté le système d'information d'une entreprise du secteur gazier de la région de Kiev et dérobé les données présentes sur ses serveurs, jouant ainsi explicitement avec les limites des règles 1 et 5 de l'article publié par les conseillers du CICR. Cette cyberopération a non seulement ciblé un « bien civil », mais aussi un système d'information possiblement lié à une infrastructure « indispensable à la survie de la population » susceptible de « libérer des forces dangereuses ». D'après les attaquants, l'opération n'a résulté qu'en un vol de données, sans que l'on sache s'il s'agissait du système industriel lui-même. On serait donc en-dessous du seuil *stricto sensu* de la « cyber-attaque » au sens du DIH, même si le statut des données civiles fait l'objet de nombreux débats, surtout lorsqu'elles appartiennent à des infrastructures faisant l'objet d'un statut spécial. Le même jour, l'IT Army annonçait avoir mis hors service les infrastructures du fournisseur d'accès à l'Internet russe Evpanet, ce qui là aussi interroge au regard de la règle 5.

Malgré des déclarations certainement destinées à soigner leur image auprès de la communauté internationale, le chemin reste encore long pour que les « hackers civils » respectent les obligations qui leurs sont opposables et qui servent notamment à les protéger. Dans ce contexte, les États parties au conflit et tiers ont un rôle particulier à jouer.

Le rôle clé des obligations des États parties au conflit et tiers

La seconde partie de l'article publié par les conseillers du CICR porte sur les obligations qu'ont les États à l'égard des activités offensives menées par des « hackers civils » dans le cadre d'un conflit armé. Or, cette partie de l'article n'a que très peu attiré l'attention, alors même qu'elle constitue un élément clé de l'organisation de la protection des civils à l'ère numérique en temps de conflit armé.

Ce silence de la part des intéressés n'est guère surprenant. On imagine mal les États réagir à un tel article. De même, il n'est guère étonnant que les « hackers civils » n'aient pas répondu à cette partie de l'article. D'une part, ils ne sont pas les débiteurs de ces obligations. D'autre part, il aurait été pour le moins incongru qu'ils rappellent aux États leurs obligations en matière de prévention et de répression de leurs propres activités. Mais la presse ayant relaté l'article n'a également pas mis en avant cette partie du post de blog, alors même qu'elle avait pu se faire l'écho il y a plusieurs mois de quelques avertissements diffusés par les États eux-mêmes à propos des activités cyber offensives privées. Or, dans un objectif de protection des civils, ces obligations sont particulièrement importantes.

Premièrement, les auteurs rappellent que les États ne peuvent laisser ces acteurs agir sur et depuis leur territoire en toute impunité. Ainsi, l'existence d'obligations pesant sur les individus et groupes désignés n'obèrent pas les obligations opposables aux États sur le territoire desquels ils produisent des effets ou sous la juridiction desquels ils se trouvent. Le non-respect des obligations mentionnées en première partie de l'article n'implique pas que les États susvisés échappent à toute responsabilité. Dans le cadre du conflit ukrainien, plusieurs groupes impliqués sont connus pour avoir des liens plus ou moins étroits avec l'une ou l'autre des parties au conflit. À titre d'exemple, un groupe russophone appelé *The Red Bandits* et se présentant comme un groupe de cybercriminels a été très actif au début de l'invasion de l'Ukraine. Des recherches indiquent toutefois qu'il pourrait s'agir d'agents des services de renseignement russes. Il en va de même pour un groupe tel que *XakNet Team*, qui a finalement été rattaché aux services de renseignement militaires russes. Côté ukrainien, des travaux font état de liens très étroits entre l'IT Army et les services de renseignement ukrainiens. Juridiquement, la qualification en droit de ces groupes interroge et les liens de rattachement existant entre ces groupes et les parties au conflit soulèvent d'importantes questions de responsabilité des États eux-mêmes. Quel que soit l'intérêt à laisser ces acteurs agir en dehors de toute structure hiérarchique étatique, les obligations des États, parties ou non à un conflit, rappellent qu'ils ont un rôle à jouer dans la protection des civils.

