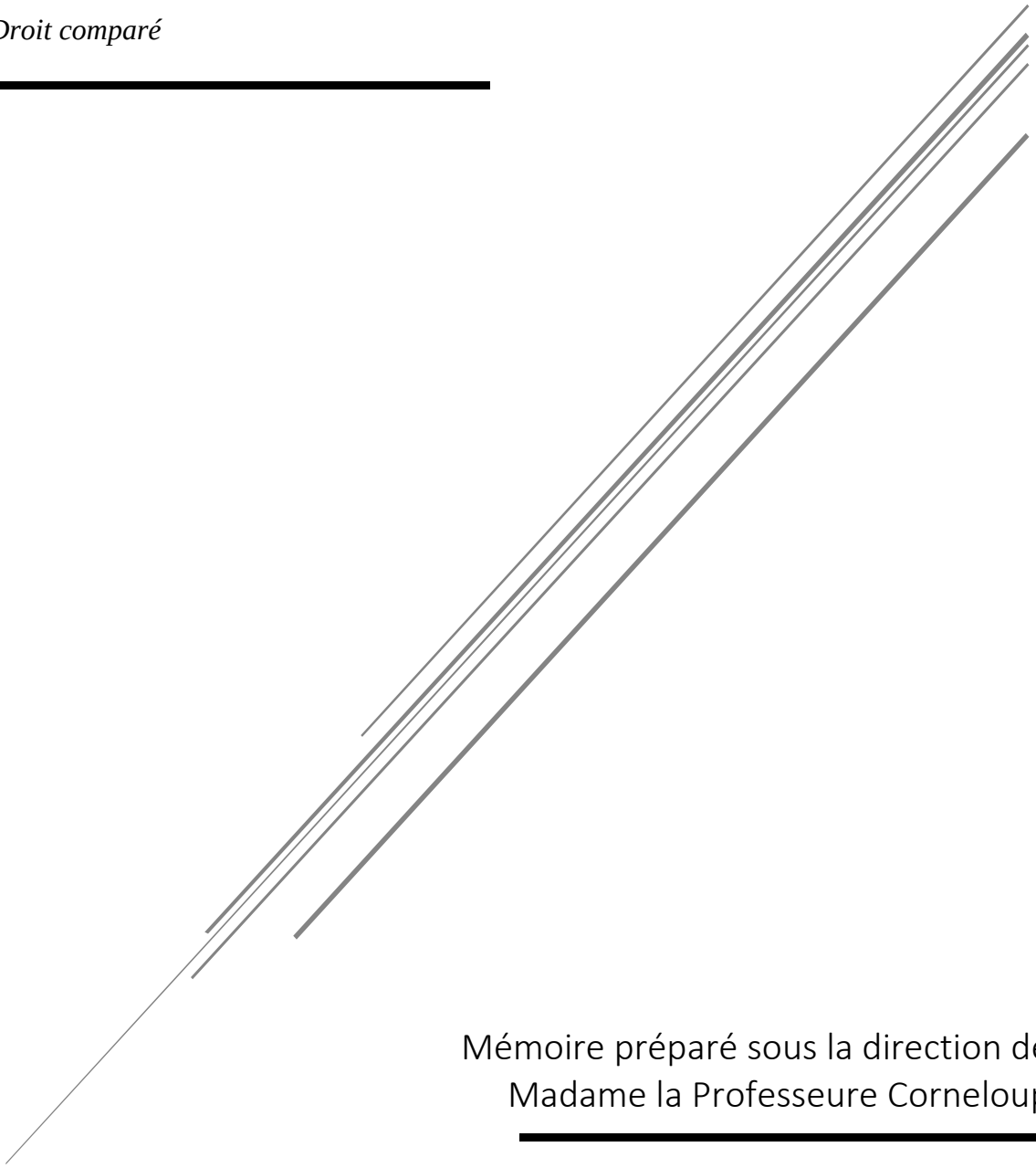
L'APPLICATION DU DROIT INTERNATIONAL DANS LE CYBERESPACE

Université Paris II Panthéon Assas

Année Universitaire 2018-2019

Master 2 Droit comparé



Mémoire préparé sous la direction de
Madame la Professeure Corneloup

Camille Rabussier

Sommaire

Résumé

La révolution numérique et l'usage de plus en plus répandu des ordinateurs et d'Internet pose la question de la régulation d'un nouveau domaine, le cyberespace. Comme l'espace terrestre, maritime, aérien ou spatial, celui-ci peut faire l'objet d'opérations hostiles entre les États mais également de la part de groupes non-étatiques qui ont également accès à cet espace et peuvent y mener des attaques. La dépendance aux systèmes et réseaux informatiques de nombreuses infrastructures vitales dans les domaines de l'énergie, de la santé, des transports ou encore des télécommunications fait désormais de ces dernières des cibles privilégiées.

A ce jour, il n'existe aucun traité ou corps de règles dictant aux États la conduite à adopter dans le cyberespace. Pour autant, il n'est pas possible d'en conclure qu'il s'agit d'un espace de non-droit : le droit international s'y applique.

Il reste que le droit international général est constitué de règles parfois vagues, rédigées à une autre époque et pour adresser des problèmes différents. L'objet de ce mémoire est de s'interroger sur l'interprétation à donner au droit international dans son application au cyberespace, mais également de voir si celui-ci est anachronique et doit être remplacé par des règles spécifiques pour régir ce nouveau domaine.

Dans un premier temps, ce travail analysera dans quels cas les opérations offensives menées dans le cyberespace – les cyberattaques – sont licites ou illicites. Dans un second temps, il s'intéressera aux moyens à disposition des États victimes pour se défendre dans le cyberespace. Différentes problématiques seront abordées, notamment l'usage de la force dans le cyberespace, le lien entre souveraineté et cyberespace, les questions d'attribution des cyberattaques, le rôle et la responsabilité des groupes non-étatiques ou enfin la légitime défense dans le cyberespace.

Enfin, ce mémoire esquissera certaines pistes de développement pour le droit international du cyberespace, une branche qui n'en est encore qu'à ces balbutiements mais qui se développera avec certitude.

Remerciements

Je tiens à remercier Madame la Professeure Corneloup pour avoir accepté de diriger ce mémoire et m'avoir permis d'aborder ce sujet qui me tenait à cœur.

Je tiens également à remercier l'ensemble de mes professeurs à l'Université Paris II Panthéon Assas ainsi qu'à la Humboldt Universität zu Berlin pour leur engagement et leur enseignement de qualité.

Enfin, je remercie ma famille et mes amis pour leur soutien et leurs conseils tout au long de la rédaction de ce travail.

Introduction

Le 13 juin 2019, alors qu'une vague de protestations secoue Hong-Kong, à l'occasion de l'examen d'un projet de loi visant à autoriser l'extradition vers la Chine, le fondateur de Telegram, une application de messagerie sécurisée en ligne, a rapporté que l'application avait été victime d'une cyberattaque importante opérée par déni de service distribués. Les attaques, provenant massivement de Chine, ont perturbé le réseau utilisé par les manifestants pour communiquer et organiser le mouvement de protestation[1].

La cyberattaque a visé une application de messagerie afin d'influer sur un mouvement de contestation, mais l'on sait aujourd'hui que des attaques peuvent viser toutes sortes de cibles comme des sites gouvernementaux ou de médias, les systèmes informatiques d'hôpitaux, d'infrastructures de transport voire de sites de production industrielle ou nucléaire. Nos sociétés modernes sont de plus en plus dépendantes des réseaux et systèmes informatiques, ce qui en fait des cibles privilégiées pour qui cherche à en perturber le bon fonctionnement.

