L'APPLICABILITÉ DU DROIT INTERNATIONAL HUMANITAIRE À LA CYBERCONFLICTUALITÉ

Jean-Baptiste Jeangène Vilmer

Le droit international humanitaire (DIH) est l'ensemble des règles qui cherchent à limiter les effets des conflits armés, à la fois en protégeant les personnes et les biens et en limitant ou en interdisant certains moyens et certaines méthodes de guerre. Cet ensemble de règles s'appuie sur des principes fondamentaux qui sont ceux du *jus in bello* traditionnel : nécessité, distinction, proportionnalité, précaution et interdiction de causer des maux superflus. Appliqués au cas particulier de la cyberconflictualité, ils posent tous de nombreux problèmes – qui sont développés dans les autres chapitres. Je souhaite ici poser une question préalable : avant même de discuter de l'application de tel ou tel principe du DIH à la cyberconflictualité, ne faut-il pas d'abord montrer que le DIH lui-même s'applique ? C'est la question de l'applicabilité.

Elle se pose parce que le DIH, donc les principes en question, ne s'appliquent pas n'importe quand et à n'importe quoi : seulement en situation de conflit armé, international ou non international. Or, la cyberconflictualité a-t-elle toujours lieu en situation de conflit armé et, si ce n'est pas le cas, peut-elle constituer un conflit armé déclenchant l'applicabilité du DIH ?

Ici, nous nous heurtons à un problème terminologique : ce volume parle de cyberconflictualité, d'autres de cyberguerre ou cyberattaques, autant de mots qui ont une connotation guerrière – mais cela ne signifie pas que les opérations qu'elles désignent ont effectivement lieu en temps de guerre. La plupart du temps, elles ont lieu en temps de paix et toutes ne constituent pas des « attaques » au sens strict.

À cette réserve, il faut ajouter que la question de l'applicabilité du DIH à la cyberconflictualité pourrait être envisagée sous l'angle politique, puisqu'un certain nombre d'États ont exprimé des positions officielles à

ce sujet (l'applicabilité est reconnue par les États-Unis, le Royaume-Uni et l'Australie par exemple, mais apparemment pas par la Chine) (Droege, 2012). Toutefois, ces déclarations restant très vagues, l'objectif de ce chapitre est plutôt de l'envisager sous l'angle juridique.

Il faut alors distinguer deux cas de figure puisque les cyberattaques peuvent avoir lieu dans le cadre d'un conflit armé (en temps de guerre), où elles ne sont alors que l'un des moyens employés, ou en dehors d'un conflit armé (en temps de paix). Dans le premier cas, la réponse est consensuelle : le DIH s'applique, même si aucune de ses conventions, rédigées bien avant l'apparition du cyber, ne le mentionne (Melzer, 2012). Dans le second, elle l'est moins.

En situation de conflit armé

Si les cyberopérations ont lieu dans le cadre d'un conflit armé, elles ne sont que des moyens parmi d'autres, qui ont la particularité d'utiliser les technologies de l'information plutôt que l'énergie cinétique, c'est-à-dire la force physique. Mais cette particularité ne change rien à l'applicabilité du DIH, qui est déclenchée par l'existence d'un conflit armé et non par le type d'opérations en cours au sein de ce conflit.

Les cyberopérations peuvent avoir des conséquences humanitaires, dans la mesure où elles ont des effets indirects dans le monde dit « réel ». La manipulation par ordinateur du système de contrôle aérien, par exemple, des centrales nucléaires, des barrages, des usines de produits chimiques, du flux d'un gazoduc ou d'un oléoduc, ou tout simplement du système d'eau ou d'électricité des bâtiments civils, y compris des hôpitaux, peut faire des dizaines de milliers de victimes civiles. Pour l'instant (Estonie, Géorgie, Iran), ce n'est pas arrivé, mais c'est techniquement faisable. Pour cette raison, le DIH s'applique comme à n'importe quelle autre méthode ou moyen susceptible de violer ses principes.

