De la sécurité numérique en période de conflit armé. Problématique de la régulation juridique des cyberopérations militaires.

David CUMIN
Maître de conférences (HDR)
Université Jean Moulin Lyon 3, Faculté de Droit, CESICE

Le temps de paix est celui où il est interdit de nuire à autrui ; le temps de guerre, celui où il est recommandé de nuire à l'ennemi. Comment assurer la sécurité et la confiance numériques dans le contexte d'un conflit armé international ?

Le droit des conflits armés

Les belligérants sont aux prises au plan cinétique comme au plan cybernétique ; sur ce dernier plan, joue pleinement la faculté qu'a chaque partie, au combat, de *semer la discorde chez l'ennemi*. Mais la guerre n'est pas un déchainement aveugle de violences ; elle est un emploi rationalisé, organisé et discipliné de la force, utilisé comme un moyen au service d'un but et d'une finalité, le but étant de vaincre ou de soumettre l'ennemi, la finalité étant d'imposer ou d'obtenir une paix favorable, puisqu'après la guerre, il y aura retour à la paix. C'est pour cela qu'existe un droit de la guerre (*jus in bello*), également appelé droit des conflits armés ou droit international humanitaire. Il sert à préserver l'instrumentalisation de la force armée, donc à limiter les hostilités, notamment en protégeant les tiers au conflit armé d'une part, les non combattants et les objectifs non militaires d'autre part. Il se subdivise selon les théâtres d'hostilité en un droit de la guerre terrestre, maritime, aérienne, éventuellement aérospatiale. En droit de la guerre terrestre, il se subdivise aussi en différents régimes applicables : régime des combats, régimes des combattants victimes des hostilités, dont la captivité, régime des personnes et biens civils, régime des institutions et biens culturels, régime de l'occupation, régime de l'assistance humanitaire. Le régime de l'environnement en période de conflit armé concerne tous les théâtres ou espaces (naturels), terre, mer, air, exo-atmosphère. De même le régime de la neutralité, qui règle les rapports entre belligérants et tiers.

Les *Manuels de Tallinn*

Le cyber est concerné : s'il est appréhendé comme moyens cybernétiques, comme le font les Russes et les Chinois, il relèvera du régime des combats, terre, mer, air, exo-atmosphère ; s'il est appréhendé comme cyberespace, comme le font les Occidentaux, il relèvera d'une nouvelle branche, à créer, le droit de la guerre cyberspatiale. Moyen technique ou

nouvel espace purement artificiel, le cyber doit faire l'objet, et fait l'objet, d'une régulation lorsqu'il est employé à des fins hostiles : s'appliquent les principes généraux du droit des conflits armés ainsi que, si des coutumes spécifiques sont pratiquées ou si des conventions spécifiques sont conclues, des règles spécifiques. Des textes spécifiques, issus de discussions internationales spécifiques, peuvent servir de code de conduite ou préparer la négociation et la rédaction de conventions. A cet égard, existent deux manuels : les *Manuels de Tallinn* 1 et 2, respectivement publiés en 2013 et 2017, le premier, sur l'applicabilité du droit international à la guerre cybernétique, initié par le Centre de cyberdéfense de l'OTAN et rédigé par un groupe international d'experts (occidentaux), en collaboration avec le Comité international de la Croix-Rouge (CICR), le second, qui étend l'applicabilité du droit international aux opérations cybernétiques en temps de paix, rédigé lui aussi par un groupe international d'experts (occidentaux) à l'initiative du Centre de cyberdéfense de l'OTAN mais sans la collaboration du CICR. S'agissant de la France, deux publications du ministère des Armées existent : *Droit international appliqué aux opérations dans le cyberespace*, 2019 ; « Le droit applicable aux opérations dans le cyberespace », chapitre 4 de la partie IV « Les règles spécifiques liées aux opérations dans différents milieux » du *Manuel de droit des opérations militaires*, 2022, pp.233-313, pp.295-313.

Quel droit applicable et comment appliquer le droit ?

Les organisations humanitaires comme les militaires et les conseillers juridiques aux armées posaient et se posaient un certain nombre de questions sur l'applicabilité du droit international aux attaques informatiques ou contre les réseaux informatiques. Ainsi, comment trouveraient à s'appliquer les *principes de distinction entre guerre et paix*, *entre belligérants et neutres*, *entre combattants et non combattants et entre objectifs militaires et non militaires* ? Les références du droit de la guerre cyberspatiale seraient-elles tirées du droit de la guerre terrestre, ou maritime, ou aérienne, ou les trois ? Quels seraient les moyens et méthodes permis ? Comment tester les nouvelles armes cybernétiques ? Quelles activités civiles liées aux cyberattaques constitueraient une participation directe aux hostilités et feraient donc perdre aux civils leur immunité ? Toute partie qui lancerait des attaques devrait prendre toutes les dispositions possibles pour éviter ou réduire les dommages causés aux réseaux civils en général, aux réseaux indispensables à la survie de la population en particulier, ce qui suppose qu'elle vérifie la nature des réseaux visés, qu'elle évalue les dommages probables et qu'elle cesse une attaque provoquant des dommages excessifs. De même, elle devrait épargner les Etats tiers. Or, l'interconnectivité *des* réseaux rend difficile - mais pas impossible, au contraire de l'intégration en *un* réseau - d'empêcher la propagation - aussi bien chez les tiers que chez l'ennemi et au-delà du temps de guerre - des perturbations causées par les cyberattaques. Ainsi le grand problème du droit des conflits armés, qui est de distinguer combattants et non combattants, objectifs militaires et non militaires, se retrouve avec une acuité particulière dans le domaine cyber.