Si jusqu'à présent, aucune cyberattaque n'a joué un rôle majeur dans le cadre d'un conflit ou causé des dégâts graves à un Etat, la dépendance de nombreux pays aux infrastructures informatiques et la vulnérabilité de certains systèmes rendent l'hypothèse de cyberattaques de large ampleur de plus en plus plausible. Les conséquences de telles attaques, loin d'être limitées au monde virtuel, peuvent être importantes et impacter de façon dramatique un Etat et sa population. Ainsi, on peut entendre dire que les prochains conflits entre Etats ne seront plus seulement physiques, mais auront lieu dans le cyberespace : c'est ce que certains appellent la « cyberguerre ».

Les termes de « cyberguerre », « cyberattaque », « cyber-offensive », etc. renvoient à des situations de conflit, lesquelles sont régies par le droit international, en particulier le *jus ad bellum* et le *jus in bello*, respectivement les règles relatives à l'engagement dans une guerre, et les règles régissant la conduite de la guerre. Pourtant, à bien des égards, les opérations menées

[1] The New York Times, Chinese Cyberattack Hits Telegram, App Used by Hong Kong Protesters, consulté le 15 juin 2019.

dans le cyberespace diffèrent des opérations de guerre « traditionnelles ». Cela amène à la question de savoir si le droit international s'applique dans le cyberespace et comment.

Dans un premier temps, il est nécessaire de définir avec précision ce que constitue le cyberespace, ce que sont les cyberattaques, et de comprendre par quels moyens techniques elles sont mises en œuvre. Suivront quelques exemples d'attaques ayant eu lieu ces dernières années et ayant parfois été qualifiées d'actes de « cyberguerre ».

Il faut également examiner dans quel cas les cyberattaques sont licites en droit international, ou plutôt, dans quel cas elles ne le sont pas. Il convient enfin de voir quelles réponses un Etat victime d'une cyberattaque peut adopter et quels mécanismes peuvent être développés à l'avenir afin d'établir un cadre juridique plus stable dans le cyberespace.

1. Terminologie

Le terme de « cyber-guerre », ou dans la littérature anglophone « *cyberwarfare* » est largement utilisé, notamment dans les médias, pour décrire des phénomènes bien différents, qui n'ont pourtant pas grand-chose à voir avec la « guerre » comme on l'entend au sens classique du droit international. L'on rencontre également souvent les termes de « guerre d'information » ou « guerre informatique » (*information warfare*), de « cyberattaque » ou « d'attaque informatique » (*cyberattack*) ou encore de « cybercrime ». Néanmoins, on peine encore aujourd'hui à trouver une définition uniforme et commune de ces termes.

Un dénominateur commun de ces différents concepts est néanmoins le terme « cyber ». Ce dernier renvoie aux nouvelles technologies de l'information, aux ordinateurs, à la « réalité virtuelle » ou encore à Internet. Les cyber-attaques, la cyber-guerre ou encore le cybercrime prennent place dans ce que l'on a coutume d'appeler le « cyberespace » (*cyberspace*).

Le cyberespace peut être décrit comme un réseau global et interconnecté d'informations, d'infrastructures de communication, incluant Internet, les réseaux de télécommunication, les systèmes informatiques et les informations qui s'y trouvent[2].

[2] N. Melzer, "Cyberwarfare and international Law", *UNIDIR*, 2011, p. 4 ; voir aussi la définition de l'ANSSI (Agence nationale de la sécurité des systèmes d'information) : « espace de communication constitué par l'interconnexion mondiale d'équipements de traitement automatisé de données numériques ».

Le cyberespace repose ainsi sur des composantes physiques (telles que les infrastructures) et non-physiques (comme les informations et données contenues dans ces infrastructures). En cela, le cyberespace se distingue des quatre domaines traditionnels régulés par le droit international que sont l'espace terrestre, maritime, aérien et spatial. Lorsque l'on dit de quelque chose qu'elle réside dans le cyberespace, cela signifie en réalité qu'elle réside physiquement dans un ordinateur, un système d'information ou qu'elle transite par une infrastructure de télécommunication[3]. Une autre caractéristique importante et différentiant le cyberespace des autres domaines, est qu'il s'agit d'un domaine créé par l'homme, qui n'existe pas à l'état « naturel »[4].

Le cyberespace, tout comme l'espace terrestre, maritime, aérien et spatial, peut être le théâtre de nombreuses opérations, nommées « opérations informatiques » ou « cyber-opérations ». Ce vocable englobe à la fois des opérations offensives et défensives. On peut garder en mémoire la définition adoptée par le Manuel de Tallinn[5], qui définit une cyber-opération comme « l'emploi de capacités cybernétiques dans le but primaire d'atteindre des objectifs dans ou au moyen du cyberespace »[6].

Une typologie issue de la stratégie nationale militaire des Etats-Unis pour les cyber-opérations (*United States National Military Strategy for Cyberspace Operations*), englobe dans les opérations informatiques (*computer network operations – CNO*) (1) les attaques informatiques (*computer network attacks – CNA*) ; (2) la défense informatique (*computer network defence – CND*) ; (3) l'exploitation informatique (*computer network exploitation – CNE*). L'exploitation informatique, contrairement aux attaques, se concentre sur la collection de renseignement et

[3] W.G. Sharp, "Cyberspace and the Use of Force", *Ageis Research Corp.*, 1999, p. 15.
[4] H. Todd, « Armed attack in Cyberspace: deterring asymmetric warfare with an asymmetric definition", *Air Force Law Review*, Vol. 64, 2009, p. 68.
[5] Le Manuel de Tallinn relatif à l'application du droit international à la cyberguerre (*Tallinn Manual on the International Law applicable to Cyberwarfare*) est une étude académique, juridiquement non-contraignante, rédigée par un « Groupe international d'experts » à l'invitation du CCDCOE de l'OTAN (*Cooperative Cyber Defence Centre of Excellence*) et publiée en 2013. Il représente une des études les plus complètes sur l'application du droit international aux cyber-opérations.
Une deuxième version enrichie a été publiée en 2017, le Manuel de Tallinn 2.0. relatif à l'application du droit international aux cyber-opérations (*Tallinn Manual on the International Law applicable to Cyber Operations*).
[6] Tallinn Manual, Glossary.

l'observation, plutôt que sur la perturbation ou la destruction des réseaux adverses[7]. L'exploitation peut notamment viser à répandre une information dans un but de propagande, à voler des informations sensibles, des mots de passe, ou des secrets commerciaux, sans que l'utilisateur du réseau ou système informatique n'en ait connaissance. En cela, la cyber-exploitation correspond à une forme moderne d'espionnage. Bien que l'espionnage soit considéré comme illégal dans la plupart des Etats, il n'est pas en tant que tel prohibé par le droit international[8].

Les cyber-attaques et les opérations de cyberdéfense sont des cyber-opérations qui vont au-delà de la simple exploitation et qui sont accompagnées par une intention hostile. L'objet de ces opérations est de perturber ou de détruire des informations contenues dans des systèmes et réseaux informatiques ou de neutraliser la maîtrise adverse de ses réseaux et systèmes. Le terme de cyberattaque englobe à la fois des opérations de faible ampleur, tel que le cybercrime, le cyberterrorisme, mais encore des opérations aux conséquences plus-graves, que certains appellent des opérations de « cyber-guerre ».

Certains auteurs ajoutent également que la cyberattaque doit être le fait d'un Etat ou conduite par des agents ou entités dont les actions sont attribuables à un Etat. Si ce critère est courant en droit international, il n'est néanmoins pas fidèle à la réalité du cyberespace dans lequel évoluent aussi bien des acteurs étatiques et non-étatiques.

