Applicabilité du droit international au cyberespace

Laurent Prosperi

laurent.prosperi@ens-paris-saclay.fr

18 octobre 2020

L'application du droit international au cyberespace est devenu un enjeu majeur des discussions internationales [1]. Dès 2013, le Groupe d'experts gouvernementaux (GGE), chargé d'examiner les progrès de l'informatique dans le contexte de la sécurité internationale au sein de l'ONU, a affirmé que « le droit international et, en particulier, la Charte des Nations Unies sont applicables et essentiels au maintien de la paix et de la stabilité ainsi qu'à la promotion d'un environnement informatique ouvert, sûr, pacifique et accessible » [2]. Par contre, les discussions achoppent sur l'absence de référentiel partagé et sur les modalités de l'application du droit. Trois questions se posent. Est-il licite pour un État de mener des cyberopérations ? Quelles réponses peuvent être adoptées en réaction à une agression cyber dans le respect du droit international ? Pourquoi n'est il pas appliqué en pratique et quelles sont ses limites ?

1 Licéité des cyberopérations

Le développement de capacités cyber par des États n'est pas encadré par le droit international, en effet « le système de sécurité collective est fondé sur la régulation de la force et non de moyens utilisés » [3]. Par contre, une cyberopération peut être illicite au regard de certaines conventions (pas forcément adoptées par une majorité de pays

1. F. Delerue et A. Géry. « Chapitre 3. Les aspects juridique et stratégique de la cyberdéfense. Le droit international et la cyberdéfense ». In : *La Cyberdéfense*. U. Paris : Armand Colin, 2018, p. 61-70, p. 61.

2. Ibid., p. 62.

3. A. Géry. « Droit international et prolifération des cyberarmes ». In : *Politique étrangère* Été.2 (2018), p. 43-54, p. 46.

et souvent non contraignantes) en fonction de la manière dont elle est conduite ou de par ses effets. La première norme est *le respect de la souveraineté territoriale* d'un État [4]. Pour qu'elle soit caractérisée, il faut cumuler les critères suivants : l'opération doit être attribuable à un État et conduite contre un autre État ; l'opération doit produire des effets sur des systèmes situés sur le territoire de l'État victime ou dans sa juridiction ; et, enfin, un seuil d'intensité doit être atteint, souvent défini comme étant la manifestation d'effets physiques voire létaux. La deuxième norme est le *principe de non-intervention* dans les affaires d'un État, c'est l'un des principes les plus bafoués par les cyberopérations. Les opérations informationnelles tombent sous le coup de cette norme. Pour que la violation soit caractérisée, il faut réunir les critères suivants : l'opération doit être attribuable à un État et conduite contre un autre État ; elle doit avoir un objectif coercitif direct ou indirect dans la conduite des affaires intérieures ou extérieures ; et elle ne s'applique que sur des matières à propos desquelles le principe de souveraineté des États permet à chacun d'entre eux d'en décider librement. La troisième est l'interdiction de recours à la force. Pour que la violation soit caractérisée, elle doit vérifier les paramètres cumulatifs suivants : l'opération doit être attribuable à un État ; un certain seuil d'intensité doit être dépassé. La littérature est réservée quant à sa définition, mais un consensus semble se faire pour le considérer comme atteint s'il y a la manifestation d'effets physiques sur les biens, la survenue de blessures ou la mort d'individus ou alors, s'il n'y a pas de dommage physique mais que la destruction cyber déstabilise l'État (par exemple son système de santé). L'opération Olympic Games (Stuxnet) conduite contre l'Iran [5] est l'une des rares cyberopérations pouvant être classée comme un usage illicite de la force. Notons [6] que seuls les cas les plus graves d'emploi de la force peuvent être qualifiés d'agression armée et ainsi ouvrir la possibilité pour l'État victime d'invoquer son droit de légitime défense.

4. En droit international le principe de souveraineté ne peut être caractérisé qu'en ce qui concerne les actes d'un État contre un autre État ou qui lui sont attribuables

5. En 2010, est dévoilé l'opération Olympic Games, menée en collaboration par les États-Unis et Israël, visant à ralentir le programme nucléaire iranien à l'aide du virus Stuxnet afin d'endommager les centrifugeuses de l'usine d'enrichissement d'uranium de Natanz.