Le fait que le DIH ne mentionne pas les cyberopérations et que celles-ci soient relativement nouvelles donne lieu à un préjugé répandu selon lequel il est mal adapté au cyber (comme à d'autres défis du XXI^{e} siècle, la robotisation et la privatisation par exemple). Il faut nuancer ce jugement.

Le DIH limite les effets de la guerre : que la cause soit nouvelle (non plus un avion mais un drone, non plus un missile mais une cyberattaque) ne change rien si ses effets sont les mêmes, c'est-à-dire si elle cause les mêmes dommages (des morts et des blessés). À partir du moment où les cyberattaques produisent indirectement, dans le monde réel, des effets réels qui sont les mêmes que ceux produits par des armes conventionnelles, elles sont gouvernées par les mêmes règles.

Que ces nouvelles technologies, celles existantes et celles à venir, sont bien prises en compte par le DIH est confirmé par l'article 36 du Protocole I aux Conventions de Genève : « Dans l'étude, la mise au point, l'acquisition ou l'adoption d'une nouvelle arme, de nouveaux moyens ou d'une nouvelle méthode de guerre, une Haute Partie contractante a l'obligation de déterminer si l'emploi en serait interdit, dans certaines circonstances ou en toutes circonstances, par les dispositions du présent Protocole ou par toute autre règle du droit international applicable à cette Haute Partie contractante. »

Cet article 36 pose toutefois plusieurs problèmes. D'abord, son interprétation est complexe comme en témoigne le *Guide de l'examen de licéité des nouvelles armes et des nouveaux moyens et méthodes de guerre* du CICR (2006). Ensuite, il ne s'applique pas aux systèmes de surveillance, alors qu'il est aisé de les armer (comme les Américains ont armé le Predator qui jusqu'en 2001 était un drone de surveillance). Enfin, il n'est pas certain qu'il s'applique seulement aux États parties au Protocole I, auquel cas il ne s'appliquerait pas à des États importants comme les États-Unis, Israël, le Pakistan, l'Inde ou la Turquie, ou s'il relève du droit coutumier et engage donc tous les États indépendamment de l'état de ratification des traités, comme le pense le CICR, ou encore s'il doit être considéré comme une simple bonne pratique.

Quoiqu'il en soit, contrairement à un préjugé commun (le premier des cinq « mythes » distingués par Schmitt), le monde cyber n'est pas hors-la-loi et les cyberopérations en temps de guerre ne sont pas dans un vide juridique. Le DIH les couvre comme n'importe quelle méthode ou moyen, avec les difficultés habituelles bien sûr, mais il les couvre et c'est précisément ce que montre le fameux manuel de Tallinn (Schmitt, 2013).

Ceci étant dit, le cyberespace présente tout de même quelques particularités qui rendent non seulement l'application mais même l'applicabilité du DIH plus difficiles.

L'anonymat

Il est souvent difficile de tracer l'origine d'une cyberattaque. Quand bien même aurait-on identifié la machine et son emplacement géographique, cela ne dit pas encore qui se trouve derrière le clavier et si cette personne la contrôle et a lancé l'attaque ou si celle-ci s'est faite à son insu, auquel cas il faut chercher la source ailleurs.

Cela pose un problème d'attribution de la responsabilité, qui n'est pas unique en DIH (c'est parfois difficile aussi avec des armes cinétiques, comme en témoigne le cas de l'attaque chimique syrienne du 21 août 2013, où un faisceau d'indices pointe vers Damas, mais aucune preuve

irréfutable n'a encore été produite), mais atteint ici une intensité remarquable, qui est encore compliquée par la nature du responsable, qui peut être un individu agissant seul, pour un groupe indépendant d'un État ou travaillant pour un État, ou encore qui peut être un service étatique directement. Et, contrairement aux opérations cinétiques, l'origine géographique de l'attaque n'est pas d'une grande aide puisqu'une attaque émanant d'un ordinateur situé en Angleterre peut en réalité avoir été lancée par un individu se trouvant au Pakistan, contrôlant la machine à distance et agissant pour le compte du gouvernement iranien.