Une classification intéressante des attaques informatiques a été établie par le *Center for Security Studies* (CSS) de Zurich, distinguant les différentes formes d'attaque par ordre d'importance croissante. On trouve ainsi au premier niveau le « cyberhacktivisme » ou « cybervandalisme » qui consiste en la perturbation ou destruction des systèmes informatiques dans un but idéologique. Cela recouvre par exemple les actions menées par des groupes comme Anonymous. On trouve ensuite le cybercrime, qui cible principalement les milieux d'affaires et dont la finalité est le gain financier. Au troisième niveau, on trouve le cyberterrorisme, qui est le fait d'acteurs non-étatiques cherchant à faire accepter à un Etat ou un groupe d'Etats leurs

[7] M. Roscini, « World wide warfare - *jus ad bellum* and the use of electronic force*", Max Planck Yearbook of United Nations Law, Vol. 14*, 2010, p. 7.
[8] M. Gervais, "Cyberattacks and the law of war", *Berkeley Journal of International Law*, Vol. 30, 2012, p. 533.

revendications. Enfin, on trouve les actes de « cyberguerre », le cas le plus grave, mettant en jeu la sécurité d'un Etat ou ses intérêts stratégiques.

Sera exclu du champ de cette étude le « cybercrime ». Le cybercrime est une des seules notions qui bénéficie d'une définition, certes non universelle, mais acceptée par de nombreux Etats, signataires de la Convention de Budapest. Cette convention adoptée sous l'égide du Conseil de l'Europe en 2001 et entrée en vigueur en 2004, vise à renforcer la coopération entre les Etats dans la lutte contre la cybercriminalité. Elle impose notamment aux Etats d'ériger en infraction pénale « le fait intentionnel et sans droit, d'endommager, d'effacer, de détériorer, d'altérer ou de supprimer des données informatiques » ainsi que « l'entrave grave, intentionnelle et sans droit, au fonctionnement d'un système informatique, par l'introduction, la transmission, l'endommagement, l'effacement, la détérioration, l'altération ou la suppression de données informatiques »[9]. Le cybercrime recouvre ainsi la fraude sur internet, le piratage d'œuvres audio-visuelles, l'usurpation d'identité, etc. Le terme de « cybercrime » dans la Convention repose sur une acception plus large que celle proposée par le CSS, en ce qu'il enveloppe aussi le cyberhacktivisme. Bien que le cybercrime fasse l'objet d'une convention internationale, il n'a pas vocation à être régi par les règles relatives à l'usage de la force ou aux conflits armés, mais bien par les différents systèmes domestiques des Etats.

Ce mémoire s'intéressera donc aux formes les plus graves de cyberattaques que certains appellent, sûrement un peu abusivement, des actes de « cyberguerre ». Ces attaques sont menées par des Etats ou des groupes organisés, dans le cadre d'un conflit armé ou non. On peut les définir comme des opérations coordonnées menées au travers du cyberespace, au moyen de systèmes d'information et de communication, perturbant le fonctionnement ou détruisant des systèmes et réseaux informatiques, pouvant menacer la prospérité, la sécurité et la stabilité des Etats.

Par commodité, le terme de « cyberattaque » sera employé, dans un sens restreint, qui n'englobe pas le cybercrime. De plus, le champ de cette étude visera seulement les opérations dites « *cyber-to-cyber* », c'est-à-dire des opérations menées par des outils et systèmes informatiques

[9] Articles 4 et 5 de la Convention sur la Cybercriminalité du Conseil de l'Europe (CETS No.185).

et visant des systèmes et réseaux informatiques. Sont ainsi exclues les opérations cinétiques[10] visant ces mêmes systèmes, par exemple une frappe aérienne visant à détruire des systèmes de contrôle.

2. Application des règles existantes

L'interprétation des règles de droit international dans le cadre du contexte cyber suppose avant tout que ces règles soient applicables. Bien qu'il n'existe pas de convention ou de règles relatives spécifiquement au cyberespace, cela ne signifie pas pour autant que le cyberespace soit une zone de « non-droit », dans lequel règne un vide juridique et où aucune règle ne s'applique.

Le groupe d'experts intergouvernemental des Nations Unies (*UN Governmental Group of Experts – GGE*), mis en place sur la base d'une résolution de l'Assemblée Générale en 2003[11] a été chargé d'examiner les risques qui se posent ou pourraient se poser dans le cyberspace et d'éventuelles mesures de coopération pour y faire face. Un premier rapport a été publié en 2010 puis un second rapport plus détaillé a été publié en 2013 et adopté par une résolution de l'Assemblée Générale[12]. Dans ce rapport, le groupe a notamment décrété que « le droit international - et en particulier la Charte des Nations Unies - est applicable et qu'il est essentiel au maintien de la paix et à la stabilité dans l'espace international ainsi qu'à la promotion d'un environnement des technologies de l'information et de la communication ouvert, sûr, pacifique et accessible »[13]. Le rapport ne contient toutefois pas plus de détails.

Il sera complété par un troisième rapport rendu en 2015[14] dans lequel la Charte est envisagée comme le cadre essentiel dans lequel les actions des Etats dans le cyberespace prennent place. Puisque la Charte doit s'appliquer aux technologies de l'information et de la communication, les Etats doivent également respecter les grands principes qu'elle contient dans le cyberespace. Le groupe intergouvernemental d'experts identifie différents principes que les Etats se sont engagés à respecter comme étant « d'importance centrale »[15]. Il s'agit de l'égalité souveraine

[10] Le terme « cinétique » est issu du terme anglais « *kinetic* », employé dans le contexte militaire pour caractériser les moyens conventionnels de combat militaire à savoir des armes à énergie cinétique utilisant la force physique générée à l'impact pour détruire une cible.
[11] A/RES/58/32.
[12] A/68/98.
[13] A/68/98, §19; "International law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment".
[14] A/70/174
[15] A/70/174, §26.

des Etats, du règlement des différends par des moyens pacifiques, du respect des droits de l'homme et des libertés fondamentales, du renoncement à la menace et à l'usage de la force contre l'intégrité territoriale ou l'indépendance politique de tout Etat ou de toute autre manière incompatible avec les objectifs des Nations Unies ainsi que du principe de non-intervention dans les affaires internes des autres Etats.

En amont de leur travail sur les règles applicables au cyberespace, les experts rédacteurs du Manuel de Tallinn ont unanimement considéré que les règles du *jus ad bellum* et du *jus in bello* s'appliquent dans le cyberespace[16]. Cette même conclusion a été adoptée par une grande partie des Etats, notamment les Etats-Unis[17], mais aussi la France[18], le Royaume-Uni[19] ou l'Allemagne[20].

Ce consensus est renforcé par l'affirmation de la Cour internationale de Justice (CIJ) dans son avis consultatif sur la *Licéité de la menace ou de l'emploi d'armes nucléaires* selon laquelle les règles du *jus ad bellum* « s'appliquent à n'importe quel emploi de la force, indépendamment des armes employées »[21].

Dire que le droit international s'applique aux cyberattaques ne répond pas à la question de savoir *comment*. Ainsi que le souligne le Comité international de la Croix-Rouge (CICR)[22], l'application de règles préexistantes à une nouvelle technologie soulève la question de savoir si ces règles sont suffisamment claires pour s'adapter aux spécificités de cette nouvelle technique.

Avant d'analyser comment le droit international s'applique dans le cyberespace, les développements qui suivent s'attachent à comprendre comment sont menées les cyber-opérations sous un angle technique et offrent quelques exemples de cyber-attaques ayant eu lieu ces dernières années.

