30 octobre 2019

IRSEM
INSTITUT DE RECHERCHE STRATÉGIQUE
DE L'ÉCOLE MILITAIRE

NOTE DE RECHERCHE – n° 84

SCHÉMA SUR L'APPLICATION DU DROIT INTERNATIONAL AUX OPÉRATIONS CYBERNÉTIQUES

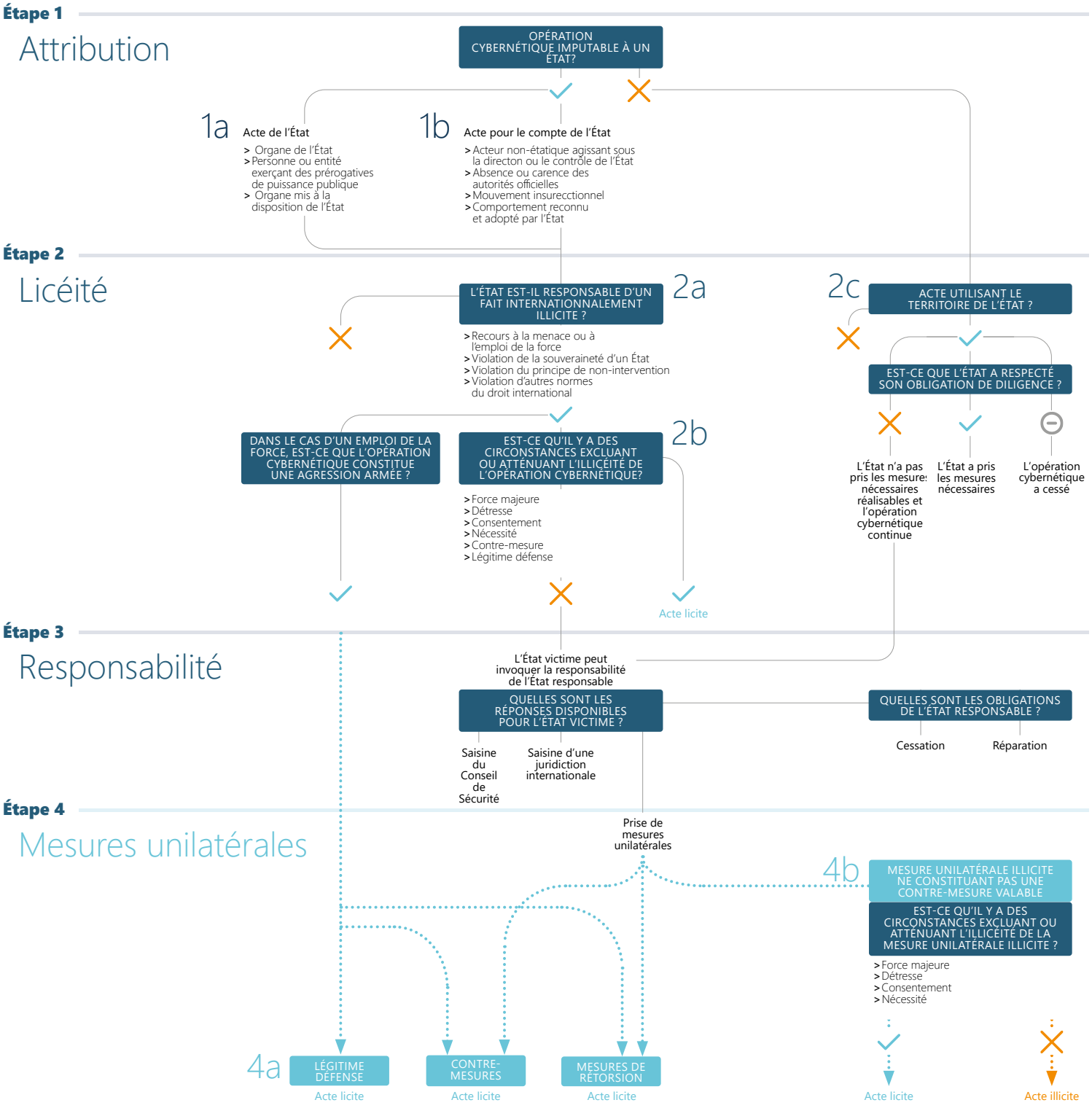
François DELERUE
Chercheur Cyberdéfense et droit international à l'IRSEM