Ce problème d'attribution de la responsabilité ne concerne pas que la question ultérieure de l'éventuelle poursuite des criminels de guerre (et celle de l'applicabilité de la dissuasion au cyber), il joue un rôle dans la question qui nous intéresse ici : celle de l'applicabilité du DIH. Car, pour que le DIH puisse être applicable à une opération quelconque, par exemple une cyberattaque, il faut non seulement qu'elle se fasse dans le contexte d'un conflit armé mais encore en lien avec lui. C'est ce qu'on appelle le lien de belligérance. Et c'est une condition *sine qua non*.

Le DIH, en effet, ne s'applique pas à des actions commises dans un contexte de conflit armé mais sans lien avec lui, par exemple à des crimes de droit commun, exécutés par des personnes privées ou des organisations criminelles qui ne peuvent pas être considérées comme parties au conflit dans le sens où elles ne cherchent pas à avantager une partie au détriment de l'autre. En l'occurrence, une cyberattaque qui serait faite dans un pays en conflit armé mais sans lien de belligérance (pour s'enrichir seulement, ou faire de l'espionnage industriel au profit d'une entreprise privée) ne relèverait pas du DIH. Donc, le fait de ne pas pouvoir identifier l'origine de l'attaque empêche de savoir s'il y a, ou pas, lien de belligérance et si le DIH s'applique.

L'interconnectivité

Le fait que les ordinateurs soient en réseau, reliés les uns aux autres et, surtout, que les ordinateurs militaires qui pourraient être des cibles militaires légitimes soient plus ou moins directement reliés au réseau civil, qui lui n'est pas une cible militaire légitime, pose problème : comment dans ces conditions serait-il seulement possible de respecter les principes du DIH ? Cela pose la question de l'applicabilité non plus *de jure* mais *de facto* : quand bien même le DIH *devrait* s'appliquer à certaines cyberattaques, est-il seulement *possible* de le faire ?

Comment par exemple appliquer le principe de distinction ? Il commande de ne viser que des objectifs militaires. Dans le cas d'une cyberattaque, cela veut dire les systèmes informatiques des infrastructures

militaires seulement – pas celles des infrastructures civiles (habitations, commerces, écoles, hôpitaux, etc.). Mais le problème est que l'interconnectivité relie les deux : les systèmes informatiques des infrastructures militaires ne sont généralement pas totalement isolés du reste. L'usage d'un ver qui a comme caractéristique de se répliquer et se propager lui-même de manière incontrôlable ne permet pas de garantir qu'il n'aura d'effet que sur des objectifs militaires, qu'il n'affectera pas des infrastructures civiles et, par conséquent, qu'il ne violera pas le DIH. Il pourrait même affecter les systèmes d'autres États, neutres ou amis, ce qui pose des problèmes de *jus ad bellum*. Par ailleurs, il y a aussi des systèmes qu'on appelle duals et qui servent par nature à la fois aux civils et aux militaires, comme les réseaux de télécommunication.

Comment également appliquer le principe de précaution ? En faisant une évaluation de cette interconnectivité précisément : le système informatique cible est-il suffisamment séparé du réseau civil ? Le risque de propagation est-il élevé ? Cette imbrication civilo-militaire remet aussi en cause l'applicabilité de certaines provisions du DIH, l'article 58 du Protocole I, par exemple, selon lequel les parties au conflit doivent s'efforcer « d'éloigner du voisinage des objectifs militaires la population civile, les personnes civiles et les biens de caractère civil soumis à leur autorité » et éviter « de placer des objectifs militaires à l'intérieur ou à proximité des zones fortement peuplées ». En l'espèce, est-il seulement possible d'éloigner le civil du militaire quand ils ne sont pas des objets physiques mais des réseaux informatiques ?

Le principe de précaution commanderait, lorsque l'on installe une base militaire ou n'importe quelle infrastructure qui pourrait être considérée comme un objectif militaire, qu'on sépare autant que possible les ordinateurs civils des militaires, qu'on protège en somme le réseau civil en ne le mêlant pas au militaire. Or, la tendance est apparemment l'inverse : une interconnectivité toujours croissante entre réseaux civils et militaires – c'est-à-dire, pour ce qui nous concerne, une applicabilité toujours plus difficile du DIH.