[16] Tallinn Manual, p. 5.
[17] White House, International Strategy for Cyberspace, May 2011, p. 9.
[18] Stratégie nationale de la cyberdéfense, parue le 29 juin 2018, p. 82.
[19] Foreign and Commonwealth Office, Response to General Assembly resolution 69/28 "Developments in the field of information and telecommunications in the context of international security", May 2015, p. 6.
[20] Voir par exemple la réponse de l'Allemagne, '"Report on Developments in the Field of Information and Telecommunications in the Context of International Security" (RES 69/28)'.
[21] Licéité de la menace ou de l'emploi d'armes nucléaires, avis consultatif, C.I.J. Recueil 1996, p. 226, §39.
[22] ICRC, International humanitarian law and the challenges of contemporary armed conflicts

3. Aspects techniques des cyberattaques

Sans viser à entrer dans les détails techniques des cyber-opérations, il peut être intéressant de voir comment celles-ci sont menées, quelles ressources sont nécessaires, afin de saisir tous les enjeux qu'elles posent, mais aussi parce qu'un régime différent est susceptible de s'appliquer.

Pour résumer de façon simple, il existe deux types de techniques pour perturber ou détruire des systèmes et réseaux informatiques à l'aide de moyens cyber : les attaques visant à interrompre ou perturber le fonctionnement d'un système et les attaques dites d'intrusion. Les premières s'opèrent principalement à l'aide d'attaques par déni de services, tandis que les secondes reposent sur l'usage de logiciels malicieux ou *malwares*.

T. Rid prend la métaphore d'un spectre pour classer les cyber-opérations, lesquelles vont des attaques génériques, mais peu destructrices (comme les dénis de service) à des attaques spécifiques voire unique, mais à fort potentiel destructeur[23].

3.1. Dénis de service et dénis de service distribués

Le but d'une attaque par déni de service est de saturer la bande passante ou les capacités d'une cible informatique en la bombardant de requêtes afin de ralentir ou de bloquer le trafic. La cible victime des requêtes est incapable d'y répondre en raison de leur nombre trop élevé et ne peut fonctionner normalement.

Un utilisateur unique ne peut causer énormément de dommages grâce à ce type d'attaques. C'est pourquoi généralement, les agresseurs ont recours à des attaques par déni de service distribués. La technique est la même, simplement, l'agresseur a recours à un « *botnet* », c'est-à-dire un réseau de machines infectées contrôlées à distance par l'agresseur et qui effectuent des attaques coordonnées par déni de service contre une même cible, souvent à l'insu du propriétaire de l'ordinateur. Cela permet de démultiplier l'effet de l'attaque, en augmentant le nombre de requêtes envoyées vers la cible. Les machines sont infectées de différentes manières par des individus ou groupes malveillants (« les maîtres ») via des virus contractés à l'ouverture de courriers électroniques (spams) ou lors de téléchargements effectués sur Internet. Certains experts informatiques soulignent d'ailleurs que le nombre de machines infectées est susceptible d'augmenter, notamment en raison de l'utilisation de plus en plus répandue d'objets connectés.

[23] T. Rid, "Cyber War Will Not Take Place", *Oxford University Press*, 2013, p. 165.

Cette technique présente l'avantage d'être facilement accessible, de requérir peu de capacités techniques et de ressources financières. Elle reste toutefois peu « élaborée » : les conséquences d'une attaque par déni de service sont immédiates – par exemple un site est rendu inaccessible durant toute la durée d'une attaque – mais cessent lorsque l'attaque prend fin.

3.2. Les logiciels malveillants ou « *malware* »

Les logiciels malveillants comme *Stuxnet,* sont des programmes qui prennent avantage d'une vulnérabilité dans le code d'un autre logiciel (comme Microsoft Word ou Java) ou un système d'exploitation (comme Windows). Cette vulnérabilité va être exploitée par l'attaquant afin d'introduire le logiciel malveillant dans un ordinateur ou un réseau. Le malware est capable de se propager de manière autonome, d'infecter d'autres ordinateurs, etc. Il peut également permettre à l'attaquant de prendre le contrôle de l'ordinateur infecté et d'avoir accès aux fichiers qui s'y trouvent.

La forme la plus courante du logiciel malveillant est le virus, un programme qui va supprimer ou endommager les fichiers d'un ordinateur ou réseau informatique. Le virus, comme son nom l'indique, à la capacité de « s'attacher » à un fichier (« l'hôte) et de se propager à d'autres ordinateurs et systèmes en se dupliquant. Les virus ont l'avantage de la discrétion, puisqu'ils n'empêchent pas le fonctionnement normal des machines qu'ils infectent et ne sont destructeurs que si l'utilisateur ouvre le fichier ou programme hôte auquel le virus s'est attaché.

Parfois confondu avec le virus, le ver fonctionne de façon similaire en se répandant d'un ordinateur à l'autre. Toutefois, le ver est capable d'infecter différents ordinateurs et machines et de se dupliquer seul, il n'a pas besoin d'un programme ou fichier hôte auquel s'attacher. Les vers se « nourrissent » des différentes ressources de l'ordinateur, notamment de la mémoire ; mais utilisent également de la bande passante réseau, ce qui peut causer le ralentissement des machines infectées et des réseaux.

Enfin, les « bombes logiques » sont un genre avancé de logiciel programmé pour se déclencher uniquement lors de la survenance d'un évènement prédéterminé. Une bombe logique peut ainsi « dormir » dans un ordinateur ou système informatique durant des mois voire des années, à

l'insu du propriétaire de la cible. Cependant, une fois déclenchée, les effets peuvent potentiellement être dévastateurs.

Il faut toutefois noter qu'une fois que le logiciel malveillant est découvert, il perd de son efficacité puisque la vulnérabilité exploitée va être corrigée. Ainsi, les malwares sont généralement utilisés de façon ponctuelle. Plus les conséquences prévues et infligées sont importantes, plus l'attaque est visible et plus il est probable que les vulnérabilités utilisées deviennent publiques et soient corrigées rapidement.

Les capacités sont infinies et certains logiciels particulièrement sophistiqués tels que *Stuxnet,* présenté ci-après, peuvent par exemple aller jusqu'à permettre à l'attaquant de prendre le contrôle d'un système informatique gérant les centrifugeuses d'un site de production nucléaire. Afin de mieux comprendre le potentiel des cyberattaques et les dégâts qu'elles peuvent commettre, le paragraphe suivant revient sur trois cyberattaques de grande ampleur.

4. Exemples de cyberattaques

Les premières cyberattaques importantes que l'on peut recenser se sont déroulées à la fin des années 90, dans le cadre du conflit en Yougoslavie. Les alliés de l'OTAN décident de mener une campagne de bombardements aériens en Serbie, l'opération « Force alliées ». En représailles, des hackers serbes décident d'attaquer les sites internet et serveurs de messagerie de la coalition. Certains resteront inaccessibles durant plusieurs jours[24]. Si les conséquences de ces premières attaques restent mineures, il en va autrement des attaques qui ont visé l'Estonie et la Géorgie, ou encore du virus *Stuxnet.*

4.1. Les cyberattaques contre l'Estonie

Les 26 et 27 avril 2007, des manifestations de grande ampleur éclatent à Tallinn, capitale de l'Estonie, à la suite de la décision du gouvernement de retirer un mémorial de l'ère soviétique post-seconde guerre mondiale. Celui-ci avait été érigé en 1947 pour célébrer la victoire de l'armée soviétique face à l'Allemagne nazie. Malgré les critiques émises par le gouvernement

[24] M. Baud, « La cyberguerre n'aura pas lieu, mais il faut s'y préparer », *IFRI – politique étrangère*, 2012/2, p. 309.

russe au sujet de cette décision, le mémorial est retiré. S'ensuivent des protestations menées par des groupes majoritairement issues d'ethnies russes. Les manifestations s'étendent à d'autres villes du pays, et même jusqu'à l'ambassade d'Estonie à Moscou. Finalement, ces manifestations physiques vont se muer en manifestations informatiques, avec une première vague de cyber-attaques visant des pages internet d'institutions gouvernementales estoniennes et de médias nationaux.