6. Notions rappelées par la Cour international de justice dans l'affaire du Nicaragua 1986

2 Quelles réponses dans le respect du droit international ?

2.1 En temps de paix

Le schéma proposé par François Delerue [7] (figure 1) se concentre sur le droit international applicable en temps de paix, il n'inclut pas le droit des conflits armés. La réponse se déroule en quatre temps. Le premier est celui de l'attribution légale qui se fait selon *les articles sur la responsabilité de l'État pour fait internationalement illicite* adoptés par la commission du droit international en 2001, qui reflètent le droit international coutumier en matière de responsabilité des États. Il faut définir l'objet (opération, situation) imputé juridiquement à un État selon deux modalités (étape 1.a. et 1.b. du schéma). La première se déclenche si l'objet est du *fait de l'État*, c'est à dire s'il est commis par ses forces (Article 4) ou par des entités exerçant des prérogatives régaliennes [8] (Article 5) ou par des forces (ou capacités) mis à la disposition d'un autre État (Article 6). La deuxième modalité correspond à un acte *commis pour le compte d'un État* par un acteur non étatique ; l'attribution se fera opération par opération. C'est à dire, qu'une opération ne sera attribuée à un État que si elle est commise sous les instructions, la direction ou le contrôle de cet État (article 8) ou alors en cas d'absence ou de carence des autorités officielles (article 9), par un mouvement (article 10) reconnu par un État comme étant sien (article 11). En pratique, cela se traduit par le fait que les actes d'un Advance Persistent Threat (APT) [9] proche d'un État peuvent ne pas être attribués à ce dernier, par exemple dans le cas où les deux entités ont poursuivi des objectifs différents sur un sujet donné.

Après l'attribution effectuée vient le temps de l'évaluation de l'illicéité (étape 2.a) et de la responsabilité de l'État (étape 2.b) qui conditionnent les réponses possibles. Notons que l'illicéité d'une opération peut être atténuée voire supprimée dans certains cas comme lors d'une réaction à un acte illicite antérieur (contre-mesures ou légitime défense) de nature numérique ou non. Une fois le caractère transgressif constaté, un État lésé est en droit d'invoquer la responsabilité de l'État effecteur et de demander la réparation du préjudice et des éventuels dommages subis. Même si une opération cybernétique n'est pas attribuée à un État, la responsabilité

7. F. Delerue. « Note de recherche n° 84 ». In : *IRSEM* 84 (2019), p. 8.

8. Comme par exemple, une société privée de cybersécurité ayant un contrat avec un État.

9. Le terme d'APT désigne des menaces persistantes souvent mises en œuvre par des groupes structurés utilisant un ensemble de techniques et d'outils de hauts niveaux.

