Frontières légales et souveraineté dans le cyberespace ?

Me Cécile Doutriaux
Avocate et membre de la Chaire Cyberdéfense & Cybersécurité des Ecoles de Saint-Cyr Coëtquidan.

Janvier 2015 - Article II.1

Ignorant les frontières, le cyberespace rend difficile l'application des règles juridiques nationales visant à le contrôler. Pour la Cour internationale de Justice, le respect de la souveraineté territoriale est un fondement essentiel des relations entre les États [1] et la simple connexion d'une infrastructure au réseau mondial du cyberespace ne peut être analysée comme la renonciation d'un État à sa souveraineté territoriale.[2]Pourtant, les atteintes à la puissance des États et les extensions de souveraineté sont légion dans le cyberespace. Les États tentent d'élaborer des stratégies pour y remédier mais sont-elles efficaces ?

I. Les notions de frontière et de territoire appliquées au cyberespace ont-t-elles un sens ?

Créé par l'appropriation géographique, politique, économique, linguistique, idéologique et sociale, le territoire est un espace que les États doivent conquérir, sécuriser et défendre. Pour délimiter l'espace où les États exercent leur souveraineté, des frontières sont instaurées et fixent la surface territoriale sur laquelle l'État impose son autorité législative, exécutive et judiciaire. Le territoire national définit le périmètre où le droit de l'État a vocation à s'appliquer uniformément et les juridictions nationales doivent juger tous les conflits informatiques commis sur ce territoire, quels qu'en soient les auteurs et les victimes. La frontière est donc une réalité juridique qui constitue la limite entre les différents espaces de juridiction sur lesquels les États exercent la plénitude de leur pouvoir.

Cependant, la frontière n'est pas une séparation immuable et figée.[3] Elle évolue dans l'espace et dans le temps et les concepts de territoire et de frontière ont perdu de leur pertinence aujourd'hui. La mondialisation et l'existence d'un monde en réseaux contribuent à construire des espaces dont il est

[1] Affaire du Détroit de Corfou (Royaume-Uni c Albanie), CIJ Recueil 1949, 4, 35
[2] Heintschel von Heinegg «la souveraineté territoriale dans le cyberespace»
[3] Amaël Catturuzza " Réflexions préliminaires sur la notion de frontière et Internet " p.2

difficile de fixer les limites avec précision. Le cyberespace, lieu d'échange et de stockage de données, utilisant des technologies électroniques englobant Internet, les réseaux de télécommunication et les systèmes informatiques, accessible en tous points du globe, est devenu le symbole de l'érosion des frontières.[4] En effet, si les souverainetés se définissent dans des espaces physiques délimités, Internet relie tous les territoires, sans en être un lui-même et les technologies numériques se conçoivent par la circulation des flux et des données dématérialisées. La couche informationnelle du cyberespace est en perpétuel mouvement alors que la souveraineté étatique suppose l'existence d'espaces territoriaux clairement délimités. Ainsi, un État ne pourrait prétendre à la souveraineté que s'il est en mesure de contrôler l'ensemble de ses activités informationnelles, sur son territoire et en dehors de ses frontières.[5]

Le caractère international des conflits numériques est certes source de difficultés pour déterminer la loi applicable et la juridiction compétente, mais face aux agissements perpétrés dans le cyberespace, les États utilisent le droit privé et public, la loi nationale et internationale, pour sanctionner les auteurs des conflits informatiques car si le cyberespace remet en cause les frontières physiques, ses utilisateurs sont bien réels et tous localisés sur le territoire d'un État. Ainsi, malgré les phénomènes de déterritorialisation et de porosité des frontières, engendrés par la mondialisation des réseaux, le concept de territoire est toujours un critère de référence en droit. Il faut donc prendre en considération non seulement les parties du litige, c'est à dire l'auteur et la cible de l'attaque informatique, agent étatique ou non, mais aussi la localisation du conflit informatique, à l'intérieur et à l'extérieur des frontières de l'État.

II. Application du droit aux conflits informatiques dans et hors des frontières de l'État ?

2.1. À l'intérieur des frontières de l'État

Sur le territoire national, à l'intérieur de leurs frontières, les États ont le pouvoir d'exercer leur pouvoir normatif et coercitif à l'encontre des auteurs des conflits informatiques. La compétence territoriale des juridictions, son aptitude à instruire ou à juger une affaire, est une notion d'ordre public et l'État doit ici exercer sa souveraineté pleine et entière.