Cette première vague d'attaques se déroule du 27 au 29 avril. D'intensité modérée et constituée d'actes relativement isolés, les attaques sont opérées par déni de service et déni de service distribués, dans le but de rendre les sites visés inaccessibles.

En revanche, une seconde phase d'attaques débuta le 30 avril, et se poursuivit jusqu'au 18 mai. Cette seconde vague est caractérisée par des attaques de plus grandes ampleur, coordonnées et plus sophistiquées. Des attaques massives par déni de service distribués sont lancées contre des sites clés du gouvernement estonien et des sites d'acteurs privés, notamment des médias, des banques et autres grandes entreprises du pays. Sont également visés les réseaux téléphoniques des services de secours. Toutefois, les infrastructures critiques de transport ou d'énergie n'ont pas été prises pour cible.

Si les techniques utilisées, principalement les attaques par déni de service distribuées, ne sont pas particulièrement sophistiquées, elles ont été mises en œuvre, en particulier durant la seconde phase, d'une manière coordonnée, simultanée et à une échelle jusqu'alors jamais vue.

Il faut savoir que dès 2007, l'Estonie était un des pays les mieux connectés du monde et repose largement sur Internet pour son développement économique et son administration. Cela fait de l'Estonie un pays particulièrement vulnérable à des cyber-attaques menées à grande échelle. Ainsi, il a été rapporté qu'à l'époque des faits, 95% du territoire était relié à Internet et que, par exemple, 99% de citoyens estoniens utilisaient Internet pour avoir accès à des services bancaires[25]. La dépendance de ce pays à Internet en fait une cible privilégiée, et les attaques dirigées contre le pays n'auraient pas nécessairement eu le même impact dans un pays moins connecté.

[25] S. Li, "When does internet denial trigger the right to self-defence", *Yale Journal of International Law, Vol. 38,* 2013, p. 200.

Les effets de ces cyber-attaques ont été principalement économiques. Même si les sites visés étaient principalement ceux du gouvernement, du parlement ou de grandes banques et entreprises, cela a également impacté de petites et moyennes entreprises. Si les dommages directs sont difficiles à estimer, on estime l'impact économique négatif entre 27,5 et 40,5 millions de dollars. Comparé au poids économique de l'Estonie, l'on estime que ces attaques ont eu un effet comparable à un blocus économique imposé lors d'un conflit armé de forte intensité[26].

Au-delà des effets économiques, les citoyens estoniens ont été coupés de différents services mais surtout, ne pouvaient pas consulter un grand nombre de médias nationaux, ceux-ci ayant également été pris pour cible. Les attaques ont empêché le pays de communiquer sur la situation à travers le monde, forçant ainsi les autorités estoniennes à recourir à des moyens alternatifs pour échanger des informations avec le monde extérieur. Finalement, une parade a été trouvée en dupliquant les sites visés sur l'hébergeur américain Blogger.

En raison du contexte politique dans lequel elles sont survenues, et de la proximité avec la décision du gouvernement estonien de retirer le mémorial soviétique, les regards se sont d'abord tournés vers la Russie, représentant un coupable à première vue évident. La Russie a toujours dénié être impliquée dans ces attaques, quand bien même les enquêtes qui ont suivi ont montré qu'une grande partie d'entre elles avaient été lancées depuis ou via la Russie et que différents sites internet en langue russe proposaient des logiciels en libre accès permettant de conduire les attaques par déni de service. Toutefois, comme on le verra au long de cette étude, le fait qu'une cyber-opération transite ou soit lancée depuis un pays ne signifie en rien que ce dernier soit à l'origine de l'attaque. En effet, une des caractéristiques principales des cyber-opérations est qu'elles ne connaissent pas de frontières. De plus, il est très facile de masquer ses traces et d'utiliser une adresse IP masquée ou de la faire transiter par un autre pays.

A ce jour, seule une personne, d'ethnie russe, vivant en Estonie, a été condamnée pour avoir visé le site internet du parti au pouvoir durant les cyber-incidents de 2007. Aucune preuve n'a pu être apportée quant à la participation du gouvernement russe à ces opérations, de façon directe ou indirecte. Le groupe Nashi, composé de jeunes militants russes, a plus tard déclaré être derrière les attaques tout en affirmant avoir agi indépendamment du gouvernement russe.

[26] *Ibid,* p. 201.

4.2. Les cyberattaques contre la Géorgie

Peu de temps après les cyberattaques ayant frappé l'Estonie, c'est au tour de la Géorgie de faire l'expérience d'attaques informatiques, toutefois dans un contexte différent.

En août 2008, un conflit éclate entre la fédération de Russie et la Géorgie concernant l'Ossétie du Sud, une région disputée entre les deux Etats. La région est *de facto* autonome depuis le conflit de 1991 entre l'Ossétie et la Géorgie, mais elle demeure *de jure* une région appartenant au territoire géorgien, et est reconnue comme telle par la communauté internationale. Malgré un cessez-le-feu et de nombreux efforts pour résoudre le conflit, celui-ci demeure irrésolu[27].

Une opération de maintien de la paix fût mise en place après le conflit de 1991 sous mandat de l'OSCE (Organisation pour la sécurité et la coopération en Europe) mais en pratique, les différentes troupes russes et géorgiennes ne parvinrent pas à coopérer, et les tensions demeurèrent vives entre d'une part la Géorgie, et de l'autre les séparatistes, majoritairement soutenus par la Russie. Le 7 août 2008, à la suite de provocations de la part des séparatistes d'Ossétie, le gouvernement géorgien décida de lancer une attaque contre ces derniers. Le lendemain, la Russie engagea des opérations militaires sur le sol géorgien, déclarées par la Géorgie comme une agression contraire au droit international.

Avant même le lancement des opérations militaires de la Russie, les premières attaques contre des sites du gouvernement géorgien furent enregistrées. Il s'agit de la première fois qu'un conflit international est accompagné voire précédé par une cyber offensive coordonnée.

Les attaques constituent principalement des opérations de défacement de sites internet et des attaques par déni de service distribuées, des méthodes similaires à celles utilisées contre l'Estonie quelques mois plus tôt. Toutefois, à la différence des attaques ayant visé l'Estonie, les rapports et enquêtes ultérieurs démontrent que les attaques étaient, dès leur lancement, coordonnées.

Preuve de cette coordination, différents blogs, forums et sites internet russes ont permis de diffuser un script ainsi que certains fichiers aisément téléchargeables donnant des instructions de sites à prendre pour cible et mettant à disposition des ressources pour conduire des attaques de type déni de service. Etaient notamment identifiés comme cibles privilégiées les sites des

[27] CCDCOE, "Cyber-attacks against Georgia: Legal Lessons identified", p. 4.

ambassades américaines et du Royaume-Uni à Tbilissi, le Parlement, la Cour suprême, le Ministère des affaires étrangères géorgien et différents sites de médias nationaux.

Tout comme dans le cas des attaques visant l'Estonie, il n'y a pas de preuve permettant de savoir qui était derrière les cyber-opérations menées à l'encontre de la Géorgie, même si les médias ont largement pointé la Russie du doigt. En revanche, des hackers russes étaient impliqués, même si leur lien avec l'administration et le gouvernement russe ne sont pas prouvés. Dans le cas de la Géorgie, la Russie a également toujours démenti être à l'origine des offensives.

En revanche, les effets de ces attaques, du point de vue du droit international, peuvent être vus comme plus importants que ceux causés par les attaques en Estonie. En effet, si là aussi, des sites gouvernementaux ont été rendus indisponibles, les conséquences étaient exacerbées du fait du conflit armé qui se déroulait en parallèle avec la Russie. Durant cette période, le gouvernement géorgien avait un intérêt crucial à pouvoir diffuser des informations à destination de la population et de la communauté internationale. Le gouvernement géorgien a été empêché de communiquer sur le conflit en cours et les citoyens géorgiens privés d'informations de première importance.