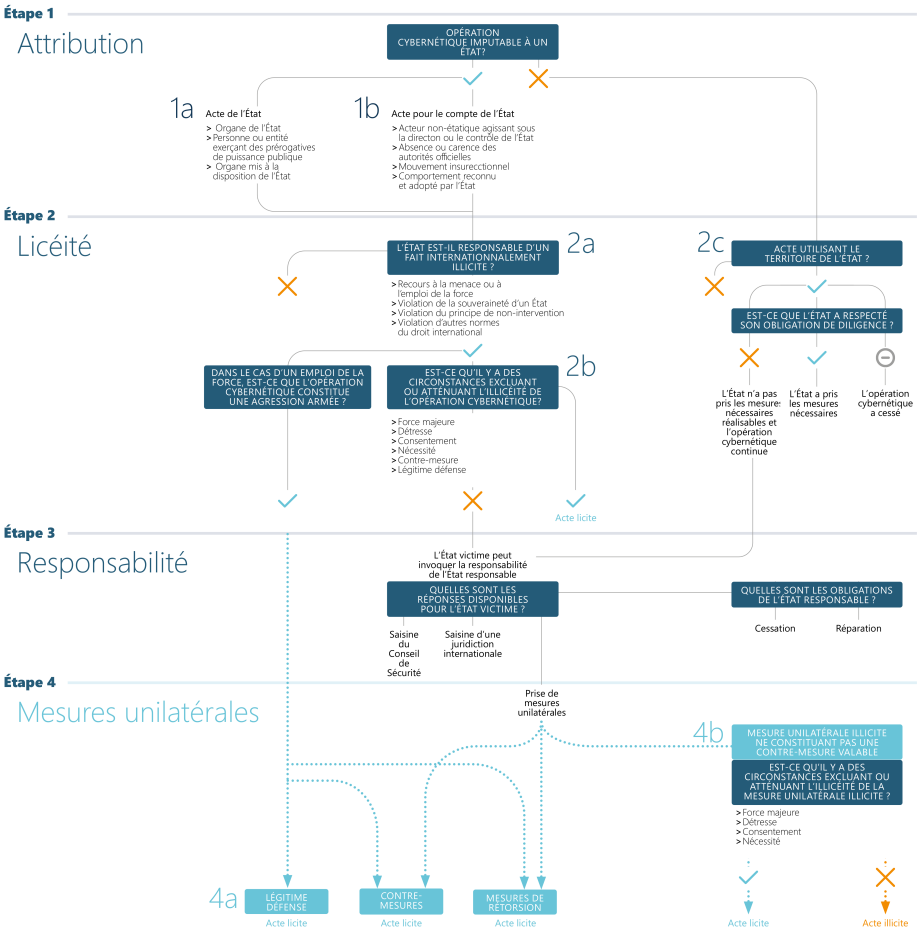

FIGURE 1 – Schéma sur l'application du droit international aux opérations cybernétiques en temps de paix [a]

a. F. DELERUE. « Note de recherche n° 84 ». In : *IRSEM* 84 (2019), p. 8.

de celui-ci peut quand même être engagée du fait de l'obligation de diligence (due diligence) qui lui incombe (étape 2c). C'est une obligation de moyens et non de résultats visant à empêcher que le territoire d'un État tiers ne serve (lancement ou transit) à des cyberattaques visant un autre État. Une fois la responsabilité d'un État engagée, plusieurs obligations lui incombent : la cessation (ou la non répétition) de l'acte ainsi que la réparation intégrale du préjudice causé (restitution, indemnisation, reconnaissance de la violation ou autre).

Une fois la responsabilité d'un État agresseur engagée, une gradation de réponses possibles [10] s'offre à la victime [11] en commençant par des mesures diplomatiques, par

10. Le droit international impose aux États l'obligation de régler leurs différends internationaux par des moyens pacifiques en respectant le principe de proportionnalité de la réponse.

11. *Entretien réalisé le 3/09/2020 avec un membre de la Direction des Affaires Juridiques*

exemple en adressant des protestations officielles ou une note blanche. Le deuxième échelon correspond au recours à une tierce partie comme arbitre en saisissant le Conseil de sécurité des Nations Unies (excluant de facto toutes les agressions commises par les membres permanents, c'est à dire par des puissances cyber majeures) ou en soumettant le différend à une juridiction internationale, comme la Cour internationale de Justice par exemple. Le troisième échelon comprends des mesures unilatérales extrajudiciaires qui peuvent être prises à l'égard de l'agresseur proportionnellement à l'agression subie. Elles vont de la rétorsion licite (mais non amicale) à des contre-mesures non militaires [12] considérées licites en réaction à un acte illicite (menace ou recours à la force, intervention illicite, violation de souveraineté). En dernier recours, l'État agressé peut mettre en œuvre des mesures militaires dans le cadre de l'article 51 de la Charte des Nations Unies en cas d'agression armée.