2.1.1. Pour les conflits informatiques entre acteurs privés.

Pour les conflits informatiques entre acteurs privés, selon le principe de territorialité, la loi nationale est applicable dès lors qu'un de ses faits constitutifs a lieu sur ce territoire.[6] La victime peut alors saisir la juridiction soit du lieu où demeure le coupable, soit celle du lieu où le dommage a été subi. Ainsi, l'accès en France à des contenus illicites suffit à attribuer la compétence aux juridictions nationales, même si les responsables se situent hors du territoire. En effet, peu importe la localisation des serveurs à partir du moment où l'infraction produit ses effets sur le territoire national. Cela signifie en théorie que pratiquement toutes les infractions commises à l'aide des réseaux informatiques relèvent de la compétence du juge national. Ainsi, dans un arrêt rendu le 9 décembre 2003, [7] la Cour de cassation a jugé que dès lors que l'infraction se produisait sur Internet, tous les pays étaient potentiellement visés, « puisque les sites litigieux sont accessibles depuis tous les pays et que le préjudice allégué, du seul fait de cette diffusion, n'est ni virtuel, ni éventuel ». On pourrait en déduire que toutes les activités en ligne sont potentiellement soumises aux législations concurrentes des ordres juridiques de tous les États où le site est accessible. Cependant, un certain nombre de liens de rattachement, entre le site mis en cause et le territoire, ont été exigés par la suite et les juges ont indiqué, dans un arrêt du 11 janvier 2005, qu'il fallait considérer le public visé (en prenant en compte la monnaie, la langue et le lieu de

[4] Nils Melzer " Cyberware fare and international law " UNIDIR, Ressources 2011 p.4
[5] Leïla Bouchera, " La souveraineté informationnelle : entre utopie et projet " Le Monde 1er février 1996
[6] A.113-2 du Code Pénal Français
[7] Société Castellblanch / Société Champagne Louis Roederer, Cour de Cassation 1ère Chambre Civile

livraison) pour que l'action puisse prospérer. [8] Il convient donc de caractériser un lien suffisant, substantiel ou significatif entre les faits commis sur Internet et le dommage allégué sur le territoire national. Dans un arrêt du 29 mars 2011, la Cour de cassation a rappelé que le seul critère de l'accessibilité d'un site internet en France ne permet pas de retenir la compétence du tribunal français. [9] Le 3 octobre 2013,[10] la Cour de Justice de l'Union Européenne a encore confirmé que si une action judiciaire peut être introduite sur le territoire où le contenu illégal est accessible, il faut en outre que le contenu litigieux soit destiné au public de cet État. En tout état de cause, la simple accessibilité du site sur un territoire national ne suffit plus à rendre les juridictions de l'État concerné compétentes, ce qui restreint la capacité des États à sanctionner, sur leur territoire, les activités illicites commises dans le cyberespace.

2.1.2. Pour les conflits informatiques entre les États.

Quand les conflits informatiques ne concernent pas des acteurs privés du cyberespace, mais des États, des forces armées, des groupes armés organisés, dans les conflits armés internationaux, d'autres règles de droit s'appliquent, mais la notion de territoire appliquée au cyberespace reste essentielle. Ainsi, pour le Manuel de Tallinn,[11] si aucun État ne peut prétendre régner sur le cyberespace, il n'en reste pas moins souverain sur son territoire. Les infrastructures numériques situées sur le territoire d'un État sont soumises à la loi et à la compétence juridictionnelle territoriale de cet État qui peut « réglementer, restreindre ou interdire l'accès à l'infrastructure digitale située sur son territoire ».[12] Par ailleurs, une atteinte portée contre l'infrastructure informatique d'un pays pourrait être interprétée comme une violation de souveraineté si la cyberopération est concomitante à une attaque qui menace l'intégrité territoriale de la nation et si elle est d'une intensité suffisante [13]c'est-à-dire lorsque un État se voit obligé de modifier des éléments fondamentaux de sa politique, de son système culturel ou socio-économique.