Même si la société géorgienne était à l'époque des attaques moins bien reliée à Internet que l'Estonie, ces opérations ont démontré que même une société peu dépendante à Internet et aux systèmes informatiques peut souffrir, en particulier en termes d'accès à l'information.

Les effets économiques en revanche sont plus durs à estimer, dans la mesure où les attaques ont eu lieu parallèlement à un conflit armé.

4.3. Le virus Stuxnet

Deux ans après les attaques ayant touché la Géorgie, le virus *Stuxnet* a été découvert en 2010 par une compagnie spécialisée dans la sécurité informatique. Il s'agit d'un logiciel malicieux, particulièrement sophistiqué, capable d'espionner et de reprogrammer des systèmes industriels, et même d'en prendre le contrôle tout en camouflant les modifications qu'il y apporte. Le ver a affecté différents systèmes informatiques spécifiques mais la plupart des experts ayant enquêté

sur *Stuxnet* en a conclu que la cible principale étaient des sites de production nucléaire iraniens, en particulier des sites d'enrichissement d'uranium situés près de la ville de Natanz.

Le logiciel, répandu par clé USB, a été conçu pour accélérer et ralentir de façon anormale le fonctionnement des centrifugeuses dans le but de causer des vibrations pouvant les endommager ou les détruire. Si le logiciel n'a pas réussi à causer des dommages catastrophiques, l'on estime néanmoins qu'il a ralenti le processus d'enrichissement d'uranium des centrales. Des analyses ultérieures ont montré que le programme avait été intentionnellement limité et qu'il aurait pu, si ses créateurs l'avaient voulu, causer des dommages bien plus importants.

Stuxnet a été décrit dans les médias et par les experts comme étant l'arme cyber la plus sophistiquée jamais créée. C'est la première fois que l'on détecte un ver capable d'espionner et de reproduire des systèmes industriels aussi bien protégés, mais surtout, le logiciel avait la capacité d'opérer de façon camouflée et aurait pu se développer encore des mois durant avant d'être découvert. Bien que l'Iran ait dans un premier temps dénié avoir été touché par une cyberattaque, le gouvernement a depuis admis que l'attaque avait eu lieu et qu'elle avait eu un effet important sur le programme nucléaire mené par le pays.

De plus, l'agence internationale de l'énergie atomique a rapporté que les centrifugeuses de Natanz ont cessé l'enrichissement d'uranium durant une semaine entière, fin novembre 2009, ce qui semble représenter une défaillance majeure du site. D'après les expertises menées, le virus *Stuxnet* aurait ralenti de 23% les opérations d'enrichissement d'uranium sur une période d'environ 12 mois. Il ne s'agit que d'estimations, et étant donné le caractère hautement stratégique de la cible de *Stuxnet*, il est peu probable d'obtenir des chiffres certains. Néanmoins, on peut affirmer que les autorités iraniennes ont été prises de cours par cette attaque technologiquement avancée qui a surpassé leurs systèmes de protection. Bien que les dommages aient été limités et réparés relativement rapidement, *Stuxnet* a montré qu'une cyberattaque sophistiquée peut infliger des dommages importants et sur le long terme, notamment à des infrastructures dites « critiques ».

Etant donné la technologie mise en œuvre pour atteindre des systèmes hautement protégés, les experts ont unanimement déclaré qu'il ne peut s'agir de l'œuvre d'une personne isolée, en ce que le développement du logiciel nécessite des ressources que seul un Etat a les moyens de

mettre à disposition. Bien que rien ne soit officiellement confirmé, de nombreuses sources ont indiqué que *Stuxnet* serait l'œuvre de la coopération des Etats-Unis et d'Israël.

Pour résumer, le virus *Stuxnet* a finalement montré l'intérêt que peut avoir la conduite d'une opération cyber dans le but de toucher des objectifs sensibles, difficilement atteignables par des opérations cinétiques, mais également la tendance à une multiplication de ces attaques, qu'il est extrêmement compliqué d'attribuer à un responsable avec certitude.

Ces exemples constituent à ce jour ce que la plupart des experts considère comme étant les trois cyberattaques les plus graves ayant touché des Etats. Dans les trois cas, les conséquences sont finalement demeurées relativement minimes, soit en raison des techniques employées (les attaques par déni de service) ; soit parce que le logiciel déployé n'avait pas pour but de causer des dommages physiques.

Néanmoins, les différents experts et gouvernements prennent au sérieux différents scenarii qu'il est techniquement possible de mettre en œuvre. Des attaques par déni de service peuvent, si elles sont déployées à grande échelle, causer la disruption des systèmes téléphoniques, empêchant par exemple la réception des appels pour les services de secours, ambulances, pompiers, etc. Les réseaux d'un gouvernement ou de médias peuvent être saturés, empêchant la diffusion d'informations via ces réseaux. L'hypothèse d'une « *infoblockade* » ou blocus de l'information est également envisageable par ce biais. Enfin, une attaque pourrait viser des banques ou la bourse d'un Etat, entraînant la panique du secteur financier.

Stuxnet est à ce jour un des logiciels les plus sophistiqués capable de causer des dommages de grande ampleur. Certains Etats ou groupes disposent aujourd'hui des capacités cyber pour développer un logiciel semblable, capable d'infiltrer des systèmes et réseaux informatiques utilisés pour gérer des infrastructures telles que des barrages, des réseaux électriques, des systèmes d'aiguillage de trains ou de contrôle aérien. Ainsi, par exemple, en 2007, lors d'une frappe aérienne menée par l'armée israélienne sur des sites de production nucléaire en Syrie, une cyberattaque menée en amont a permis de compromettre les systèmes aériens de défense de la Syrie. La méthode employée reste inconnue, mais il semble qu'Israël ait été capable de nourrir de fausses informations les radars syriens, les rendant « aveugles »[28].

L'hypothèse de cyber-attaques causant des dommages physiques voire des morts ne relève plus de la science-fiction, ce qui fait dire à de nombreuses personnes – spécialistes des technologies

[28] O.A. Hathaway/ R. Crootof, "The Law of Cyber-Attack", *California Law Review, Vol. 100*, 2012, p. 838.

de l'information, juristes, militaires ou personnalités politiques – que la menace cyber est le risque le plus sérieux qui pèse sur la sécurité des Etats et la paix internationale.

Cette introduction a permis de définir avec plus de clarté ce que constitue le cyberespace, ce que sont les cyberattaques et d'affirmer que les règles du droit international, issues de traités ou de la coutume, s'appliquent dans le cyberspace. Il reste maintenant à savoir comment ces règles s'appliquent.

Dans un premier temps, il convient d'analyser dans quel cas une cyber-opération peut être licite en droit international. Seront notamment abordés les principes relatifs à la prohibition de l'usage de la force et de la non-intervention. Dans un second temps, il faut s'intéresser aux réponses qui peuvent être apportées par l'Etat victime d'une cyber-attaque.

Première partie - L'illicéité des cyber-attaques au regard du droit international

Nous avons vu dans l'introduction que le cyberespace et les cyberattaques n'échappent pas à l'application du droit international. Le droit international « définit les responsabilités juridiques des États dans leurs relations les uns avec les autres et les rapports que peuvent avoir ces États avec les individus qui vivent sur leur territoire » [29]. Il est constitué de différentes conventions internationales, du droit international coutumier ainsi que des principes généraux de droit international[30]. Pilier du droit international, la Charte des Nations Unies codifie les grands principes des relations internationales, notamment du *jus ad bellum*, c'est-à-dire les règles relatives à la licéité de l'emploi de la force, et est applicable au cyberespace. Elle est complétée par d'autres traités qui contiennent des règles relatives à la licéité des actes des Etats en droit international ainsi que les règles du droit international coutumier.