En pratique, cette hiérarchie de réponses est mises à mal par la temporalité des opérations cyber (avec une exploitation souvent très rapide). Pour y palier et pour conserver sa capacité de réponse, le concept de légitime défense préemptive s'applique, comme pour la défense anti-missile, en fonction de de l'ampleur des dommages supposés et seulement si l'acte adverse est imminent (en terme d'heures). En cas de mise en œuvre, une notification doit être adressée au conseil de sécurité de l'ONU, les contre-mesures non militaires sont soumises à la même obligation de notification. Dans le cas de l'invocation de l'*état de nécessité*, que les acteurs mis en cause soit étatiques ou non, la notification peut avoir lieu a posteriori. Pour F.Delerue, « le scénario le plus probable [impliquant un recours à la force] serait celui de l'invocation de l'état de nécessité, seul moyen pour l'État de sauvegarder un intérêt essentiel contre un péril grave et imminent ».

2.2 En temps de guerre

Le Manuel de Tallinn [13] de 2013, est la référence otanienne définissant l'applicabilité du Droit des Conflits Armés (DCA) au cyberespace [14]. Il a fallu attendre le 9

(SGA/DAJ).

12. Les contre-mesures collectives sont interdites en droit international. Par exemple, pour que le régime de sanction de l'Union Européenne soit appliqué, il faut que l'UE dans son ensemble se sente menacée.

13. M. N. Schmitt et N. C. C. D. C. of Excellence, éd. *Tallinn manual on the international law applicable to cyber warfare : prepared by the international group of experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence*. Cambridge ; New York : Cambridge University Press, 2013. 282 p.

14. Notons que le DCA ne s'applique que dans les conflits armés à caractère international (i.e, entre plusieurs États) ou non international lorsqu'il implique des acteurs non étatiques opposés à

septembre 2019, pour que le ministère des Armées rende public un rapport intitulé *Droit international appliqué aux opérations dans le cyberespace* définissant l'interprétation française de l'application du DCA aux opérations cyber. Premièrement, les cyberopérations peuvent transformer un conflit armé non international en conflit armé international (opposant plusieurs États) de par l'utilisation d'outils cyber par un État extérieur en soutien à l'une des parties contre un adversaire étatique. C'est le cas le plus plausible, car les cyberopérations offrent un moyen particulièrement efficace [15] d'intervention pour les acteurs extérieurs dans un conflit. Par ailleurs, le rapport considère que des cyberopérations prolongées peuvent caractériser un conflit armé non international [16] si un seuil (non défini) de violence est atteint. En l'état actuel de la technologie, il semble improbable qu'un niveau de violence suffisant soit obtenu par le seul recourt aux actions cyber.

Suivant le manuel de Tallinn, les opérations cyber peuvent constituer des attaques, au sens de l'article 49 du Protocole additionnel I aux Conventions de Genève (PA I), si elles produisent des dommages physiques. Le recueil d'informations et l'altération des capacités d'influence adverses ne sont pas considérées comme des attaques mais restent soumis au DCA. A la différence du texte de référence otanien, la France a une interprétation plus large des attaques dans son rapport de 2019 qui englobe la mise hors d'état de systèmes d'information ou qui nécessite une intervention pour rendre le système de nouveau opérant [17]. Les principes de proportionnalité et de distinction entre objectifs militaires et biens civils, entre civils et combattants du DCA s'appliquent. Le document français renforce le principe de discrimination dans le monde numérique, en considérant que l'article 52 alinéa 3 du PA I oblige les États à appliquer en cas de doute une présomption de caractère civil à un bien traditionnellement affecté à un usage civil.

En plus du DCA, le droit à la neutralité s'applique dans le cyberespace dans le cadre d'un conflit armé international. À ce titre, les parties impliquées ne peuvent mener des cyberopérations en lien avec ce conflit à partir d'un territoire d'un État neutre, ni prendre le contrôle de systèmes informatiques de l'État neutre (ou sous

un ou plusieurs États.

15. Delerue et Géry, op. cit., p. 66.

16. opposant des forces armées gouvernementales aux forces d'un ou de plusieurs groupes armés, ou opposant plusieurs groupes armés entre eux

17. Ainsi, l'altération des capacités de propagande de l'adversaire, notamment le fait de rendre indisponible un site d'influence par saturation ou déni de service, non prohibée par le DIH par analogie aux actions classiques de brouillage des communications radio ou d'émissions de télévision, ne saurait être caractérisée comme une attaque.

sa juridiction) pour conduire de telles opérations [18]. Par contre, le statut de partie neutre est assorti de l'obligation d'empêcher tout usage offensif des infrastructures informatiques situées sur son territoire (ou sous son contrôle) par des États belligérants [19].