RÉSUMÉ

Le droit international est applicable au cyberespace et aux cyberopérations. Il convient néanmoins de s'interroger sur l'interprétation et la mise en œuvre concrète de ce corpus juridique : que peut faire un État si son système de transport, son réseau d'énergie ou toute autre infrastructure critique est mis hors service pendant une période prolongée en raison d'une opération cybernétique ? Quelles réactions doit-il adopter face à d'importantes perturbations sur son fonctionnement, des pertes économiques voire, potentiellement, des pertes humaines ? Une réponse militaire serait-elle justifiée ? Ces questions, qui n'épuisent pas le sujet, découlent des modalités d'application au cyberespace du droit international. Si des réponses spécifiques doivent toujours être apportées au cas par cas à la suite d'une analyse factuelle et juridique approfondie, il est possible de schématiser le processus logique d'application du droit international à une opération cybernétique, de la détermination de l'identité de son auteur à l'adoption de mesures unilatérales contre l'État ou l'acteur responsable.

SOMMAIRE

AVERTISSEMENT : l'IRSEM a vocation à contribuer au débat public sur les questions de défense et de sécurité. Ses publications n'engagent que leurs auteurs et ne constituent en aucune manière une position officielle du ministère des Armées.



EU CYBER DIRECT
Supporting EU Cyber Diplomacy

INTRODUCTION

Le 9 septembre 2019, le ministère des Armées rendait public un rapport intitulé *Droit international appliqué aux opérations dans le cyberespace*[1]. La France, en tant qu'État, a toujours marqué son attachement au respect du droit international perçu comme moyen d'assurer la paix et la stabilité. Depuis le *Livre blanc sur la défense et la sécurité nationale* de 2013[2], elle a réaffirmé régulièrement son attachement à l'application du droit international et développé publiquement son approche[3], notamment dans la *Revue stratégique de défense et de sécurité nationale* de 2017[4], la *Stratégie internationale de la France pour le numérique* de 2017[5], la *Revue stratégique de cyberdéfense* de 2018[6] et plus récemment avec la présentation de la *Stratégie cyber des armées*[7].

Touchant au cœur des relations internationales, ces principes juridiques s'avèrent essentiels au maintien de la stabilité. Cela est encore plus vrai lorsqu'il s'agit de réguler les actions des États et des autres acteurs dans l'espace numérique devenu un enjeu politique et stratégique marqué par de nombreuses utilisations malveillantes, voire belliqueuses, des technologies de l'information et de la communication. Si les revendications sont rares, les accusations sont nombreuses, ce qui traduit une escalade des conflits dans ce domaine. Le développement de ces technologies représente donc à la fois une chance pour l'humanité mais aussi un enjeu important pour sa sécurité. Dans cette perspective, le droit international offre un cadre et des solutions pour pacifier cet environnement devenu instable.

Il convient néanmoins de s'interroger sur l'interprétation et la mise en œuvre concrète de ce corpus juridique : que peut faire un État si son système de transport, son réseau d'énergie ou toute autre infrastructure critique est mis hors service pendant une période prolongée en raison d'une opération cybernétique ? Quelles réactions doit-il adopter face à d'importantes perturbations de son fonctionnement, des pertes économiques voire, potentiellement, des pertes humaines ? Une réponse militaire serait-elle justifiée ? Ces questions, et bien d'autres encore, découlent des modalités d'application au cyberespace du droit international. Si des réponses spécifiques doivent toujours être apportées au cas par cas à la suite d'une analyse factuelle et juridique approfondie, il est possible de schématiser le processus logique d'application du droit international à une opération cybernétique, de la