Deuxièmement, le numérique bouleverse la territorialisation des conflits en permettant à des individus, au-delà de ce que l'on avait pu voir en matière de drones, de s'immiscer dans un conflit armé tout en étant en dehors de son champ géographique, c'est-à-dire en agissant depuis le territoire d'un État non-partie à ce conflit armé. La numérisation et la déterritorialisation des hostilités confèrent un rôle particulier à l'obligation qu'ont les États de respecter et de faire respecter le DIH en toutes circonstances, obligation coutumière énoncée à l'article 1 commun aux Conventions de Genève. Cette obligation est mise en œuvre à travers des obligations spécifiques (diffusion du DIH, organisation de son exécution en droit interne, poursuite des violations, *etc.*) mais implique également que les États « ont une certaine latitude dans le choix des mesures devant permettre de faire respecter les Conventions » (para. 146). Ainsi, les États non-parties à un conflit armé désigné ont l'obligation de s'assurer que les « hackers civils » situés sur leur territoire respectent le DIH. Ils doivent également amener les États (para. 153) qui font appel à ces acteurs ou les laissent agir à s'acquitter de leurs obligations dès lors qu'il peut être établi que les activités menées sont contraires au DIH. Un État depuis le territoire duquel un « hacker civil » agirait se voit donc opposer des obligations particulières et a un rôle à jouer dans la protection des civils d'un conflit armé. Compte tenu de la numérisation croissante des

conflits armés et des enjeux territoriaux que cela soulève, cette obligation, ainsi que toutes celles entrant en ligne de compte dans le fait pour un État d'encourager des acteurs non étatiques à agir, mérite donc une attention renouvelée.

Au-delà des obligations du DIH, ces enjeux territoriaux confèrent à d'autres branches du droit international un rôle particulier dans la protection des civils en cas de conflit armé. Ainsi, le droit du recours à la force, le droit international général, le droit international des droits de l'homme (DIDH) ou encore le droit de la neutralité font peser des obligations sur les États depuis le territoire desquels ces acteurs peuvent agir. Ces questions et l'articulation entre ces différentes branches du droit sont éminemment complexes et dépassent le cadre de cet article. Parmi les réflexions en cours, plusieurs auteurs se sont par exemple interrogés sur les obligations spécifiques découlant du droit de la neutralité (Conventions V et XIII de La Haye, CLH) au regard du recrutement et de la participation d'individus à des formations impliquées dans des conflits armés et des articles 4 et 6 CLH V, et de l'obligation de prévention et de répression des attaques informatiques sous l'angle de l'article 5 CLH V. À propos de cette dernière, rappelons qu'il s'agit d'une obligation de moyens et non de résultat. La question qui se pose est celle de savoir si, en matière cyber, le contenu de cette obligation est plus proche de celui s'appliquant en matière d'hostilités terrestres ou navales (art. 25 CLH XIII). En effet, en matière navale, les critères de mise en œuvre de l'obligation sont plus souples et laissent une plus grande marge de manœuvre à l'État débiteur de l'obligation. De même, la nature du critère de connaissance (actuelle ou constructive) nécessaire des activités litigieuses pour que l'obligation s'applique ne fait pas consensus. Peu d'États se sont exprimés sur le droit de la neutralité et sur cette obligation de prévention, à l'exception de la France, des États-Unis (sec. 15.3.2.2), de la Suisse et des Pays-Bas. Les positions exprimées informent toutefois peu sur le périmètre exact de cette obligation dans le cas d'étude qui nous intéresse.

Qu'il s'agisse d'obligations pesant sur un État partie au conflit ou tiers, le droit international contient de nombreuses obligations susceptibles d'intéresser les pratiques de « hackers civils ». Il peut donc être mobilisé à différents niveaux pour assurer une protection des civils dans un conflit armé. Cet objectif de protection des civils ne saurait toutefois être atteint sans s'intéresser à une troisième catégorie d'acteurs : les entreprises dont les biens et services sont utilisés.

Les responsabilités des entreprises dont les produits et services sont utilisés : un enjeu majeur

Pour mener leurs opérations, les « hackers civils » utilisent des biens et services fournis par des entreprises, parfois avec leur consentement explicite. Le cas de l'IT Army of Ukraine illustre bien ce phénomène. Le site internet de l'organisation fournit des instructions et liens vers différents outils permettant de mener des attaques par déni de service. Tous ces outils sont hébergés sur une plateforme de droit américain appelée GitHub. Or, la protection des civils ne peut être assurée qu'en prenant en compte le rôle joué par les entreprises fournissant ces services dans les attaques informatiques menées par ces acteurs, puisqu'elles en fournissent le support ou les moyens. Cette troisième dimension du droit mobilisable dans la protection des civils n'est pas abordée par l'article de T. Rodenhäuser et M. Vignati, mais elle en découle. Deux situations doivent être distinguées ici.