3 Le droit international à la peine

Bien que l'applicabilité du droit international au cyberespace fasse l'objet d'un consensus, sa mise en œuvre effective est rendue complexe par la nature du cyberespace et par l'absence d'un corpus normatif dédié. En pratique, la difficulté d'attribution restreint de facto son application. De plus, les traités actuels régulant les cyberarmes sont non contraignants et ne permettent pas « à eux seuls de garantir la stabilité du cyberespace » [20]. Par ailleurs, la construction d'un corpus dédié aux problématiques du milieu cyber achoppe sur l'absence de référentiel partagé et sur les modalité de l'application du droit. Les positions américaines et chinoises (et russes) sont séparées par un fossé conceptuel. Les premiers considèrent que la cybersécurité est une affaire de couche matérielle et logique alors que les seconds se préoccupent de la sécurité et du contrôle de l'information principalement à des fins de politique intérieure afin de maitriser les usages numériques de leur population pour garantir la survie du régime et pour se positionner face aux États-Unis qu'ils perçoivent comme la menace majeure dans le cyberespace. Cette ligne de fracture existe depuis le milieu des années 1990 [21]. Depuis 1998, Moscou soumet chaque année un projet de traité de désarmement du cyberespace, soutenu par Pékin, qui traite aussi de la liberté de circulation des informations car celle-ci représentent une menace de premier plan pour ces régimes. Ce traité est rejeté par les Américains. Ils sont rétifs à toute action pouvant brider leur prééminence en matière numérique, en partant du postulat que le contrôle des armements pourrait jouer en leur défaveur du fait de leurs (sur)capacités offensives. La cristallisation de ces divergences est l'échec du dernier cycle de négociations des GGE (2016-2017) qui s'est terminé sans

18. Article 1 de la Convention V concernant les droits et les devoirs des Puissances et des Personnes neutres en cas de guerre sur terre, et de la Convention XIII concernant les droits et les devoirs des Puissances neutres en cas de guerre maritime, La Haye, 18 octobre 1907

19. Article 8 de la Convention V concernant les droits et les devoirs des Puissances et des Personnes neutres en cas de guerre sur terre, et de la Convention XIII concernant les droits et les devoirs des Puissances neutres en cas de guerre maritime, La Haye, 18 octobre 1907.

20. Géry, op. cit., p. 43.

21. J. Nocetti. « Géopolitique de la cyber-conflictualité ». In : *Politique étrangère* Été.2 (2018), p. 15-27, p. 24.

consensus et donc sans rapport final.

Deux approches s'opposent pour assurer la stabilité et la sécurité dans le cyberespace [22]. La première, ayant prévalue pendant les GGE et soutenue par les États-Unis, repose sur des engagements politiques. Son hypothèse de travail est que le droit international existant est suffisant pour réguler les comportements et son objectif est de « traduire les attentes de la communauté internationale » [23] par l'adoption de normes de comportements responsables entre États. Cependant, les limites d'une telle approche sont vite atteintes car les normes sont non contraignantes et sont endossées selon un engagement unilatéral. La seconde est légaliste, l'objectif étant de créer de nouveaux droits et devoirs afin d'adapter le droit international aux réalités du cyberespace. Cette voie part du principe que le droit international existant ne permet pas de réguler les comportements étatiques dans le cyberespace du fait des caractéristiques intrinsèques de ce dernier. Cette approche est défendue par les États membres de l'organisation de coopération de Shanghai [24].