Ruse ou perfidie ?

La distinction entre la ruse et la perfidie est importante car la première est légale et la seconde illégale. Les ruses de guerre sont des « actes qui ont pour but d'induire un adversaire en erreur ou de lui faire commettre des imprudences, mais qui n'enfreignent aucune règle du droit international applicable dans les conflits armés et qui, ne faisant pas appel à la bonne foi de l'adversaire en ce qui concerne la protection prévue par ce droit, ne sont pas perfides ». Il s'agit par exemple de « l'usage de camouflages, de leurres, d'opérations simulées et de faux renseignements ». La perfidie, en

revanche, désigne « les actes faisant appel, avec l'intention de la tromper, à la bonne foi d'un adversaire pour lui faire croire qu'il a le droit de recevoir ou l'obligation d'accorder la protection prévue par les règles du droit international applicable dans les conflits armés ». Il s'agit par exemple de feindre une volonté de négocier ou de se rendre en agitant un drapeau blanc, feindre d'être blessé, d'être un civil ou d'avoir un statut protégé en utilisant des signes comme ceux du CICR, de l'ONU etc. (PI, art. 37).

Appliquée à la cyberconflictualité, cette distinction est beaucoup moins claire. Le simple fait de planter un ver dans un système en ne le présentant pas, évidemment, comme une attaque militaire mais comme un transfert de données innocent (téléchargement d'un logiciel, pièce jointe à un e-mail, etc.) peut-il être considéré comme de la perfidie puisque l'on se fait passer pour un civil, c'est-à-dire une personne protégée ? Le fait d'envoyer un virus par e-mail à des militaires en se faisant passer pour une ONG ou le CICR est-il équivalent à une usurpation d'emblème sur le terrain, par exemple, comme le fait de cacher des combattants ou des armes dans une ambulance ou un véhicule de la Croix-Rouge ? Cette interprétation est discutable, mais défendable. Utiliser les codes et les signaux que l'Organisation de l'aviation civile internationale réserve au transport médical, en revanche, pourrait plus clairement être considéré comme de la perfidie (Kodar, 2012).

La participation des civils aux hostilités

Le cyber exacerbe une tendance devenue évidente depuis la fin du siècle dernier : la *civilianisation* des conflits armés, qui ont davantage lieu dans des zones peuplées, souvent urbaines, dans lesquelles il est de plus en plus difficile de distinguer les civils des combattants, parce que les premiers participent aux hostilités et les seconds font de moins en moins d'efforts pour se distinguer des civils (ils ne portent pas d'uniformes, ni leurs armes ouvertement, etc.) – une tendance encore renforcée par la privatisation du militaire.

Par voie de conséquence, il est devenu nécessaire de distinguer non seulement entre civils et combattants, mais aussi entre les civils participant directement aux hostilités et ceux ne le faisant pas. D'où la notion de « participation directe aux hostilités » introduite en 1977 dans le Protocole I : « Les personnes civiles jouissent de la protection accordée par la présente Section, sauf si elles participent directement aux hostilités et pendant la durée de cette participation » (art. 51(3)). Le *Guide interprétatif sur la notion de participation directe aux hostilités en DIH* du CICR (2010) explique que, pour constituer une participation directe aux hostilités, un acte spécifique doit satisfaire trois critères cumulatifs : qu'il atteigne un certain seuil de nuisance, qu'il y ait une relation de causalité directe entre l'acte et ses effets nuisibles et qu'il y ait également un lien de

belligérance permettant d'établir que l'acte était spécifiquement destiné à avantager une partie au conflit au détriment d'une autre.

