Sous la direction de
MARYLINE GRANGE
ANNE-THIDA NORODOM

CYBERATTAQUES
et droit international

Problèmes choisis

Préface de
Frédérick DOUZET

Editions A. PEDONE

NUMERIQUE ET DROIT

Sous la direction de
MARYLINE GRANGE
ANNE-THIDA NORODOM

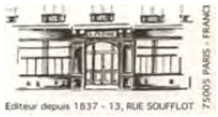
CYBERATTAQUES ET DROIT INTERNATIONAL

PROBLÈMES CHOISIS

EDITIONS PEDONE

Les contributions réunies dans cet ouvrage sont issues du colloque organisé le 2 juin 2017 à l'Université de Rouen, avec le soutien du Centre universitaire rouennais d'études juridiques (CUREJ), de l'Institut de Recherche Inter-disciplinaire Homme Société, l'Université de Rouen, l'UFR de droit, sciences économiques et gestion de l'Université de Rouen et le Centre de recherches critiques sur le droit (CERCRID).

Cette publication a été financée par le Centre universitaire rouennais d'études juridiques.



13 rue Soufflot
75005 PARIS
2018

I.S.B.N. 978-2-233-00902-9

LISTE DES CONTRIBUTEURS

Philippe ACHILLEAS, *université Paris-Sud*

Anne-Laure CHAUMETTE, *université Paris Nanterre, CEDIN*

Olivier CORTEN, *université Libre de Bruxelles, Centre de droit international*

Claire CRÉPET-DAIGREMONT, *université Panthéon-Assas (Paris II)*

François DELERUE, *Institut de recherche stratégique de l'Ecole militaire (IRSEM)*

Mathias FORTEAU, *université Paris Nanterre, CEDIN*

Maryline GRANGE, *université de Lyon, UJM-Saint-Etienne, CERCRID UMR 5137*

Patrick JACOB, *université Versailles-Saint-Quentin (Paris-Saclay)*

Anne-Thida NORODOM, *université Paris Descartes, Centre Maurice Hauriou*

Serge SUR, *université Panthéon-Assas (Paris II)*

PRÉFACE

Le 12 novembre 2018, le président de la République française Emmanuel Macron lançait « l'Appel de Paris[1] pour la confiance et la sécurité dans le cyberespace » lors du Forum mondial de la gouvernance de l'Internet à l'UNESCO à Paris. Ce vibrant plaidoyer pour « un cyberespace ouvert, sûr, stable, accessible et pacifique » affichait dès son lancement le soutien d'une cinquantaine d'Etats et de centaines d'entreprises et d'institutions privées, publiques et académiques. La paix, la sécurité et la stabilité du cyberespace étaient également au cœur des discussions du Forum de la Paix de Paris, qui se tenait en même temps à l'occasion du centenaire de l'armistice de la Première Guerre Mondiale, et de la semaine numérique de Paris. La semaine précédente, la Première Commission de l'Assemblée générale des Nations unies votait deux projets de résolutions, depuis adoptés par l'Assemblée Générale, pour relancer les discussions multilatérales visant à réguler le comportement des Etats dans le cyberespace. Ces enjeux faisaient aussi l'objet, au même moment, d'une vaste opération de diplomatie commerciale orchestrée par l'entreprise Microsoft, avec le lancement d'une pétition pour la « paix numérique » (Digital Peace Now)[2], ainsi que des travaux publiés à cette occasion par la Global Commission on the Stability of Cyberspace (GCSC). Ce groupe international d'experts issus de la société civile, des gouvernements, des secteurs privés, techniques et académiques proposait une série de normes de comportement responsable afin de limiter les pratiques déstabilisatrices menées par les Etats et les acteurs privés dans le cyberespace.

En l'espace d'une décennie, le cyberespace est ainsi devenu un enjeu majeur des relations diplomatiques et un nouvel objet du droit international. Les questions de paix et de régulation internationales sont devenues étroitement liées aux questions numériques, alors que la conflictualité s'est propagée dans le cyberspace, désormais qualifié d'enjeu stratégique majeur, de terrain d'affrontement voire, pour de nombreux Etats, de nouveau domaine militaire. Pendant des années, les Etats ont agi en grande impunité dans l'espace numérique, profitant de son opacité pour mener des opérations

[1] L'appel de Paris pour la confiance et la sécurité dans le cyberspace <https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/diplomatie-numerique/la-france-et-la-cybersecurite/article/cybersecurite-appel-de-paris-du-12-novembre-2018-pour-la-confiance-et-la>

[2] Voir la campagne de Microsoft <https://digitalpeace.microsoft.com>

offensives en toute discrétion. Mais la prolifération des attaques, de plus en plus dangereuses, ciblées et sophistiquées leur a fait prendre conscience de leur propre vulnérabilité et notamment des risques d'atteinte aux infrastructures d'importance vitale, de déstabilisation massive ou d'escalade des conflits. Au-delà de la paix et la sécurité internationales, l'enjeu est aussi la stabilité même du cyberespace, dont la mise à mal pourrait avoir des conséquences catastrophiques en raison de la dépendance croissante de nos sociétés au numérique. La régulation et la coopération internationale sont ainsi devenues indispensables pour assurer la sécurité collective face aux menaces et aux risques que représentent les cyberattaques.