La singularité opérationnelle des cyberhostilités

De même qu'il est possible de parler de cybercriminalité, il est possible de parler de cyberguerre, c'est-à-dire des actions hostiles, préparées, déclenchées et menées dans le cyberespace, plus ou moins intensément ou durablement, par des Etats ou des collectivités non étatiques contre d'autres Etats ou collectivités, aux fins de les contraindre. Les actions matérielles (attaques, bombardements, opérations de commandos ou de forces spéciales) contre la couche physique du cyberespace ne sont pas *de la guerre cybernétique* ; elles sont *de la guerre classique*

(cinétique), menée par l'armée de terre, la marine ou l'armée de l'air, contre des cibles *matérielles* à terre, sous la mer ou dans l'exo-atmosphère. Ce sont les actions immatérielles contre les couches logicielle et sémantique du cyberespace qui relèvent spécifiquement de la guerre cybernétique. La cyberguerre combine les deux types d'action : les unes et/ou les autres. Elle inclut aussi l'utilisation des moyens cybernétiques pour frapper des personnes ou des biens adverses. Visant le cyber ou se servant du cyber, la stratégie acquiert une dimension *totale*, car la cybernétique ou le cyberespace embrasse et articule une très grande partie des activités humaines, qu'il s'agisse de systèmes de production ou de distribution, de transports ou de communications. Aussi ouvre-t-elle la possibilité d'une guerre à la fois *totale* et *non létale*. La non létalité ne doit pas faire illusion : elle ne serait qu'immédiate, car les désorganisations, paralysies ou pénuries créées par les attaques matérielles ou immatérielles contre les réseaux informatiques causeraient des victimes à terme. Concrètement, au cas où les effets des cyberattaques déborderaient le cyberespace - ne se borneraient pas à endommager les matériels, à altérer les logiciels ou à corrompre les informations - pour affecter les activités se déroulant dans les autres espaces - viser ou toucher les systèmes de contrôle de la circulation aérienne, maritime ou terrestre, les digues, barrages, centrales nucléaires, raffineries de pétrole, usines chimiques, laboratoires pharmaceutiques, les services de distribution de l'eau, du gaz, de l'électricité ou du carburant - leur impact humanitaire serait énorme.

L'encadrement juridique des cyberhostilités

Il n'existe nulle convention et nulle coutume spécifiques traitant de la cyberguerre. Mais sont disponibles les principes généraux du droit des conflits armés. *« Il n'y a pas de vide juridique dans le cyberespace »*, a répété le CICR ; le droit international y est applicable. Depuis 2004, un Groupe d'experts gouvernementaux (GGE) chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale a été mis en place par l'Assemblée générale des Nations Unies ; le GGE a reconnu l'applicabilité du droit international humanitaire à l'utilisation de technologies numériques dans le contexte d'un conflit armé. Mais le dissensus prévaut entre Occidentaux et Sino-Russes. Quoi qu'il en soit, les auteurs d'une cyberguerre seraient des Etats ou des collectivités non étatiques. S'agissant des opérations cybernétiques, les acteurs -combattants *de jure* ou *de facto*, donc cibles *humaines* - seraient les spécialistes de l'informatique - au cœur du fonctionnement du cyberespace en temps de paix comme en temps de guerre. S'agissant des opérations cybernétiques, les instruments - eux-mêmes vulnérables - seraient des ordinateurs, des logiciels et des informations, utilisés comme des armes matérielles ou immatérielles par destination. Les modalités devraient être conformes aux principes généraux du droit des conflits armés. Quel droit, terrestre, maritime ou aérien ? La notion d'objectif militaire est plus stricte sur terre que dans les deux autres espaces, où il est question de « contrebande de guerre » ou d'« objectif militaire aérien légitime ». Quelle notion doit prévaloir ? D'un côté, les populations civiles vivant à terre, les effets des cyberhostilités doivent être compatibles avec les principes généraux du droit de la guerre terrestre ; la notion d'objectif militaire doit donc être strictement entendue. D'un autre côté, l'interconnectivité du cyberespace fait que les réseaux militaires sont souvent reliés aux réseaux civils ou que les réseaux civils couvrent des objectifs militaires ou mixtes. Ils ne constitueraient donc pas des biens civils au sens terrestre : de même que la navigation marchande - maritime ou aérienne - assimilable de la contrebande peut être interceptée, saisie voire détruite, une partie de la navigation cybernétique pourrait être attaquée en tant qu'*objectif militaire cybernétique légitime*. Ne seraient alors protégés que les réseaux informatiques *indispensables à la*

survie de la population, ou affectés à la santé, à la protection civile, au fonctionnement des digues, barrages et centrales nucléaires, à l'assistance humanitaire, aux institutions et biens cultuels ou culturels... Il s'agit là du problème relatif à la détermination du droit de la guerre applicable ou transposable.