Cette première partie cherche à examiner dans quels cas les cyberattaques sont licites en droit international, ou plutôt, dans quel cas elles ne le sont pas. En effet, l'on considère généralement que le droit international est prohibitif par nature, c'est-à-dire que ce qu'il n'interdit pas doit être considéré comme permis[31].

La plupart de la littérature s'est intéressé à la relation entre les cyberattaques et le principe de prohibition de la force contenu dans l'article 2(4) de la Charte des Nations Unies ainsi qu'au concept d'agression armée. Une attaque qui constitue un usage de la force ou une agression armée est illicite en droit international. Néanmoins, des cyberattaques moins graves peuvent également constituer des actes illicites au regard du droit international, soit parce qu'elles violent le principe de non-intervention, soit plus généralement au regard de la souveraineté des Etats.

[29] https://www.un.org/fr/sections/what-we-do/uphold-international-law/
[30] Article 38 du Statut de la Cour internationale de Justice.
[31] Affaire du Lotus, Publications de la Cour permanente de Justice Internationale, série A, n°10, p. 18 ; Kosovo, §84.

Chapitre 1 : Les cyber-attaques comme violation du principe de prohibition de l'usage de la force

L'article 2(4) de la Charte des Nations Unies est une des dispositions les plus importantes de ce traité, et *a fortiori,* du droit international. Il dispose que

> *« Les Membres de l'Organisation s'abstiennent, dans leurs relations internationales, de recourir à la menace ou à l'emploi de la force, soit contre l'intégrité territoriale ou l'indépendance politique de tout État, soit de toute autre manière incompatible avec les buts des Nations Unies ».*

Ainsi que l'a rappelé la Cour internationale de justice dans l'affaire des Activités militaires et paramilitaires au Nicaragua, ce principe a également acquis une valeur coutumière.

Puisque ce principe trouve à s'appliquer également dans le cyberespace, il convient d'analyser si une cyber-opération peut constituer un usage de la force tel que prohibé par l'article 2(4).

I. La notion de force en droit international

La notion de force utilisée par l'article 2(4) n'est pas définie dans la Charte et à ce jour, il n'existe pas d'interprétation unanime de ce que recouvre la notion de « force » dans la communauté internationale. Il faut donc interpréter ce terme.

Dans le cadre de l'interprétation d'une disposition d'un traité, il peut être intéressant de se référer à la Convention de Vienne sur le droit des Traités de 1969, qui donne dans ses articles 31 à 33 des règles d'interprétation. Bien que la Convention ne soit pas universellement ratifiée et qu'elle soit entrée en vigueur postérieurement à l'adoption de la Charte des Nations Unies, il est généralement admis en droit international que la plupart des dispositions de ce traité ont acquis une valeur coutumière, notamment les articles relatifs aux règles d'interprétation.

L'article 31 de la Convention de Vienne propose une règle générale selon laquelle les traités doivent être interprétés « suivant le sens ordinaire à attribuer aux termes du traité dans leur contexte et à la lumière de son objet et de son but ».

Le dictionnaire propose différentes définitions du mot « force ». Il peut s'agir de l'usage de « moyens violents, contrainte exercée pour obtenir un résultat » mais aussi du « pouvoir, puissance, ascendant, supériorité de quelqu'un, d'un groupe »[32].

Dans le contexte du droit international, la même tension se fait sentir quant à l'interprétation à donner au terme de « force ». Relativement large, il peut englober à la fois la force par les armes, mais également la force économique ou d'autres mesures contraignantes. Puisque l'étendue de ce que recouvre le terme « force » ne peut être définie avec certitude, il faut observer comment le terme est employé dans le traité et prendre en compte son objet et son but.

Si l'on observe la Charte dans son ensemble, le terme « force » est employé dans d'autres dispositions. Il se trouve tout d'abord dans le Préambule, qui pose pour objectif aux Etats d'éviter qu'il ne soit fait usage de la « force des armes ». L'article 41 de la Charte parle quant à lui de force « armée ». Se pose alors la question de savoir si le terme « force » de l'article 2(4) doit être compris comme dans le Préambule et l'article 41 et renvoyer à la force « armée », ou si, au contraire, l'absence du terme « armé » implique d'envisager le terme « force » dans l'article 2(4) de façon plus large, comme comprenant également le recours à la contrainte politique ou économique par exemple.

Il existe principalement deux interprétations opposées. La première se base sur une interprétation littérale des termes de l'article 2(4). Les rédacteurs de la Charte ont intentionnellement choisi de ne pas parler de force « armée » dans l'article 2(4) afin de donner à la prohibition de l'usage de la force un champ d'application plus large. Si les rédacteurs avaient voulu seulement se référer à l'usage de la force militaire, l'article 2(4) aurait contenu l'adjectif « armé ».

La seconde interprétation se base sur une approche plus systémique et soutient que l'article 2(4) doit être compris comme se référant à l'usage de la force armée. La septième clause du Préambule de la Charte énonce que « il ne sera pas fait usage de la force des armes, sauf dans l'intérêt commun ». Le Préambule vise à introduire les dispositions que contient le corps de la

[32] Dictionnaire Larousse.

Charte, et ses clauses sont formulées de façon large. Ainsi, pour les supporters d'une interprétation restrictive de l'article 2(4), les termes utilisés dans le Préambule doivent nécessairement être interprétés de façon plus large que les termes contenus dans les dispositions qui constituent le corps du traité. Comme le souligne Schmitt, les dispositions de la Charte sont conçues pour effectuer les aspirations du préambule[33]. Puisque le Préambule se réfère explicitement à l'usage de la force des armes, l'article 2(4) ne saurait être interprété plus largement et inclure la contrainte économique ou politique.

On peut également noter l'argument d'Albrecht Randelzhofer qui souligne que si l'article 2(4) visait également à prohiber la contrainte économique ou politique, il ne resterait plus aucun moyen licite pour les Etats d'exercer une pression sur un autre Etat se conduisant en violation avec le droit international[34].

Malgré ces arguments, la règle d'interprétation générale posée dans l'article 31 de la Convention de Vienne est insuffisante pour trancher entre l'interprétation extensive et l'interprétation restrictive. Il convient donc d'avoir recours aux instruments complémentaires d'interprétation proposés dans l'article 32 de la Convention de Vienne. Il s'agit des travaux préparatoires et « des circonstances dans lesquelles le traité a été conclu ».

Lors de la conférence de San Francisco en 1945 durant laquelle a été rédigée la Charte, certains Etats ont proposé que soit inclus dans le texte la contrainte économique comme un usage de la force, mais cela ne fut finalement pas entériné. De nouveau, en 1970, lors des négociations portant sur la rédaction de la résolution de l'Assemblée Générale des Nations Unies sur les relations amicales et la coopération entre les États[35], la question ressurgit de savoir si le terme « force » englobe toutes formes de pressions, y compris celles à caractère économique ou politique, qui ont pour effet de menacer l'intégrité territoriale ou l'indépendance politique d'un Etat. Il y fût finalement répondu de façon négative et la contrainte économique a été incluse dans le principe de non-intervention.

[33] M. Schmitt, « Computer network attacks and the use of force in international law: Thoughts on a normative framework", *Columbia Journal of Transnational Law, Vol. 37*, 1999, p. 904.
[34] Nolte/Randelzhofer, « The Charter of the United Nations: a Commentary", Vol. II (3rd edition), Article 2(4), p. 118.
[35] Résolution 26/25 (XXV) de l'Assemblée générale relative aux principes du droit international touchant les relations amicales et la coopération entre Etats conformément à la Charte des Nations Unies du 24 octobre 1970.