Du point de vue du droit international, les obligations en cause sont d'abord celles des États sous la juridiction desquels ces entreprises opèrent, rejoignant en cela les développements précédemment abordés. En raison du caractère transnational des réseaux et services proposés, la question de la responsabilité de certains États extérieurs au conflit se posera particulièrement dans la mesure où des entreprises qui y sont domiciliées voient leurs services largement utilisés par les belligérants. Ici aussi, l'articulation du droit de la neutralité et du droit de la sécurité collective sera un enjeu clé, notamment dans la définition du périmètre des obligations de prévention pouvant exister dans ces différentes branches du droit. Le DIDH pourra également être mobilisé puisque un État a non seulement l'obligation de respecter les droits de l'homme, mais également celle de les protéger, ce qui implique l'existence d'obligations positives visant à protéger les violations des droits de l'homme par des tiers relevant de sa juridiction. Dans notre cas d'étude, la dimension extraterritoriale de la situation compliquera l'interprétation des obligations en cause. Ici, il ne sera pas tant question d'application extraterritoriale des obligations dans l'hypothèse d'un contrôle effectif sur le titulaire des droits situé sur le territoire d'un autre État que d'application extraterritoriale en raison d'« un contrôle effectif sur une cause potentielle de préjudice à cette personne ».

Aux côtés des obligations des États, la question des obligations des entreprises elles-mêmes devient de plus en plus saillante. Elle n'est pas nouvelle, mais se renouvelle avec la numérisation des sociétés. Même si les entreprises ne sont généralement pas considérées comme des sujets de droit international, il est de plus en plus admis que certains instruments internationaux, notamment du DIDH, leur imposent des responsabilités juridiques directes. Pour ce qui est du DIH, une entreprise dont les activités sont étroitement liées à un conflit armé doit respecter le DIH et peut donc voir sa responsabilité civile ou pénale engagée si elle viole elle-même le DIH ou si elle contribue à des violations du DIH par les parties au conflit. La détermination de ces activités n'est toutefois pas chose aisée, puisque « les entreprises commerciales sont susceptibles de mener toute une série d'autres activités qui peuvent être plus ou moins liées à un conflit armé ». Dans les hypothèses envisagées, la question de la nature de la contribution et du lien de causalité avec une violation du DIH pour engager sa responsabilité est loin d'être évidente,

notamment selon le degré de passivité de l'entreprise.

Plusieurs initiatives ont émergé au sein de différentes organisations internationales (OCDE, OIT, ONU) pour mieux prendre en compte le caractère transnational des activités des entreprises et les responsabiliser face aux potentielles conséquences de leurs activités sur les droits de l'homme. Même si elles ne créent pas de nouvelles obligations juridiques pour les entreprises, on retrouve au cœur de cette responsabilité sociétale se trouve l'adoption de mesures de prévention et de réaction visant à empêcher les atteintes aux droits de l'homme. Face à l'implication croissante d'entreprises dans les conflits armés, le Programme des Nations Unies pour le développement a également publié un guide relatif au *Renforcement de la diligence raisonnable des entreprises en matière de droits humains dans les contextes marqués par des conflits*. Il détaille le concept de diligence raisonnable (*due diligence*) renforcée afin de prendre en compte les risques spécifiques aux conflits armés. La numérisation des conflits nécessite de s'intéresser de plus près à ces concepts et recommandations afin d'assurer la pleine protection des civils.

Conclusion

La protection des civils en temps de conflit armé n'est pas de la responsabilité d'un seul acteur mais relève d'un continuum d'obligations pesant sur une diversité d'acteurs. La numérisation des conflits et l'implication de « hackers civils » doivent conduire à une pédagogie et une sensibilisation renforcées quant aux droits et responsabilités des uns et des autres. Elle nécessite surtout une analyse plus poussée, non pas des obligations des seuls belligérants, mais aussi des tiers, y compris ceux dont les technologies sont utilisées.

Photo : gorodenkoff

•— ••— — • ••— •—• •••

Aude Géry, Marie-Gabrielle Bertran

Aude Géry (@AudeGery) est docteure en droit et chercheuse au sein du projet GEODE hébergé au sein de l'Institut français de géopolitique. Ses recherches portent sur l'application du droit international aux cyberopérations, notamment le droit de la sécurité internationale et le droit international humanitaire, mais aussi sur les politiques juridiques extérieures des Etats, le multilatéralisme en matière de TIC dans le contexte de la sécurité internationale et les enjeux normatifs des instruments portant sur le numérique.

Marie-Gabrielle Bertran est doctorante à l'Institut Français de Géopolitique (IFG-Lab) et jeune chercheuse du projet GEODE depuis septembre 2019. Son travail porte sur les nouvelles politiques de l'État russe en matière de souveraineté numérique et leurs conséquences sur les pratiques des développeurs russes, ainsi que sur les marchés du numérique russe et international.

Comment citer cette publication

Aude Géry, Marie-Gabrielle Bertran, « La protection des civils dans un contexte de numérisation et de "civilianisation" des conflits armés : un continuum d'obligations internationales », *Le Rubicon*, vol. 3, 9 novembre 2023 [https://lerubicon.org/la-protection-des-civils-dans-un-contexte-de-numerisation-et-de-civilianisation-des-conflits-armes-un-continuum-dobligations-internationales/].