Le droit international se trouve dès lors pleinement mobilisé pour répondre à ces nouveaux défis sécuritaires et, de fait, au cœur des discussions diplomatiques. Et pourtant cela n'allait pas de soi, pour des raisons moins juridiques que géopolitiques. Il a fallu attendre 2013 pour que les Etats s'entendent sur l'applicabilité du droit international au cyberespace, permettant ainsi de sortir de la représentation d'un vide juridique dans lequel se développeraient les opérations numériques. La première avancée majeure fut en effet le rapport du Groupe des Experts Gouvernementaux de l'ONU (UNGGE) de 2013, adopté par les experts des 20 pays participant − dont les Etats-Unis, la France, la Chine et la Russie −, qui reconnaît explicitement l'applicabilité du droit international au cyberespace. Or la question des modalités d'application de ce droit restait entière. Dans quelle mesure le droit international est-il suffisant pour répondre aux défis propres à l'espace numérique ? Comment préciser ou compléter le droit international pour répondre à ces difficultés spécifiques, en tenant compte de l'évolution rapide et incessante de la technologie et des concepts d'attaques ?

L'attribution représente par exemple un défi majeur. Les cyberattaques sont en effet très difficiles − certains disent impossibles − à attribuer avec certitude, tant il est facile de masquer ses traces et son identité dans le cyberespace. Les acteurs sont multiples car la technologie est facilement accessible et à faible coût, les liens entre les individus, les criminels, les mercenaires et les Etats sont souvent complexes à établir. L'intention d'une attaque peut être tout aussi difficile à caractériser. Les effets d'une cyberattaque sont souvent incertains et dépendent largement de la configuration de la cible, la proportionnalité de la réponse peut s'en trouver tout aussi incertaine. Enfin les outils et les concepts d'attaque développés par les Etats peuvent être volés, récupérés et réutilisés, ce qui soulève des questions de responsabilité.

Les travaux du GGE se sont concentrés sur l'adoption de normes non contraignantes, de principes et de mesures de confiance, qui permettent d'aboutir à une vision commune sur ce qui constitue un comportement

responsable des Etats dans le cyberspace. Quelles que soient leurs limites, ces normes permettent d'améliorer la prévisibilité du comportement des Etats et préparent le terrain juridique et politique − loin d'être mûr − pour l'interprétation du droit international positif et l'adoption de nouvelles obligations contraignantes. Le rapport du GGE de 2015 a ainsi permis d'établir un consensus sur le fait que les Etats ne doivent pas laisser leur territoire être sciemment utilisé pour mener des attaques informatiques, ou encore causer de dommages intentionnels aux infrastructures d'importance vitale ni aux centres de réponse d'urgence (CERTs). Les Etats se sont engagés à échanger de l'information et se prêter assistance, renforcer la coopération pour la sécurité et la stabilité du cyberespace, et limiter la prolifération de vulnérabilités et logiciels malveillants, et notamment d'assurer l'intégrité de la chaîne d'approvisionnement. Or en 2017, les négociations du GGE ont achoppé justement sur des points d'interprétation du droit international dans un contexte de forte défiance politique, échouant ainsi à produire un consensus.

Cet ouvrage, centré sur l'application du droit international aux cyberattaques, ouvre une discussion indispensable entre les spécialistes du droit international et les praticiens, mais aussi entre deux disciplines complémentaires, le droit et la géopolitique. Le consensus autour de l'application du droit international aux cyberattaques se construit en effet dans un contexte géopolitique et n'échappe pas aux rivalités de pouvoir entre Etats qui peinent à surmonter la défiance liée à leurs différences de capacités, leurs rapports de force et leurs représentations géopolitiques. Ces Etats, pourtant préoccupés du risque systémique engendré par la prolifération des attaques, ne sont pas prêts à renoncer à certaines pratiques offensives qui participent de leur puissance mais mettent en péril la sécurité et la stabilité du cyberespace.