1. Ministère des Armées, *Droit international appliqué aux opérations dans le cyberespace*, 2019.
2. Commission du Livre blanc sur la défense et la sécurité nationale, *Livre blanc sur la défense et la sécurité nationale*, La Documentation française, 2013, p. 32.
3. Voir notamment la déclaration sur la cyberdéfense de M. Jean-Yves Le Drian, ministre de la Défense, lors de la visite de la DGA-MI, à Bruz (Ille-et-Vilaine), le 12 décembre 2016.
4. Ministère des Armées, *Revue stratégique de défense et de sécurité nationale*, 2017.
5. Ministère de l'Europe et des Affaires étrangères, *Stratégie internationale de la France pour le numérique*, 2017 ; Présentation de la stratégie internationale de la France pour le numérique par Jean-Yves Le Drian, ministre de l'Europe et des Affaires etrangères, à l'espace thecamp, Aix-en-Provence, 15 décembre 2017.
6. Secrétariat général à la Défense et la Sécurité nationale, *Revue stratégique de cyberdéfense*, 2018 ; publiée sous le titre *Stratégie nationale de la cyberdéfense*, Economica, 2018.
7. Ministère des Armées, *Éléments publics de doctrine militaire de lutte informatique offensive*, 2019 ; ministère des Armées, *Politique ministérielle de lutte informatique défensive*, 2019 ; discours de Florence Parly, ministre des Armées, *Stratégie cyber des Armées*, 18 janvier 2019 ; prise de parole du général d'armée François Lecointre, chef d'état-major des Armées, Séquence communication consacrée au « Cyber militaire », 18 janvier 2019.

détermination de l'identité de son auteur à l'adoption de mesures unilatérales contre l'État ou l'acteur responsable.

Le schéma contenu dans cette note illustre ce processus afin d'aider toute personne intéressée à naviguer parmi les différentes normes du droit international et à comprendre le processus logique de leur application. Il présente la diversité des qualifications juridiques possibles. Il démontre aussi que la qualification d'une opération cybernétique comme recours à la force, voire comme agression armée ouvrant la possibilité pour l'État victime d'invoquer le droit de légitime défense, ne constitue qu'une option parmi d'autres qui reste inapplicable ou inappropriée dans la grande majorité des cas. Le schéma proposé ici se concentre sur le droit international applicable en temps de paix et n'inclut pas le droit des conflits armés. Ce dernier, également appelé droit international humanitaire, prévaut lors d'un affrontement entre deux ou plusieurs États ou mettant aux prises des acteurs non étatiques.

ÉTAPE 1. ATTRIBUTION D'UNE OPÉRATION CYBERNÉTIQUE

En droit international, le processus d'attribution vise à déterminer si l'opération cybernétique peut être attribuée à un État. Plus précisément, il s'agit de déterminer si le comportement de l'individu ou du groupe responsable de l'opération peut être attribué à un État. En d'autres termes, la première étape consiste à identifier le coupable[8].

Aux termes des *Articles sur la responsabilité de l'État pour fait internationalement illicite* adoptés par la Commission du droit international en 2001[9], qui reflètent le droit international coutumier en matière de responsabilité des États, il convient de distinguer deux situations.

Premièrement, un acte ou une omission est imputable à un État s'il est commis par l'un de ses organes (article 4), par des personnes ou entités exerçant des prérogatives de puissance publique (article 5) ou par des organes mis à la disposition de l'État par un autre État (article 6) (étape 1a). Par exemple, les forces armées ou les services de renseignement sont des organes de l'État, par conséquent les opérations cybernétiques conduites par ces entités sont attribuables à l'État. Une société privée de cybersécurité ayant un contrat avec un État pour conduire en son nom des opérations cybernétiques pourrait constituer un exemple d'entité exerçant des éléments d'autorité gouvernementale.

