INTERNET ET LE DROIT INTERNATIONAL

COLLOQUE ANNUEL DE LA SFDI

ROUEN

30 MAI- 1ER JUIN 2013

ATELIERS

APPELS A PROJETS

UNIVERSITÉ DE ROUEN

CUREJ

INSTITUT DE RECHERCHE INTER-DISCIPLINAIRE HOMME SOCIÉTÉ IRIHS

Sfdi Société française pour le droit international

ATELIER N° 1 :
DROIT INTERNATIONAL ET CYBERGUERRE

Président
Paul TAVERNIER
Professeur émérite de l'Université de Paris sud

Discutant
Abdelwahab BIAD
Maître de Conférences de l'Université de Rouen

Les normes du droit international humanitaire (DIH) imposent un standard de comportement auquel les belligérants doivent s'astreindre dans les situations de conflit armé. Ces lignes directrices résident dans un ensemble de règles que la CIJ avait qualifiées de « principes intransgressibles du droit international coutumier » (*affaire* de la *Licéité de la menace ou de l'emploi d'armes nucléaires*, avis consultatif). Les principes de distinction et de proportionnalité dans l'attaque, ainsi que celui qui interdit les méthodes et moyens de guerres causant des maux superflus, constituent le fondement de l'équilibre entre « nécessité militaire » et « considérations d'humanité ». Mais, à l'aube du XXIème siècle, une préoccupation se fait jour à propos de la transformation radicale de la nature de la guerre sous l'effet de l'apparition des cybertechnologies. Le *Manuel de Tallin* (2013) aborde la problématique de la cyberguerre et l'émergence d'un nouveau champ de bataille virtuel, le cyberespace, et ses implications. Les règles du *jus in bello* s'appliquent à toutes les armes et méthodes de guerre, du présent comme du futur. L'article 36 du *Protocole additionnel I aux Conventions de Genève* prescrit aux parties de vérifier lors de l'acquisition d'une nouvelle technologie à usage militaire, si son emploi en est interdit par les règles en vigueur du *jus in bello.*

1. Une cyber opération peut-elle être qualifiée de « conflit armé », condition essentielle à l'application du DIH ? Si elle est conduite dans le cadre d'une opération globale faisant appel aux méthodes et moyens létaux et cinétiques conventionnels, la question de l'applicabilité des règles du *jus in bello* ne se pose en principe pas. Mais, qu'en est-il si elle a pour effet de causer des pertes humaines et des destructions matérielles importantes, sans qu'elle s'inscrive dans le cadre d'opérations classiques ? Cela suffit-il en soi pour la qualifier de conflit armé ? La distinction classique entre « conflit armé international » et « conflit armé non international » est-elle pertinente dans un contexte d'emploi de moyens virtuels à vocation transfrontalière, dans un réseau de réseaux au sein duquel la propagation d'une attaque devient vite incontrôlable et peut infecter les systèmes d'autres États non belligérants ?

2. La « cyberattaque » que l'on pourrait déjà définir comme une opération cybernétique à caractère offensif ou défensif peut-elle être qualifée d'agression ? Comment réagir à ces cyberattaques dans le respect du droit international ? Cette cyberattaque, dont on pourrait attendre qu'elle cause des pertes en vies humaines, des blessures aux personnes, des dommages ou des destructions de biens, n'est pas interdite en elle-même par le DIH. Il n'en demeure pas moins que sa légalité doit être analysée à la lumière du principe de distinction destiné à protéger les personnes et biens civils, et du principe de proportionnalité qui interdit de causer des pertes et des dommages excessifs, allant au-delà de l'avantage militaire attendu.

Mais, peut-on respecter le principe de distinction à l'occasion d'une cyberattaque dès lors que les systèmes informatiques civils et militaires d'un pays sont interconnectés ? Des « virus » ou des « vers » introduits dans un système informatique militaire peuvent se répandre et endommager des systèmes gérant également des infrastructures civiles.

3. Dans le contexte d'une cyberattaque, qu'est-ce qu'un objectif militaire ? Une cyberattaque peut-elle être menée contre les membres des forces armées ou de groupes armés organisés, mais aussi contre des installations ou des cibles qui n'entrent pas dans la définition traditionnelle des objectifs militaires ? Une base de données ou des réseaux sociaux peuvent-ils ainsi être considérés comme des objectifs militaires ? Mais, infiltrer les réseaux internet en vue de détruire, altérer ou collecter des données ou pour détourner ou manipuler des systèmes informatiques à des fins hostiles ne pourrait-il pas causer des catastrophes humanitaires majeures (perturbation des infrastructures de fourniture d'énergie et d'eau, ou des systèmes de contrôle du trafic aérien et ferroviaire) ?