2.2. Hors des frontières nationales de l'État

Si l'exercice de la puissance législative des États est en principe limité à son territoire national, en vertu du droit international général, des facteurs de rattachement comme le domicile et la nationalité sont acceptés et permettent aux États d'exercer leur compétence au delà de leurs frontières nationales. Ainsi, le principe de l'extra-territorialité permet de considérer qu'une loi nationale est applicable à tout crime ou délit puni d'emprisonnement, commis par un français ou par un étranger, sur une victime de nationalité française. [14]Cependant, le droit ne conserve sa vocation à régir les infractions réalisées hors de son territoire que si les attaques informatiques sont également punies par la législation du pays où elles ont été commises, selon le principe de la double incrimination. [15] Dans la mesure où les réseaux et Internet couvrent des espaces qui relèvent de conceptions culturelles, morales, sociales, économiques et sociologiques différentes, il est évident que les règles nationales ne suffisent pas et que la solution doit être nécessairement trouvée au niveau international, pour garantir la poursuite et la condamnation effective des auteurs des cyberconflits. C'est la raison pour laquelle accélérer l'harmonisation des lois nationales régissant les conflits numériques est nécessaire. À ce jour, quatre vingt deux pays ont signé ou ratifié plusieurs conventions contraignantes relatives à la cybercriminalité telles que la Convention de Budapest du Conseil de l'Europe, la Convention de la Ligue des États arabes sur la lutte contre les infractions liées aux technologies de l'information, les Accords des États indépendants en matière de lutte contre les infractions informatiques et l'Accord de l'organisation de Shanghai pour la coopération dans le domaine de la sécurité internationale de l'information. Ces instruments législatifs permettent d'assurer plus facilement la répression des

[8] Cour de Cassation, Arrêt du 11 janvier 2005, Hugo Boss / Reemtsma Cigarettenfabriken
[9] Cour de Cassation, Arrêt du 29 mars 2011, Ebay Europe et autres / Maceo et autres
[10] CJUE, arrêt du 3 octobre 2013 Peter P. / KDG Mediatech AG
[11] Manuel de Tallinn, Cambridge University Press mars 2013
[12] Manuel Tallinn, (article 1 de la souveraineté)
[13] J.Combacau et S Sur, Droit international public (Montchrestien, Paris 2012), 266
[14] Article 113-7 Code Pénal
[15] Article113-6 Code Pénal

attaques informatiques émises hors des frontières nationales des États, mais les États demeurent bien évidemment libres d'adhérer ou pas à ces conventions.

III – Quelles atteintes et extensions de souveraineté des États dans le cyberespace ?

3.1. L'exercice difficile de la souveraineté de l'État dans le cyberespace.

3.1.1. Sur le territoire national.

S'il appartient aux États d'exercer leur souveraineté et de faire respecter leurs lois sur leur territoire national, les Etats n'ont pas toujours les moyens d'assurer le respect de leur réglementation à l'intérieur de leurs frontières, quand ils ordonnent aux fournisseurs d'accès à internet de bloquer l'accès de sites illégaux sur leur territoire national. Ces intermédiaires techniques, au sens de l'article 8.3 de la directive 2001/29/CE du parlement européen, peuvent agir selon trois techniques, à savoir par blocage de l'adresse "Uniform Resource Locator" (URL), de l'adresse "internet Protocol" (IP) ou encore par blocage du nom de domaine ("Domaine Norme System" ou "DNS").Mais la mise en place de telles mesures est longue, coûteuse et peut s'avérer inefficace. Dans une affaire jugée le 14 octobre 2011 par le Tribunal de Grande Instance de Paris, le site Copwatch, localisé au États-Unis pour dénoncer les violences policières en diffusant les données personnelles (nom, prénom, adresse internet, numéro de téléphone, photographies) de nombreux fonctionnaires des forces de l'ordre avait été bloqué par les fournisseurs d'accès.[16] Une nouvelle action en justice a été engagée un an plus tard, car une version identique du site Copwatch était mise en ligne et il convenait d'interdire, à l'ensemble des abonnés situés sur le territoire national, l'accès aux 34 « sites miroirs ». Mais les experts ont indiqué que les délais nécessaires à la mise en place de ces mesures techniques seraient de six mois à un an et représentait un investissement initial de l'ordre de 10 millions d'euros par opérateur. Dans une décision rendue le 28 novembre 2013,[17] le TGI de Paris a ordonné à cinq fournisseurs d'accès à internet de bloquer les sites du réseau Allostreaming et à trois moteurs de recherche (Google, Microsoft et Yahoo) de les déréférencer pour faire cesser la représentation illicite de films ou de séries, en mode streaming, au profit des internautes français. Là encore, les fournisseurs d'accès à internet ont indiqué que les sites visés allaient contourner ces dispositions. Ici, ce n'est donc pas la règle de droit qui est défaillante, mais l'impossibilité pour un État d'exercer la plénitude de sa souveraineté sur son territoire et d'assurer l'effectivité de ses décisions judiciaires quand les serveurs et les données sont localisés à l'étranger.