L'intérêt de cet ouvrage est d'explorer la richesse du droit international, en puisant dans d'autres domaines déjà existants, pour faire face aux cyberattaques. Car révolution technologique ne veut pas nécessairement dire révolution juridique et, comme le rappellent les auteurs dès l'introduction, il n'est pas question de faire table rase du passé. Bien au contraire, dans un contexte de fortes tensions géopolitiques, rappeler les fondements du droit international, la coutume, les principes déjà acquis, et montrer comment ils peuvent s'appliquer à de nouveaux types de conflits offre une base solide sur laquelle construire plus efficacement un consensus pour la régulation de la conflictualité dans l'espace numérique. Cette exploration est d'autant plus nécessaire que les défis futurs s'annoncent importants, alors que la numérisation massive de nos sociétés contribue à accroître l'imbrication complexe des enjeux civils, militaires et économiques et pose la question de la responsabilité des Etats.

Les attaques WannaCry et NotPetya en sont emblématiques. La propagation incontrôlée rapide et massive de ces logiciels malveillants à l'échelle mondiale en 2017 a provoqué de lourds dégâts au sein d'entreprises et même d'hôpitaux britanniques qui n'avaient pas initialement été pris pour cibles. Or ces attaques, initialement présentées comme criminelles, seraient d'origine étatique. Le Royaume-Uni et les Etats-Unis accusent la Corée du Nord pour WannaCry alors qu'une coalition d'Etats tient la Russie responsable de NotPetya. Enfin ces deux attaques ont été conduites avec le même outil, EternalBlue, initialement développé par la National Security Agency (NSA) à partir d'une vulnérabilité sur le système de Microsoft puis volé et mis à disposition sur Internet. Ces circonstances interrogent sur la part de responsabilité, au-delà des attaquants, des différents acteurs. Et surtout, la qualification de l'attaque en acte de guerre est venue d'un assureur, qui refusait d'indemniser son client pour les dégâts occasionnés.

Il ne fait nul doute que les réflexions entamées dans cet ouvrage seront amenées à se poursuivre. L'évolution de la conflictualité dans le cyberespace n'a de limites que la créativité et l'ingéniosité des attaquants. L'avènement de nouvelles technologies de rupture comme l'ordinateur quantique ou encore les développements rapides de l'intelligence artificielle ne manqueront pas de fournir matière à discussion entre les spécialistes du droit international de la cybersécurité et de la géopolitique.

Frédérick DOUZET,

Professeure à l'Institut Français de Géopolitique (Paris 8),
directrice du centre Géopolitique de la Datasphère (GEODE)

TABLE DES MATIÈRES

SECONDE SOUS-PARTIE :
ACTIONS ENTREPRISES PAR LES ETATS, VICTIMES DE CYBERATTAQUES

PROPOS CONCLUSIFS

NUMERIQUE ET DROIT

Un nord-coréen accusé d'avoir piraté le studio Sony ou orchestré l'attaque Wannacry pour le compte du régime, des interventions via les réseaux sociaux dans les campagnes électorales américaine, lettone ou française, un programme malveillant paralysant la cérémonie d'ouverture des derniers Jeux Olympiques, une tentative de perturbation de missions d'avion de chasse, une attaque de sociétés gérant le fonctionnement de centrales nucléaires américaines… la liste pourrait être longue pour recenser les cyberattaques entreprises seulement depuis 2017.

Pourtant, la réponse à apporter n'est toujours pas évidente : qui peut agir ? contre qui ? à quelles conditions et dans quel but ? Autant de questions qui se posent et auxquelles il faut apporter une réponse à la suite de l'identification de tels actes. S'il a été reconnu que le droit international existant doit s'appliquer en cas de cyberattaques, il reste encore à en identifier les modalités.

C'est à cet ambitieux objectif que la Journée d'études organisée à l'université de Rouen le 2 juin 2017 entendait contribuer en confrontant les besoins des praticiens aux réflexions d'universitaires. Le présent ouvrage rassemble les contributions des intervenants qui ont accepté de proposer des analyses, souvent prospectives, des questions posées quant à la définition des cyberattaques, l'identification de leurs auteurs et des réactions envisageables.

Ont contribué Philippe ACHILLEAS, Anne-Laure CHAUMETTE, Olivier CORTEN, Claire CREPET-DAIGREMONT, François DELERUE, Mathias FORTEAU, Maryline GRANGE, Patrick JACOB, Anne-Thida NORODOM, Serge SUR.

GEODE

Ouvrage publié avec le soutien du CUREJ CUREJ

CYBERATTAQUES ET DROIT INTERNATIONAL

Commande aux Editions A. PEDONE - 13 Rue Soufflot - 75005 PARIS, ou par télécopie: +33 (0)1.46.34.07.60 et sur editions-pedone@orange.fr - **30 € l'ouvrage, nous consulter pour un envoi par la poste.**

Le montant peut être envoyé par :

❏ Chèque bancaire
❏ Règlement sur facture

❏ Carte Visa

N°...../...../...../.....

Référence : ISBN 978-2-233-00902-9

Cryptogramme .....

Date de validité.....

Signature :

Nom.....

Adresse.....

Ville ..... Pays.....