4. Internet, le réseau des réseaux, outil de communication en temps de paix, peut-il aussi être un théâtre de la cyberguerre avec toutes ses déclinaisons (« cyberattaque », « cyber défense », « cyberopération », « cyberespace », « cybersécurité ») ? Les cybertechnologies posent un certain nombre de défis liés non seulement au caractère virtuel et déterritorialisé des moyens utilisés, mais aussi à la difficulté d'identifier immédiatement l'auteur de l'attaque - le cybercombattant - et par conséquent à mettre en oeuvre la responsabilité pénale individuelle pour infractions graves aux Conventions de Genève (crimes de guerre et violations des lois et coutumes de la guerre).

Les propositions de contribution devront s'efforcer d'approfondir les questions abordées ou pourront soulever d'autres thèmes dans le cadre de la thématique générale de l'atelier.

Les personnes intéressées sont invitées à transmettre leur projet d'intervention (5 pages maximum) accompagné d'un *curriculum vitae*.

Les propositions doivent être envoyées à Paul Tavernier (credho@credho.org) et Abdelwahab Biad (biad.abdelwahab@univ-rouen.fr) avec copie à Anne-Thida Norodom (anne-thida.norodom@univ-rouen.fr) et Philippe Lagrange (philippe.lagrange@univ-rouen.fr), avant le **18 mars 2013**.

ATELIER N°2 :
DROIT INTERNATIONAL ET CYBERCRIMINALITE

Présidente
Geneviève BURDEAU
Professeur à l'Ecole de droit de la Sorbonne (Paris I)

Discutant
Philippe GUILLOT
Maître de conférences à l'Université de Rouen

Pas plus que le monde réel, le monde virtuel n'échappe aux comportements déviants, transgressifs et malfaisants. Le droit doit donc appréhender la criminalité télématique ou « cybercriminalité », laquelle « concerne l'ensemble des infractions pénales susceptibles de se commettre sur ou au moyen d'un système informatique généralement connecté à un réseau. » (Myriam Quéméner & Joël Ferry, *Cybercriminalité, défi mondial*, Economica, 2e éd., 2009, p. 2). Compte-tenu du caractère transnational de l'Internet et de l'ubiquité spatio-temporelle des cybercriminels, le droit international, privé comme public, a un rôle essentiel à jouer.

1. Pourtant, les traités en la matière sont loin d'abonder puisque le seul texte spécifique est la *Convention de lutte contre la cybercriminalité*, adoptée sous l'égide du Conseil de l'Europe à Budapest le 23 novembre 2001, qui est entrée en vigueur le 24 mars 2004 – en revanche, son *Protocole additionnel relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes d'information* du 28 juillet 2003 n'a toujours pas recueilli suffisamment de ratifications.

2. De surcroît, une coopération universelle peine à se concrétiser en dépit des déclarations politiques ou de textes de *soft law* en ce sens émanant de nombreuses institutions internationales (Organisation des Nations Unies, Organisation de Coopération et de Développement Économique, Organisation de Coopération de Shanghai, etc.). L'Union européenne se distingue par une activité réglementaire importante en la matière mais, par définition, limitée à ses États membres.

3. Cet atelier accueillera des contributions relatives au traitement en droit international des infractions traditionnelles commises sur Internet comme la fraude et les falsifications informatiques ou la diffusion de contenus illicites (pédophilie, contenu raciste ou xénophobe, « joyeuse farce » ou *happy slapping*) et des infractions propres à l'Internet (piratage et usurpation d'identité – *cybersquatting, phishing, spoofing*, déni de services distribués, défigurations de site et attaques sémantiques, etc.) – toutefois les contributions ne devront pas porter principalement sur les problèmes de propriété intellectuelle, lesquels relèvent de l'Atelier n° 3 – mais aussi aux défis du cyberterrorisme.

4. Les contributions sur l'entraide policière internationale (INTERPOL, EUROPOL, Système d'Information Schengen) ou l'entraide judiciaire européenne (EUROJUST, Projet conjoint Union européenne-Conseil de l'Europe *CyberCrime@IPA*) sont également les bienvenues surtout si elles portent sur les outils d'investigation (interceptions de communication, saisies de données, perquisitions en ligne, infiltrations) et sur le problème de leur éventuelle contradiction avec les autres règles internationales, notamment celles relatives aux droits de l'Homme.