Cette notion est d'une importance particulière dans le cas du cyber, car les lanceurs d'attaque peuvent être des civils, recrutés pour leur expertise – c'est même souvent le cas. La question est alors de savoir s'ils participent directement aux hostilités et perdent du même coup leur protection, c'est-à-dire peuvent devenir eux-mêmes la cible d'attaques légitimes. Le problème bien entendu est que l'anonymat empêche souvent d'effectuer le test des trois critères en question. Il faudrait d'abord pouvoir distinguer entre le lanceur d'attaque lui-même, qui pourrait participer directement et les civils s'occupant de la maintenance des ordinateurs, même s'il s'agit d'ordinateurs militaires.

Il faudrait ensuite que le lien de belligérance soit démontré. Durant le conflit Russie-Géorgie de 2008, par exemple, on a vu les deux cas de figure : le « hacking patriotique », qui satisfait le lien de belligérance puisque les civils agissent pour avantager une partie au conflit au détriment d'une autre, soit en utilisant leur ordinateur eux-mêmes, soit en le laissant être utilisé par d'autres et l'usage de *botnets*, qui ne le satisfait pas puisque l'opération se fait à l'insu du civil dont l'ordinateur est utilisé.

Le cas échéant, si la participation directe est avérée, il y aurait encore le problème de la réponse puisque la protection de ces civils ne cesse que « pendant la durée de cette participation » qui, dans le cas d'une cyberopération, n'est en général que de quelques minutes, voire quelques secondes et est souvent en décalage avec la réalisation des effets : une bombe logique, par exemple, peut se révéler des mois voire des années après avoir été placée par un civil qui ne participe donc plus aux hostilités depuis longtemps au moment de sa découverte. Cette contrainte temporelle rend inopérant le droit de frapper des civils participant directement aux hostilités (Schmitt, 2011).

En dehors d'une situation de conflit armé

Si la cyberattaque n'est pas l'un des moyens employés dans un conflit armé, mais le seul acte hostile, en l'absence de toute opération cinétique, est-il suffisant pour remporter la qualification de conflit armé et du même coup l'applicabilité du DIH ? Autrement dit, la cyberattaque peut-elle être constitutive d'un conflit armé ? Peut-elle déclencher seule l'applicabilité du DIH ?

Qu'est-ce qu'une cyberattaque ?

Le problème est que l'applicabilité du DIH est liée à l'existence d'un conflit qualifié d'*armé*. Or, peut-on dire d'une cyberattaque qu'elle est

armée ? Tout dépend de la manière dont le DIH définit l'attaque. « L'expression "attaques" s'entend des actes de violence contre l'adversaire, que ces actes soient offensifs ou défensifs » (PI, art. 49(1)). On voit qu'en DIH la notion d'attaque n'est pas exactement la même que dans le langage courant, où elle est réduite à l'action offensive, voire l'agression. En DIH, une attaque peut être défensive parce qu'elle est simplement une opération militaire violente limitée dans le temps et l'espace, quel que soit celui qui a commencé.

Ce qui nous intéresse dans cette définition est l'expression « actes de violence » : le fait d'introduire un ver ou un virus dans un système informatique peut-il être considéré comme un acte de violence ? La doctrine s'entend généralement pour dire que les « actes de violences » en question doivent être physiques : des moyens comme l'embargo, les sanctions économiques, les pressions diplomatiques ou psychologiques, la propagande, ne sont pas considérés comme des attaques au sens de l'article 49. En revanche, l'emploi d'agents bactériologiques et chimiques est considéré comme une attaque, même s'ils tuent silencieusement, sans aucune explosion ni brutalité physique. C'est donc que le DIH conçoit l'attaque de manière conséquentialiste : ce qui est constitutif d'une attaque n'est pas tant sa force physique en tant que telle que ses conséquences létales.

Si la raison d'être du DIH est de limiter les effets destructeurs des conflits armés, il n'y a pas de raison à priori qu'il ne puisse pas s'appliquer à des cyberattaques si et seulement si elles sont des effets destructeurs comparables à ceux des armes physiques. De ce point de vue, sont considérées comme des attaques dans un contexte cyber « les opérations qui causent – ou, si elles échouent, étaient censées causer – la mort ou des blessures chez des individus, ou la destruction ou le dommage d'objets » (Schmitt, 2012).