3.1.2. Lors des enquêtes internationales pour identifier les auteurs des attaques informatiques

D'autres atteintes à la souveraineté des États existent dans le cadre des enquêtes criminelles internationales. Les États sont généralement tenus de transmettre les données de connexion permettant d'identifier l'auteur d'un conflit informatique situé sur leur territoire aux autorités répressives étrangères.[18] Pour pouvoir accéder à ces informations techniques auprès des fournisseurs d'accès à internet, recueillir le consentement préalable de l'État qui détient les données de connexion est indispensable, selon la Cour Permanente de justice internationale dans son arrêt sur l'affaire " Lotus".[19] Cet arrêt précise que tout exercice de la puissance d'un État ne peut s'exercer hors de son territoire, sauf s'il existe une règle permissive contraire, découlant du droit international coutumier ou d'une convention. En théorie, seuls sept pays autorisent l'accès aux données de connexion (Finlande, Portugal, Pologne, Chili, Monténégro, Japon et États-Unis) aux autorités étrangères. En revanche, cet accès sans consentement n'est plus autorisé dans neuf autres pays, (République tchèque, Lituanie,

[16] Tribunal de grande instance de Paris Ordonnance de référé 10 février 2012, http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=3337
[17] Tribunal de grande instance de Paris Ordonnance de référé 28 novembre 2013, http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=3935
[18] Articles 31 et 32 de la convention de Budapest du 23 novembre 2001.
[19] Affaire du Lotus (France c/Turquie ° CPIJ série A, n°10, p.18 (1927).

Allemagne, Suède, Turquie, Bosnie-Herzégovine, Hongrie, Estonie et Pays-Bas)[20]. En pratique, malgré l'obligation de recueillir le consentement de l'État concerné, les autorités répressives obtiennent fréquemment l'accès à des données stockées à l'étranger en coopérant avec des entreprises privées, sans qu'aucune demande d'entraide judiciaire ne soit adressée à l'État où les données sont localisées. La Chambre de Commerce Internationale a révélé que de multiples entreprises sont soumises aux fortes pressions des gouvernements étrangers qui veulent obtenir la communication des données de connexion, alors que cet accès sans consentement n'est pas autorisé par la législation de leur pays.[21] Ainsi, de nombreux États portent atteinte à la souveraineté nationale d'autres États, dans le cadre des enquêtes internationales, visant à réprimer les infractions informatiques.

3.2. Les extensions de souveraineté des États.

3.2.1. L'application du droit national hors des frontières de l'État.

Un juge national peut-il appliquer le droit de son État en dehors des limites de son territoire et méconnaître ainsi la souveraineté des autres États ?Au delà des difficultés techniques, les mesures de filtrage et de blocage de sites étrangers sur le territoire national peuvent être aussi de nature à porter atteinte à la souveraineté d'un autre État. Dans un litige qui a opposé l'Allemagne à la société Américaine CompuServe,[22] la justice avait ordonné de rendre des forums inaccessibles sur le territoire allemand, en application de la loi allemande qui en réprimait le contenu. Cette décision judiciaire avait eu pour effet de priver d'accès aux sites 4 millions de souscripteurs de la société Compuserve, répartis dans 140 pays. Dans une autre affaire, le Tribunal de Grande Instance de Paris avait exigé de la société américaine Yahoo Inc. la mise en place d'un système de filtrage destiné à identifier les internautes français, afin de leur interdire l'accès au site de ventes aux enchères d'objets nazis. [23] La société Yahoo a estimé qu'une juridiction étrangère ne pouvait pas lui imposer d'intervenir sur ses serveurs localisés aux Etats-Unis et qu'une mesure coercitive à son encontre ne pouvait recevoir aucune application, puisqu'elle était en contradiction avec le 1er amendement de sa Constitution, garantissant à tout citoyen la liberté d'expression. Ici, l'application d'un droit national a des impacts hors des frontières, quand il s'applique à l'ensemble des usagers du réseau situés sur d'autres territoires nationaux et l'État peut se voir reconnaître un surcroît de puissance, une extension de sa sphère de souveraineté, qui met en concurrence la puissance des autres États.