Deuxièmement, le comportement d'un acteur non étatique est imputable à un État s'il est commis sous les instructions, la direction ou le contrôle de cet État (article 8), en cas d'absence ou de carence des autorités officielles de l'État (article 9), par un mouvement insurrectionnel (article 10) ou reconnu et adopté par un État comme étant sien (article 11) (étape 1b). Il est important de noter que dans cette seconde situation, l'attribution à l'État

8. Il convient de distinguer le processus juridique de l'attribution, également appelé imputation, des autres formes d'attribution comme l'attribution publique. L'attribution publique est la décision politique de nommer publiquement l'État ou l'acteur responsable d'une opération cybernétique.

9. Commission du droit international, *Articles sur la responsabilité de l'État pour fait internationalement illicite*, document adopté par la Commission du droit international des Nations unies à sa 53e session en 2001, annexé à la Résolution 56/83 de l'Assemblée générale des Nations unies en date du 12 décembre 2001, corrigé par le document A/56/49 (Vol. I)/Corr.3.

de chaque acte de l'acteur non étatique concerné sera évaluée séparément, par opposition à l'étape 1a dans laquelle tous les actes de l'acteur concerné sont automatiquement attribués à l'État. Un bon exemple d'acte accompli sous les instructions, la direction ou le contrôle d'un État serait le cas d'un État donnant instruction à un groupe de pirates informatiques de mener une attaque par déni de service contre une cible définie.

Toute situation ne rentrant pas dans les catégories mentionnées ci-dessus ne pourra normalement pas être imputée juridiquement à un État.

ÉTAPE 2. ÉVALUER L'ILLICÉITÉ DE L'OPÉRATION CYBERNÉTIQUE

La deuxième étape vise à déterminer si une opération cybernétique attribuée à un État constitue un fait internationalement illicite de cet État (étape 2a). Une telle action est un acte inamical qui n'est pas en soi un acte illicite en droit international. Malgré l'absence d'interdiction générale des opérations cybernétiques, leur mise en œuvre peut mener à une violation de normes spécifiques telles que la souveraineté des États, le principe de non-intervention, les droits de l'homme ou encore l'interdiction de la menace ou de l'emploi de la force (article 2, paragraphe 4, de la Charte des Nations unies). De plus, certains cas de recours à la force peuvent atteindre le seuil de l'agression armée.

L'illicéité d'un comportement qui constituerait normalement une violation d'une obligation internationale de l'État responsable peut être exclue ou atténuée si l'opération est perpétrée dans certaines circonstances particulières : force majeure, détresse, consentement, nécessité, contre-mesures ou légitime défense (étape 2b). En effet, l'opération cybernétique peut elle-même constituer une réaction à un acte illicite antérieur, qui peut ne pas être de nature numérique, et donc être justifiée comme une contre-mesure, voire dans les cas les plus extrêmes comme l'exercice du droit de légitime défense.

Par ailleurs, dans certains cas, même si une opération cybernétique n'est pas attribuée à un État, la responsabilité de cet État peut être engagée suivant l'obligation de diligence qui lui incombe (étape 2c). Ce principe impose aux États l'obligation de ne pas permettre que leur territoire soit utilisé pour le lancement ou le transit d'opérations cybernétiques visant un autre État. L'obligation de diligence est une obligation de moyen et non de résultat. Un État verra sa responsabilité engagée non pas parce qu'il n'a pas obtenu le résultat escompté, c'est-à-dire la cessation de l'opération cybernétique dans la plupart des cas, mais parce qu'il a manifestement omis de prendre les mesures nécessaires et réalisables pour mettre un terme à l'acte en cause alors qu'il était tenu de le faire. Ainsi, un État qui ne prend aucune mesure pour atténuer les effets d'une opération cybernétique provenant de son territoire peut être tenu pour responsable en vertu du droit international, non pas de l'acte en lui-même mais du fait de ne pas avoir adopté les mesures nécessaires. L'attribution de l'acte n'a pas d'importance ; l'opération cybernétique peut être perpétrée par un État ou un acteur non étatique. Dans cette perspective, l'obligation de diligence peut constituer un palliatif intéressant au problème de l'attribution.