Les propositions pourront porter sur les thèmes précédemment évoqués mais d'autres thèmes en rapport avec la cybercriminalité pourront être proposés.

Les personnes intéressées sont invitées à transmettre un bref projet d'intervention (5 pages maximum) et un *curriculum vitæ* à Philippe Guillot (philippe.guillot@univ-rouen.fr) avec copie à Anne-Thida Norodom (anne-thida.norodom@univ-rouen.fr) et Philippe Lagrange (philippe.lagrange@univ-rouen.fr) avant le **18 mars 2013.**

ATELIER N° 3 :
INTERNET ET COMMERCE INTERNATIONAL

Présidente
Laurence BOISSON DE CHAZOURNES
Professeur à l'Université de Genève

Discutante
Valérie PARISOT
Maître de conférences à l'Université de Rouen

Le développement d'Internet a largement contribué à l'expansion du commerce international, entendu comme l'ensemble des relations économiques internationales qui se nouent entre des opérateurs privés ou publics. La Toile constitue aujourd'hui un espace d'échange commercial par excellence. Elle rend particulièrement nécessaire une protection tant européenne qu'internationale des droits de la propriété intellectuelle. Telles sont les deux pistes de réflexion qui pourront être traitées lors de cet atelier.

Internet comme espace d'échange commercial

Le commerce via Internet, présenté quelquefois comme une simple variante du commerce traditionnel, présente un certain nombre de spécificités irréductibles, qui tiennent avant tout au caractère électronique des échanges qu'il appréhende. De surcroît, ce type de commerce est appelé à se développer plus particulièrement au profit du consommateur, ce qui rend nécessaire une protection renforcée desdits internautes.

1. Les spécificités du contrat conclu via Internet. Le propre d'une transaction électronique est de supprimer les documents papiers commerciaux. La première des contributions proposées pourrait s'intéresser aux implications de cette dématérialisation – et, par suite, de cette internationalisation – des échanges. Non seulement Internet conduit les opérateurs du commerce international à conclure des contrats spécifiques mais il oblige également à revisiter les règles applicables aux contrats « classiques ». L'objet même du contrat électronique interroge : tout contrat international peut-il réellement être conclu par Internet ? Dans quelle mesure les restrictions au commerce international posées par les États sont-elles compatibles avec les principes européens de libre circulation des marchandises et des services ainsi qu'avec le principe de la liberté des échanges posé par l'OMC (v. par exemple la question de la situation de monopole des pharmaciens dans certains pays européens ou encore les restrictions nationales relatives aux jeux en ligne). Le principe même du contrat électronique étant admis, c'est alors l'ensemble du processus de la contractualisation qui met à l'épreuve les règles du droit des contrats. Sur ces questions également, des sources européennes et internationales de réglementation s'imposent et l'on assiste à un « dialogue » intéressant entre les diverses instances supranationales. Concernant d'abord la formation même de la transaction, la Directive 1999/93/CE du 13 décembre 1999 sur la signature électronique a influencé la loi-type de la CNUDCI du 5 juillet 2001 ayant le même objet. À l'inverse, la loi-type de la CNUDCI du 12 juin 1996 sur le commerce électronique a inspiré dans une large mesure la Directive 2000/31/CE sur le commerce électronique, laquelle reconnaît juridiquement l'écrit sur support électronique. Une approche comparée des différentes transpositions intervenues ces dix dernières années pourrait être proposée. Concernant ensuite l'exécution du contrat électronique, des réflexions relatives au paiement

en ligne ainsi qu'à la responsabilité des acteurs de l'Internet pourraient être envisagées. Ces différentes règles, qui visent à faciliter le développement du commerce électronique, rendent d'autant plus nécessaire une protection internationale du consommateur.