On notera que cette définition étroite ou technique ne correspond pas à celle, large, selon laquelle la « cyberattaque désigne l'usage d'activités délibérées pour modifier, interrompre, tromper ou détruire des systèmes ou des réseaux informatiques utilisés par un adversaire ou l'information et/ou les programmes se trouvant dans ou transitant par ces systèmes ou réseaux » (Lin, 2012). Et encore moins à celle, encore plus large et dominante dans les milieux journalistiques, qui appelle « cyberattaque » toute pénétration des systèmes ou des réseaux informatiques de l'adversaire, même si c'est pour l'espionner seulement, c'est-à-dire obtenir de l'information sans qu'il s'en aperçoive. Dans ce cas, on devrait plutôt parler de cyberexploitation (Lin, 2012). Quoiqu'il en soit, suivant Schmitt, nous considérons que les cyberopérations qui ne causent pas de destruction physique ou dont les effets sont réversibles ne sont pas des « attaques ».

Plus difficile est le cas de celles qui neutralisent sans détruire. La neutralisation fait partie de la définition traditionnelle des objectifs militaires, qui sont des « biens qui, par leur nature, leur emplacement, leur destination ou leur utilisation apportent une contribution effective à l'action militaire et dont la destruction totale ou partielle, la capture ou la neutralisation offre en l'occurrence un avantage militaire précis » (PI, art. 52(2)). La doctrine est divisée quant à la question de savoir si une simple neutralisation est une attaque. Tout dépend en réalité de ce qui est neutralisé : autant une simple attaque par déni de service d'un site commercial, par exemple, pourrait difficilement être qualifiée d'« attaque » au sens du DIH, autant le fait de désactiver des défenses anti-aériennes devrait logiquement mériter cette qualification (Melzer, 2011).

Pour notre enquête sur l'applicabilité du DIH, deux critères semblent pertinents. D'une part, le type d'opérations : celles causant des dommages physiques, par exemple parce qu'elles paralysent un hôpital ou qu'elles emballent un réacteur nucléaire et celles consistant seulement à manipuler ou effacer des données sans conséquences physiques. Les premières pourraient éventuellement constituer un conflit armé, mais pas les secondes. D'autre part, le degré de dommage causé : il est aussi intuitif d'imaginer que, plus le dommage est grand, plus l'attaque risque d'être considérée comme constituant un conflit armé. Dès lors, l'intensité de l'attaque pourrait aussi être un critère.

Les cyberopérations constituant des attaques selon cette interprétation pourraient alors suffire à déclencher l'applicabilité du DIH (Knut, 2004). On pourrait objecter qu'en DIH l'occupation et la détention sont aussi constitutives d'un conflit armé, même si elles ne causent aucun dommage physique. Certes, mais elles le sont uniquement parce qu'elles impliquent un usage potentiel de la force physique – ce qui n'est pas le cas de cyberopérations non destructives telles que de l'espionnage et toute opération visant à pénétrer les systèmes ou réseaux de l'adversaire sans qu'il s'en rende compte ou même des attaques par déni de service.

Contrairement à un préjugé répandu, ces dernières, qui n'atteignent donc pas le seuil qualifiant d'« attaques », peuvent légalement viser des civils et des infrastructures civiles. Elles ne le peuvent plus lorsqu'elles deviennent des attaques et le consensus actuel est que ce seuil est atteint lorsque les dommages causés aux infrastructures en question nécessitent réparation (Schmitt, 2013).

Les opérations ne faisant aucun dommage physique peuvent toutefois être très handicapantes pour l'État visé, qui pourrait être tenté de les qualifier d'attaque armée et d'y répondre par la force physique cette fois. Il aurait certes juridiquement tort, mais il faut s'attendre à ce type de réaction.