3.2.2. Garantir la souveraineté des États par la prévention des attaques informatiques sur son territoire.

Enfin, si la souveraineté est entendue comme le droit d'exercer, à l'exclusion de tout autre État, ses prérogatives sur son territoire, elle implique aussi le devoir de protéger le territoire des autres États, en vertu du principe de l'égalité souveraine des États consacré par l'article 2 (1) de la Charte des Nations Unies. Ainsi, en droit international « aucun État n'a le droit d'utiliser ou de permettre l'utilisation de son territoire de manière à causer un préjudice sur le territoire d'un autre État ».[24] Dans l'affaire relative au Détroit de Corfou, la Cour de Justice Internationale a indiqué que chaque État avait l'obligation « de ne pas laisser son territoire servir aux fins d'actes contraires aux droits d'autres États ».[25] Selon le Manuel de Tallinn, il existe un devoir à la charge des États pour prévenir les actes illégaux commis dans le cyberespace qui émanent de leur territoire et qui causent des dommages suffisamment graves à des personnes ou à des biens. Mais l'application du devoir de prévention dans le cyberespace doit tenir compte de la capacité réelle des États à maîtriser les infrastructures

[20] http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY2012/TCY(2012)3F_transborder_repV31public_7Dec12.pdf

[21] ICC Policy Statement: Cross-border law enforcement access to company data – current issues under data protection and privacy law » (février 2012)

[22] Affaire Ministère Public de Munich Allemagne contre CompuServe, jugement du 28 mai 1998 – 8340, Ds 465

[23] TGI Paris, ordonnance du référé du 20 novembre 2000, http://www.juriscom.net/txt/jurisfr/cti/tgiparis20001120.htm

[24] Affaire Fonderie de Trail (United States v Canada) Recueil des sentences arbitrales internationales, Vol III pp 1905-1982, 1965 (1941)

[25] Détroit de Corfou, fond, arrêt, C.I.J. Recueil 1949, p. 21

numériques localisées sur leur territoire. De fait, elles appartiennent le plus souvent à des sociétés privées, sur lesquelles les États n'ont pas toujours de véritable emprise.

Conclusion

La loi s'est révélée insuffisante pour garantir la puissance d'une nation face aux atteintes et aux extensions de souveraineté des autres États. Dans ces conditions, quelles sont les stratégies envisagées par les États pour retrouver leur souveraineté numérique ? En réalité, les mesures prises sont d'avantage d'ordre technique que juridique. Ainsi, les États souhaitent retrouver leur indépendance et développer leurs propres réseaux numériques. Par exemple, le Brésil veut construire un câble de fibre optique qui relierait l'Europe et l'Amérique latine. Certains États envisagent la possible fermeture d'une partie des infrastructures numériques pour contrer un incident cybernétique mettant en danger leurs intérêts essentiels, même si cela peut avoir une incidence sur les réseaux et les systèmes informatiques des autres États. L'affaire Prism a alerté les États sur l'importance de relocaliser les serveurs et les données sur les territoires nationaux. En France, il a été décidé de privilégier les infrastructures nationales pour garantir la confidentialité des données stockées dans le nuage avec Numergy et Cloudwatt. L'Allemagne a pris des mesures de repli stratégique sur les achats de matériels et logiciels informatique et a appelé à la création d'un espace internet européen dans lequel les données personnelles seraient préservées. Pour assurer la sécurité des systèmes d'information de l'État, le gouvernement français oblige les administrations à utiliser exclusivement les réseaux et infrastructures nationales, à héberger les données sensibles sur le territoire et à acquérir des produits et des services de sécurité labellisés par l'Agence Nationale de Sécurité des Systèmes d'information.[26] Sans toutefois opter pour la position de la Chine, de la Russie et de l'Iran qui militent pour un cyberespace fermé et ultra-contrôlé, nous assistons à la mise en place d'un certain protectionnisme numérique. Cela signifie-t-il pour autant que nous allons assister au morcellement du cyberespace en plusieurs territoires isolés et à la fragmentation des couches matérielle, logicielle et informationnelle, pour aboutir à une « Balkanisation » du cyberespace ? En réalité, on en est loin car si les États, avec le soutien des entreprises, souhaitent proposer une alternative aux produits et logiciels asiatiques et américains, elles ne peuvent avoir pour stratégie, à long terme, de garder toutes leurs infrastructures et leurs données uniquement sur leur territoire, pour garantir une offre réellement compétitive dans un contexte mondialisé. Ainsi, malgré la volonté politique des États et la meilleure sécurisation de leurs systèmes d'information essentiels, les mesures prises sont aujourd'hui d'une efficacité relative pour se réapproprier leur part de souveraineté dans le cyberespace.

[26] Voir Politique de sécurité des systèmes d'information de l'État-ANSSI du 17 juillet 2014