2. La nécessité d'une protection renforcée du consommateur. Les règles protectrices du consommateur ne sont pas propres au commerce via Internet. Une seconde contribution pourrait s'interroger sur la spécificité de la protection du consommateur internaute. Plusieurs pistes pourraient à cet égard être suivies. La première question qui se pose est celle de savoir contre quoi le consommateur mérite d'être protégé : en quoi la dématérialisation et l'internationalisation des échanges propres au commerce électronique génèrent-elles des risques particuliers ? L'identification des risques encourus par le consommateur conduit naturellement à s'interroger sur les moyens de protection des consommateurs. En ce domaine, les initiatives européennes se sont multipliées (voir par exemple la Directive n° 2000/31/CE du 8 juin 2000 sur le commerce électronique, qui se propose notamment de garantir « la sécurité juridique et la confiance du consommateur », la Directive n° 2005/29/CE du 11 mai 2005 relative aux pratiques commerciales déloyales des entreprises vis-à-vis des consommateurs, dont les règles sont applicables à l'Internet ou encore la Directive n° 2011/83/CE du 25 octobre 2011 relative aux droits des consommateurs). Peut-on aller au-delà du cadre européen et envisager des règles internationales standard de protection du consommateur ? À cet égard, les lignes directrices de l'OCDE régissant la protection des consommateurs dans le contexte du commerce électronique ou encore les réflexions de la CNUCED relatives au rapport entre, d'une part, la protection du consommateur et, d'autre part, les politiques mondiales en matière de concurrence et de compétitivité, pourraient constituer un point de départ utile de réflexion. Différents aspects de la protection du consommateur, tant au niveau européen qu'au niveau mondial, pourront être abordés (protection du consommateur au stade de la formation du contrat ou au stade de son exécution, développement des solutions extrajudiciaires au règlement des litiges, lesquelles sont particulièrement prisées en droit du commerce international, etc.).

Internet n'est pas seulement innovant en tant qu'espace d'échange commercial. Il conduit également à revisiter les règles classiques en matière de droits de la propriété intellectuelle.

Internet et la protection nécessaire des droits de la propriété intellectuelle

Le deuxième temps de notre réflexion concerne plus particulièrement la protection internationale des droits de la propriété intellectuelle, laquelle peut être appréhendée à la fois sous un angle matériel et sous un angle conflictuel.

3. Aspect matériel des droits de la propriété intellectuelle. Les droits de propriété intellectuelle ont toujours suscité l'attention des autorités européennes et internationales. Au niveau européen d'abord, la propriété intellectuelle est reconnue explicitement par la Charte des droits fondamentaux de l'Union européenne. De surcroît, la mise en place d'un « marché unique des droits de propriété intellectuelle » figure au cœur des préoccupations de l'Union européenne, bien décidée à aller au-delà de l'harmonisation mise en œuvre par de très nombreuses directives, complétées au demeurant par une jurisprudence audacieuse de la Cour de justice (voir notamment la communication de la Commission du 24 mai 2011). Au niveau international ensuite, différents accords entre États s'intéressent plus particulièrement aux droits d'auteur (Convention de Berne et traités de l'OMPI, accord ADPIC signé dans le cadre de OMC et enfin ACTA). Une première contribution pourrait, après avoir précisé l'objet des droits d'auteur (Quelles sont les œuvres de l'esprit protégées par le droit d'auteur ? *Quid* d'une œuvre multimédia, d'un logiciel ou d'une page web ?), porter plus spécialement sur la diversité des techniques de protection tant des droits moraux de l'auteur que de ses droits

patrimoniaux. Elle pourrait également s'intéresser à la question de l'adaptation du droit des marques aux fins de protéger les titulaires de signes qui ont été repris comme noms de domaine. Plus largement, la question de la protection de la diversité culturelle mériterait d'être posée : la Convention de l'UNESCO sur la diversité des expressions culturelles permettra-t-elle de répondre efficacement aux défis du numérique ?

4. Aspect conflictuel des droits de la propriété intellectuelle. Cette internationalisation croissante de la protection substantielle des droits de propriété contraste avec le principe de territorialité qui domine classiquement la matière. Certes, la nécessité de recourir aux règles de droit international privé n'est pas discutable, en raison tant de la dimension internationale des questions soulevées que de la diversité des droits nationaux en matière de droits de propriété intellectuelle. En revanche, la question de savoir si – et dans quelle mesure – les droits de la propriété intellectuelle appellent des règles de droit international spécifiques pourrait constituer l'objet de débats intéressants (v. par exemple, en matière de conflit de lois, l'article 8 du Règlement Rome II ou encore la Convention de Berne pour la protection des œuvres littéraires et artistiques du 9 septembre 1886).

Les communications devront privilégier la réflexion juridique sur les axes évoqués ci-dessus, mais d'autres propositions originales pourront également être étudiées.

Les personnes intéressées sont invitées à transmettre un bref projet d'intervention (5 pages maximum) ainsi qu'un *curriculum vitae*.

Les propositions doivent être envoyées à Valérie Parisot (valerie.parisot@univ-rouen.fr) avec copie à Anne-Thida Norodom (anne-thida.norodom@univ-rouen.fr) et Philippe Lagrange (philippe.lagrange@univ-rouen.fr), avant le **18 mars 2013**.