Dans l'hypothèse où les cyberopérations pourraient être considérées comme des attaques, parce qu'elles causent des dommages physiques et constitueraient donc un conflit armé déclenchant l'applicabilité du DIH, il faudrait encore savoir si ce conflit armé est international ou non international. C'est un enjeu majeur en DIH, parce que les mêmes règles ne s'appliquent pas à chacune de ces deux catégories.

La cyberattaque peut-elle être constitutive d'un conflit armé international (CAI) ?

Il y a conflit armé international (CAI) « chaque fois qu'il y a recours à la force armée entre États »[1]. Le problème est que la cyberconflictualité implique souvent des acteurs non étatiques. Le conflit peut malgré tout être considéré comme un CAI à condition que ces acteurs non étatiques puissent être considérés comme des agents d'un État tiers. En droit de la responsabilité internationale des États pour fait illicite, « le comportement d'une personne ou d'un groupe de personnes est considéré comme un fait de l'État d'après le droit international si cette personne ou ce groupe de personnes, en adoptant ce comportement, agit en fait sur les instructions ou les directives ou sous le contrôle de cet État »[2].

La jurisprudence montre que l'attribution à un État de la responsabilité des actes commis par des personnes privées dépend du degré de contrôle que cet État exerce sur ces personnes[3] : il faut prouver davantage que le financement et l'équipement de ces forces, il faut prouver la participation à la planification et la supervision des opérations militaires. C'est ici que revient le problème de l'anonymat dans la cyberconflictualité : il est très difficile de prouver l'existence de ces liens, le degré de contrôle, dans le monde virtuel.

Pour qu'une cyberattaque conduite par des acteurs non étatiques soit considérée comme un CAI, il faudrait non seulement qu'elle cause des dommages physiques (pour pouvoir être qualifiée d'attaque au sens du DIH), mais encore qu'un État tiers soit derrière le groupe de hackers et qu'il exerce sur eux un contrôle réel. Le simple fait de tolérer cette activité, ou que la cyberattaque émane de son territoire n'est pas un lien suffisant (d'autant plus qu'un territoire peut être détourné, on peut lancer une attaque depuis la France en faisant croire qu'elle émane d'ailleurs). C'est précisément ce qui s'est produit dans le cas de l'Estonie et de la Russie : l'origine des attaques est restée floue, la plupart d'entre elles ont été émises depuis le territoire russe mais cela ne suffit pas à impliquer formellement la responsabilité du gouvernement russe.

1 TPIY, Chambre d'appel, *Le Procureur c. Dusko Tadic*, IT-94-1-A, Arrêt relatif à l'appel de la défense concernant l'exception préjudicielle d'incompétence (2 octobre 1995), § 70.
2 Art. 8 du rapport de la Commission du droit international, UN Doc A/56/10, 2011.
3 CIJ, *Affaire des Activités militaires et paramilitaires au Nicaragua*, 1986 et TPIY, Tadic.

S'il n'est donc pas impossible, en théorie, qu'un cyber échange entre deux États soit constitutif d'un CAI, il est souvent, dans les faits, difficile de le prouver.

La cyberattaque peut-elle être constitutive d'un conflit armé non international (CANI) ?

Le cas du CANI est plus difficile, car il est soumis à davantage de conditions. Un conflit armé non international (CANI) a lieu entre un État et un ou des groupes armés non étatiques, ou entre des groupes armés entre eux. Mais, pour être qualifié de conflit armé, il doit satisfaire deux critères : avoir une certaine organisation et une certaine intensité. En l'occurrence, atteindre un certain niveau d'organisation exclut des hackers individuels ou non coordonnés : ne constituant pas un « groupe armé » au sens du DIH, leur cas relève du droit pénal interne, pas du DIH. En revanche, des hackers appartenant à une organisation virtuelle dotée d'un leadership coordonnant leurs opérations pourraient satisfaire ce critère. Plus difficile est le cas d'un groupe informel opérant de manière collective mais non coordonnée[1].