Cette dichotomie a mené à la création en 2019 de deux groupes de travail sous mandat de l'ONU : le GGE 2019-2021 [25] et l'Open-ended Working Group (OEWG) 2019-2020 [26]. Le premier rassemble 25 États membres (dont la France, la Russie et la Chine) autour des États-Unis alors que le second rassemble tous les états membres qui le souhaitent (notamment la Chine, la Russie, les États-Unis et la France) mais aussi des acteurs non étatiques qu'ils soient industriels (comme Microsoft et Kaspersky), académiques (e.g. National Law University Delhi's Centre for Communication Governance)ou des organisations non gouvernemental (e.g l'Internet Society). Les deux groupes disposent d'un plan de vol similaire : développer (ou faire évoluer) des normes, des lois et des principes ; renforcer la confiance entre les acteurs et faire augmenter le niveau général de cybersécurité ; travailler sur l'application du corpus existant du droit international au cyberespace.

22. Delerue et Géry, op. cit., p. 69.
23. Ibid., p.62.
24. Celle-ci a proposé des codes de conduite pour la sécurité de l'information en 2011 et 2015 (ibid.)
25. *Résolution 73/266 des Nations Unies*. 22 décembre 2018.
26. *Résolution 73/27 des Nations Unies*. 11 décembre 2018 ; *Open-ended Working Group – UNODA*. URL : `https://www.un.org/disarmament/open-ended-working-group/` (visité le 15/09/2020).

Conclusion

Certes, l'applicabilité du droit international au cyberespace fait consensus, cependant son utilité en l'état est fortement remise en question car les instruments juridiques sont non contraignants, non universels (n'englobant pas tous les acteurs), d'une précision variable (absence de définitions communes) et souffrent d'une absence d'articulation entre les différents instruments existants. À ce jour, « très peu d'États ont officiellement recouru au droit international pour adopter des mesures unilatérales extrajudiciaires en réaction à un comportement dans l'espace numérique et la Cour internationale de justice n'a pour l'instant été saisie d'aucune affaire relative à un comportement dans l'espace numérique. » [27]. Par ailleurs, toute évolution, à court terme, semble compromise de par l'opposition entre les conceptions sur la définition de la cybersécurité et de par la divergence d'approche. Enfin, notons que les textes en vigueur ne régissent que les interactions entre États, or le cyberespace est constitué d'une multitude d'acteurs non étatiques pouvant rivaliser avec les états en terme de puissance. Par exemple, les textes n'encadrent pas l'usage du hack-back [28] par les acteurs privés. Il n'y a pas de consensus en Occident. Les Anglo-saxons encouragent cette pratique et la France milite pour son interdiction (c'est déjà le cas en droit national).

27. Delerue et Géry, op. cit., p. 64.

28. Le hack-back , apparenté à au concept de cyberdéfense active, consiste en une action offensive visant à faire cesser une attaque.

Bibliographie

Bibliographie générale

Open-ended Working Group – UNODA. URL : `https://www.un.org/disarmament/open-ended-working-group/` (visité le 15/09/2020).

Delerue, F. « Note de recherche n° 84 ». In : *IRSEM* 84 (2019), p. 8.

Droit international appliqué aux opérations dans le cyberespace. Ministère des Armées, 2019.

Delerue, F. et A. Géry. « Chapitre 3. Les aspects juridique et stratégique de la cyberdéfense. Le droit international et la cyberdéfense ». In : *La Cyberdéfense*. U. Paris : Armand Colin, 2018, p. 61-70.

Géry, A. « Droit international et prolifération des cyberarmes ». In : *Politique étrangère* Été.2 (2018), p. 43-54.

Nocetti, J. « Géopolitique de la cyber-conflictualité ». In : *Politique étrangère* Été.2 (2018), p. 15-27.

Résolution 73/266 des Nations Unies. 22 décembre 2018.

Résolution 73/27 des Nations Unies. 11 décembre 2018.

Schmitt, M. N. et N. C. C. D. C. of Excellence, éd. *Tallinn manual on the international law applicable to cyber warfare : prepared by the international group of experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence*. Cambridge ; New York : Cambridge University Press, 2013. 282 p.

Liste des entretiens

Entretien réalisé le 3/09/2020 avec un membre de la Direction des Affaires Juridiques (SGA/DAJ).

28. Le terme d'agent désigne un poste technique, le terme de conseiller désigne un poste s'intéressant à la stratégie et le terme de responsable désigne un poste d'encadrement et de décision.