ÉTAPE 3. RESPONSABILITÉ DE L'ÉTAT

L'État lésé par une opération cybernétique d'un autre État peut être en droit d'invoquer la responsabilité de l'État responsable et de demander la réparation du préjudice et des éventuels dommages subis. Plusieurs obligations pèsent alors sur l'État responsable, notamment une obligation de cessation et de non-répétition de l'acte illicite, ainsi qu'une obligation de réparation intégrale du préjudice causé.

L'État responsable a l'obligation de réparer intégralement le préjudice et les éventuels dommages résultant d'un fait internationalement illicite. Cette réparation peut prendre trois formes :

1. La restitution (rétablissement de la situation qui existait avant que le fait illicite ne soit commis, par exemple en restituant un objet saisi) ;
2. L'indemnisation (paiement d'une somme) lorsque le préjudice causé n'est pas réparable intégralement par la restitution ;
3. La satisfaction (prenant généralement la forme d'excuses, d'expression de regret ou de reconnaissance de la violation) lorsque le préjudice causé n'est pas réparable intégralement par le biais de la restitution et de l'indemnisation.

Prenons l'exemple d'une opération cybernétique menée par un État contre le système bancaire d'un autre. Cette opération prendrait vraisemblablement la forme d'un programme informatique malveillant infectant les systèmes informatiques des banques de l'État visé en vue de causer des pertes économiques importantes. La pénétration des systèmes informatiques sur le territoire d'un autre État constituerait une violation de sa souveraineté territoriale. Il découlerait de cette situation plusieurs obligations pour l'État responsable. Premièrement, si l'opération cybernétique a un caractère continu, c'est-à-dire que le programme malveillant continue à opérer, l'État responsable a l'obligation d'y mettre fin. En d'autres termes, il a l'obligation de cesser son acte internationalement illicite ayant un caractère continu. Deuxièmement, il se doit de ne pas répéter le comportement fautif, et d'offrir des assurances et garanties en ce sens. Troisièmement, il est dans l'obligation de réparer le préjudice et les dommages subis. Dans le cas présent, la restitution n'étant pas envisageable, l'État responsable devra indemniser les pertes financières.

ÉTAPE 4. RÉPONSES DISPONIBLES POUR L'ÉTAT VICTIME

Le droit international impose aux États l'obligation de régler leurs différends internationaux par des moyens pacifiques. Plusieurs options s'offrent à l'État victime. Il peut notamment décider de saisir le Conseil de sécurité des Nations unies ou de soumettre le différend à une juridiction internationale, comme la Cour internationale de Justice par exemple.

Toutefois, cette solution n'est pas toujours possible, le droit international étant dépourvu de mécanisme judiciaire centralisé. Pour cette raison, les États victimes d'une opération cybernétique peuvent adopter des mesures unilatérales extrajudiciaires dans le but de contraindre l'État fautif à respecter ses obligations en mettant un terme à l'attaque

et en réparant le préjudice subi sous certaines conditions. Trois modes opératoires sont ici envisageables : le droit de légitime défense, les contre-mesures et les mesures de rétorsion (étape 4a).

La légitime défense ne pourra être invoquée qu'en réaction à une opération cybernétique atteignant le seuil de l'agression armée. Les mesures prises alors pourront être de nature numérique ou non. Il n'existe pas de définition universelle de l'agression armée ni de son interprétation au regard des opérations cybernétiques[10]. Néanmoins, il est généralement admis qu'une opération cybernétique causant des dommages physiques, des blessures ou la mort et atteignant un certain seuil d'intensité, pourrait atteindre le seuil de l'agression armée ouvrant la possibilité pour l'État victime d'invoquer le droit de légitime défense. Il convient de souligner ici que la très grande majorité des opérations cybernétiques n'atteint pas le seuil de l'agression armée et, qu'à ce jour, aucun État n'a invoqué son droit de légitime défense. Dans de tels cas, il faudra alors se tourner vers d'autres formes de mesures unilatérales.