Quant au niveau d'intensité, le CANI se distingue en cela du CAI : alors que le seuil de déclenchement d'un CAI est très bas (on dit pour caricaturer qu'un coup de feu suffit), celui d'un CANI est beaucoup plus élevé car il y a de nombreuses situations, qu'on appelle de troubles intérieurs ou de tensions internes, dans lesquelles il y a des affrontements entre des manifestants et les forces de l'ordre, la police voire l'armée, qui sont préoccupantes mais ne relèvent pas (encore) du DIH – elles relèvent du droit interne et du DIDH.

Or, appliqué au cas de la cyberconflictualité, ce critère de l'intensité exclut la plupart des opérations : non seulement celles qui ne causent aucun dommage physique, comme le vol de données par exemple, ou le fait de bloquer certains sites Internet, mais même celles qui en causent de manière irrégulière, non continue, ou qui n'atteignent pas un seuil de dommage assez élevé. Cela exclut aussi les incitations à la révolte (comme celles à destination de la minorité russe en Estonie en 2007) ou à commettre des attentats terroristes[2].

Pour ces deux raisons – les degrés d'organisation et de violence nécessaires –, il est peu probable dans les faits qu'un cyberéchange puisse être qualifié de CANI.

1 *Tallinn Manual*, *op. cit*., Rule 23.13 et 15, p. 89-90.
2 *Ibid*., Rule 23.5, p. 86.

Conclusion

La cyberconflictualité pose au DIH de nombreuses difficultés, pour des raisons évidentes : le droit international humanitaire a été conçu à une époque où la cyberconflictualité n'existait pas, où les attaques ne pouvaient être que cinétiques. Cela rend son applicabilité difficile, non seulement lorsqu'il existe déjà un conflit armé (car l'anonymat et l'interconnectivité, par exemple, posent problème), mais plus encore en l'absence de conflit armé : s'il n'est pas impossible qu'une cyberattaque puisse constituer seule un conflit armé et déclencher l'applicabilité du DIH, il est dans les faits difficile de satisfaire les conditions requises.

Comme on peut s'attendre à ce que la cyberconflictualité se développe, parce qu'elle a de nombreux avantages (de coût, aussi parce qu'elle permet au faible de s'en prendre au fort), il est important de continuer à réfléchir à l'applicabilité du DIH et à d'éventuelles réformes ou reformulations. Dans cette entreprise où le droit atteint ses limites, l'éthique – qui est le droit de demain – peut aider.

C'est pourquoi les principes traditionnels du *jus in bello* – nécessité, distinction, proportionnalité, précaution et interdiction de causer des maux superflus – méritent une discussion plus détaillée, qui s'arrache de la traduction contemporaine qu'en a fait le DIH pour retrouver leurs racines dans la doctrine millénaire de la guerre juste.

Bibliographie

Droege C., 2012, « Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians », *International Review of the Red Cross*, 94 : 886, p. 536-537.

Knut D., 2004, « The Applicability of the Additional Protocols to Computer Network Attacks: An ICRC Viewpoint », in K. Byström (éd.), *International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law, 17-19 November 2004, Stockholm, Sweden*, Swedish National Defence College, p. 142.

Kodar E., 2012, « Applying the Law of Armed Conflict to Cyber Attacks: From the Martens Clause to Additional Protocol I », ENDC Proceedings, vol. 15, p. 127.

Lin H., 2012, « Cyber Conflict and International Humanitarian Law », *International Review of the Red Cross*, 94 : 886, p. 518-519.

Melzer N., 2011, « Cyberwarfare and International Law », UNIDIR Resources, p. 22-26.

Schmitt M.N. (éd.), 2013, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge, Cambrige University Press.

Schmitt M.N., 2011, « Cyber Operations and the *Jus in Bello*: Key Issues », *International Law Studies US Naval War College*, 89, p. 102.

Schmitt M.N., 2012, « 'Attack' as a Term of Art in International Law: The Cyber Operations Context », in Czosseck C., Ottis R. et Ziolkowski K. (éd.), *4th International Conference on Cyber Conflict*, Tallinn, NATO CCD COE, p. 291.

Schmitt M.N., 23 septembre 2013, « Five Myths in the Debate about Cyber War », blog justsecurity.org.