Les principaux problèmes en amont

C'est plus en amont qu'un triple problème se pose : le seuil d'entrée en guerre - dans l'hypothèse où seules des opérations cybernétiques seraient effectuées (1) ; l'identification de l'ennemi (2) ; la nature de la riposte à des cyberattaques (3).

1) Des opérations cybernétiques lancées par des Etats ou des collectivités non étatiques contre d'autres Etats, peuvent être considérées, de par leur gravité matérielle et leur intention coercitive, comme un recours à la force armée dans les relations internationales, voire comme une agression. Mais la mesure de la gravité coercitive de telles opérations appartient aux Etats la subissant, ainsi qu'au Conseil de Sécurité des Nations Unies. Même objectivement, il est difficile de distinguer entre une opération constitutive d'une simple atteinte à la sûreté de l'Etat, appelant des mesures de police, et une opération constitutive d'un emploi de la force armée, justifiant la réaction militaire au titre de la légitime défense. Depuis le tournant des années 2000-2010, l'essor des cyberattaques, ciblées ou massives, illustrent à la fois l'importance de la cyberstratégie et la difficulté de qualifier les actions ou épreuves de force dans le cyberespace : continuation de la paix, fût-elle troublée, ou passage à la guerre, fût-elle de basse intensité ? Notoirement, le cyberespace est devenu LE théâtre de l'affrontement furtif entre les grands Etats atlantiques et eurasiatiques : le lieu des confrontations « immatérielles » qui ne sont pas prolongées dans le monde « réel », mais qui pourraient l'être. Il est clair que des activités délibérées ayant pour effet d'affecter substantiellement des capacités militaires, de paralyser ou détruire des installations ou matériels sensibles, de provoquer des dysfonctionnements graves, étendus et/ou durables dans la vie économique, sociale et politique d'un pays, sont des actes d'hostilité. On entre alors dans le temps de guerre, régulé par le droit applicable.

2) Reste à identifier l'ennemi. Ou à imputer à un Etat ou à une collectivité les actes commis par des particuliers. Or, le cyberespace étant opaque et les opérations cybernétiques étant le plus souvent secrètes ou commises par des services secrets, leur attribution à tel Etat ou collectivité est difficile. *L'inattribution permet la discrétion*, cependant qu'*elle empêche l'imputation de responsabilité*, aussi bien de la part de l'adversaire que des Nations Unies ou des Etats tiers. Elle facilite donc des actions contraires au droit international. D'un autre côté, le recours à la force armée vise à obtenir quelque chose vis-à-vis de l'adversaire ; comment l'obtenir sans revendication, donc sans se faire connaître ? A moins que le recours à la force ait pour unique but, *sans létalité*, l'affaiblissement de l'adversaire ou la destruction de secteurs sensibles (exemple de *Stuxnet*, qui visait, côté israélo-américain, à stopper ou à retarder le programme nucléaire iranien). Il y a ainsi une *destructivité* de la cyberstratégie, d'autant plus inquiétante que la cyberstratégie, si elle est possiblement *discrète*, peut également être *totale*.

3) L'Etat victime de cyberattaques doit-il cantonner sa riposte au cyberespace ou peut-il l'étendre à d'autres espaces ? Il convient de répondre par l'affirmative à cette seconde proposition, pourvu que la riposte demeure compatible avec l'encadrement normatif de la légitime défense, notamment la nécessité et la proportionnalité.

De l'identification du cyber-assaillant à la régulation juridique de la cyberguerre

Revenons à l'identification, qu'il faut prouver. Si l'on ne peut identifier le cyberbelligérant, donc si l'on ne peut lui imputer aucune responsabilité, pourquoi respecterait-il les règles de la guerre ? Comment astreindre un *anonyme* à respecter le droit ? Comment même le dissuader d'attaquer ? Il est possible, et même facile, de se défendre vis-à-vis de cyberattaques. Mais contre qui ? Aux services de renseignement d'accomplir leur mission. Aux autorités politiques de désigner publiquement, ou de taire, l'identité de l'assaillant, prouvée ou *supputée*, en choisissant de le combattre dans d'autres espaces ou en confinant la lutte au cyberespace. Des cyberguerres secrètes seraient-elles possibles ? Les critères objectifs d'identification du seuil de la belligérance : organisation des parties hostiles et intensité de la violence coercitive, font que toute guerre est nécessairement connue du public (sinon reconnue par les Gouvernements). Des opérations cybernétiques atteignant une certaine gravité matérielle dans le pays visé ne pourront probablement pas demeurer secrètes. Restera à désigner l'ennemi. Dans l'hypothèse où une telle désignation s'effectuera, la cyberguerre sera un duel devant des tiers, appelant une régulation juridique, à laquelle participeront le CICR, l'ONU et les Etats, notamment les grandes puissances.