En réaction à une opération cybernétique constituant un acte internationalement illicite, l'État victime peut adopter des contre-mesures, de nature numérique ou non. Les contre-mesures sont des actions ou des omissions de l'État victime à l'encontre de l'État responsable constituant normalement un acte internationalement illicite, mais dont l'illicéité est exclue car elles sont adoptées en réaction à un acte internationalement illicite. À titre d'exemple, il serait possible pour l'État victime d'une opération cybernétique violant sa souveraineté territoriale de mener une action similaire à l'encontre de l'État responsable. Dans ce cas, l'opération constituera une contre-mesure et sera licite. Les contre-mesures sont la forme principale de mesures unilatérales qu'un État peut adopter en réaction à une opération cybernétique internationalement illicite.

Les mesures de rétorsion sont la troisième forme de mesures unilatérales. Il s'agit de mesures licites mais inamicales, comme par exemple l'expulsion de diplomates de l'État visé.

Finalement, il convient de noter que, dans certaines circonstances, les mesures prises par un État qui ne seraient pas justifiées en tant que contre-mesures ou mesures de légitime défense en réaction à une opération cybernétique, pourraient voir leur illicéité exclue ou atténuée par certaines circonstances telles que la force majeure, la détresse, le consentement ou la nécessité (étape 4b). Le scénario le plus probable 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.

10. L'article 51 de la Charte des Nations unies précise que le droit de légitime défense peut être invoqué en réaction à une agression armée, sans en donner une définition : « Aucune disposition de la présente Charte ne porte atteinte au droit naturel de légitime défense, individuelle ou collective, dans le cas où un Membre des Nations unies est l'objet d'une agression armée, jusqu'à ce que le Conseil de sécurité ait pris les mesures nécessaires pour maintenir la paix et la sécurité internationales. Les mesures prises par des Membres dans l'exercice de ce droit de légitime défense sont immédiatement portées à la connaissance du Conseil de sécurité et n'affectent en rien le pouvoir et le devoir qu'a le Conseil, en vertu de la présente Charte, d'agir à tout moment de la manière qu'il juge nécessaire pour maintenir ou rétablir la paix et la sécurité internationales. »

CONCLUSION

Le présent schéma expose le processus logique de l'application du droit international à une opération cybernétique. Il permet de mettre en lumière, à la fois, la diversité des qualifications juridiques possibles, ainsi que celle des formes de réactions que pourrait mettre en œuvre l'État victime.

Cette note est une version traduite et revue d'une publication en anglais réalisée dans le cadre du projet européen EU Cyber Direct[11] *: François Delerue,* International Law in Cyberspace Matters: This Is How and Why, *EU Cyber Direct, Policy in Focus, 2019.*

François Delerue est chercheur en cyberdéfense et droit international à l'IRSEM et enseignant à Sciences Po Paris. Il est également rapporteur pour le droit international de l'*Academic Advisory Board* du projet EU Cyber Direct. Il mène des recherches sur les questions de cyberdéfense et de cybersécurité sous l'angle juridique, stratégique et politique. Il s'intéresse tout particulièrement au droit international, aux normes et à la coopération internationale, ainsi qu'aux différents types d'acteurs impliqués (États, entreprises privées, organisations non gouvernementales, etc.). Plus généralement, il s'intéresse à l'impact des nouvelles technologies (conquête spatiale, robotique, intelligence artificielle, etc.) sur le droit international et les relations internationales. Son ouvrage intitulé *Cyber Operations and International Law* paraîtra chez Cambridge University Press (Cambridge Studies in International and Comparative Law) en janvier 2020.

Contact : françois.delerue@irsem.fr

11. Le projet EU Cyber Direct réunit des responsables gouvernementaux, des chercheurs et d'autres acteurs pour explorer les principales questions entourant l'application du droit international existant dans le cyberespace, les normes de comportement responsable des États, les mesures de confiance et les efforts pour renforcer la résilience des États et de la société dans le cyberespace. Le projet est financé par l'Union européenne dans le cadre de l'instrument de coopération numérique internationale : confiance et sécurité dans le cyberespace.