Ainsi, même si la « force » au sens de l'article 2(4) n'est pas précisément définie, elle n'englobe pas la contrainte économique et politique. Malgré une certaine proximité, les frontières du terme de « force » dans l'article 2(4) ne coïncident pas exactement avec celles du terme « agression armée » de l'article 51 de la Charte, ou, exprimé de façon différente, le terme de « force » dans l'article 2(4) mérite une interprétation large[36]. Ainsi, la Cour internationale de Justice, dans l'arrêt sur les *Activités militaires et paramilitaires au Nicaragua,* a énoncé que l'entraînement, la fourniture d'armes ou toute autre forme de soutien peut constituer un usage illicite de la force[37], ce qui va au-delà du seul emploi de la force armée strictement parlant.

Enfin, comme l'a précisé la Cour internationale de Justice dans son avis sur la *Licéité de la menace ou de l'emploi d'armes nucléaires,* l'interdiction de l'emploi de la force vaut « indépendamment des armes employées »[38]. Dès lors, de la même manière que l'emploi d'armes classiques, chimiques ou biologiques, l'usage d'armes informatiques semble pouvoir constituer un usage de la force.

II. Les cyberattaques comme usage de la force au sens de l'article 2(4)

Puisque la qualification « d'usage de la force » est indépendante du type d'armes employé, les cyber-opérations devraient, théoriquement, pouvoir constituer un usage de la force. Néanmoins, il n'est pas possible de conclure qu'une cyberattaque constitue toujours un usage de la force, puisque celles-ci peuvent être menées par des moyens et à une échelle qui varie. Il s'agit donc d'analyser au cas par cas les cyberattaques.

L'on a vu que la notion de force n'est pas précisément définie en droit international. On peut également tirer deux enseignements des différentes interprétations qu'en ont donné la Cour internationale de Justice ou l'Assemblée Générale des Nations Unies et les Etats : la contrainte

[36] HH. Dinniss, "Cyberwarfare and the laws of war", *Cambridge Studies in International and comparative Law,* 2014, p. 47.
[37] Activités militaires et paramilitaires au Nicaragua et contre celui-ci (Nicaragua c. Etats-Unis d'Amérique), fond, arrêt, CIJ, Recueil 1986, p. 14, §195.
[38] CIJ, Licéité de la menace ou de l'emploi d'armes nucléaires, avis consultatif, C.I.J. Recueil 1996, p. 226, §39.

économique ou politique ne constitue pas un usage de la force au sens de l'article 2(4) ; et l'usage de la force militaire constitue un usage de la force au sens de l'article 2(4).

Selon quel critère définir si une attaque, *a fortiori* une cyberattaque, constitue un usage de la force ? Il existe différentes théories à ce sujet. La méthode dite « instrumentaliste » (*instrument-based approach*) s'attache aux méthodes employées pour conduire une attaque. Une cyber-opération constitue un usage de la force si les cyberattaques présentent les caractères physiques traditionnellement associés à une opération militaire. Une deuxième théorie s'intéresse à la cible de l'opération (*target-based approach*). Lorsque celle-ci vise une infrastructure nationale vitale, l'opération équivaut à un usage de la force. Enfin, la troisième méthode prend en compte les conséquences de l'attaque dans sa globalité (*consequence-based approach*) et cherche à analyser si les effets de l'opération sont suffisamment graves pour la qualifier d'usage de la force.

A. Différentes approches permettant de caractériser l'usage de la force

1. Approche instrumentaliste

L'approche instrumentaliste prend en compte l'instrument par lequel un Etat vient faire usage de la force (dans un sens large). Un Etat peut recourir à la force économique, diplomatique/politique ou la force armée, c'est-à-dire avoir recours à une opération militaire.

Une opération ne sera qualifiée d'usage de la force au sens de l'article 2(4) que lorsqu'elle est physique et présente un caractère militaire[39], puisque la coercion politique ou économique est exclue du champ d'application de l'article 2(4) de la Charte.

Cette approche se concentre sur les moyens employés : plus ceux-ci ressemblent à l'emploi d'armes militaires traditionnelles, plus il est probable que l'opération soit qualifiée d'usage de la force[40].

Il n'existe pas exactement de définition de ce que constitue le caractère « militaire » d'une opération, d'autant plus que les techniques employées évoluent très rapidement. Certains

[39]M. Benatar, "Use of cyberforce: need for legal justification?", *Goettingen Journal of International Law* 1, 3, 2009, p. 388.
[40] Nguyen, "Navigating *jus ad bellum* in the age of cyberwarfare", *California Law Review, Vol. 101(4)*, 2013, p. 1118.

auteurs proposent ainsi de présumer le caractère militaire d'une technique, dès lors qu'elle est employée ou fait partie de l'arsenal des armées d'un Etat. De nombreux Etats ont désormais créé des unités spécialisées dans l'attaque et la défense par des moyens cyber. On peut donc considérer que les cyber-opérations peuvent présenter un caractère militaire.

Certains auteurs ajoutent un second critère, celui du caractère physique de l'opération. Le caractère physique d'une opération s'entend généralement de la production d'une onde de choc, d'un effet explosif. Selon cette approche, une cyberattaque ne pourrait pas constituer un usage de la force, puisqu'il lui manque le caractère physique associé à la coercion militaire[41]. En effet, une cyberattaque s'opère grâce à l'emploi de codes informatiques, qui ne ressemblent pas suffisamment à des armes conventionnelles et ne présentent pas le caractère physique associé à la coercion militaire. La cyberattaque ne cause pas de dommages physiques en soi, même si elle peut en être à l'origine, lorsqu'elle vise à rendre inopérant des systèmes informatiques. Cette approche est renforcée par le fait que l'article 41 de la Charte des Nations Unies considère « l'interruption complète ou partielle des relations […] télégraphiques, radioélectriques et des autres moyens de communication » comme une mesure n'impliquant pas l'usage de la force.

Selon l'approche instrumentaliste, même si l'emploi de cyberattaques peut ressembler à l'emploi d'armes militaires, le fait qu'elles ne présentent pas un caractère physique empêcherait la qualification d'usage de la force au sens de l'article 2(4) de la Charte.

Cette approche est trop limitative et exclut inutilement toutes les cyberattaques de la qualification d'usage de la force. En effet, en conditionnant cette qualification au caractère physique de l'opération, elle exclut toutes les cyber-opérations qui visent à mettre hors d'usage certains réseaux et systèmes informatiques, sans causer directement de dommages. Pourtant, de telles attaques peuvent causer indirectement des dommages physiques, comme une explosion. De plus, certaines opérations peuvent en effet ressembler à l'usage de techniques militaires, mais d'autres, notamment les attaques par déni de service, peuvent difficilement être qualifiées comme semblables à une opération militaire. Puisque cette approche prend uniquement le caractère militaire et physique d'une opération en compte, elle exclut de nombreuses attaques qui produisent pourtant des conséquences graves. Néanmoins, faire une distinction en fonction

[41] D. B. Hollis, "Why states need an informational law for information operations", *Lewis & Clark Law Review, Vol. 11,* p. 1041.

de la gravité des conséquences revient à appliquer l'approche basée sur les conséquences. Par exemple, la question de savoir si l'attaque Stuxnet constituait un usage de la force ne serait même pas adressée, puisque l'opération a été menée à l'aide d'un virus informatique, et non par un missile ou une arme conventionnelle.

2. Approche basée sur la cible

L'approche basée sur la cible considère qu'une cyber-opération constitue un usage de la force lorsqu'elle vise à pénétrer les systèmes des infrastructures nationales vitales, même si l'opération ne cause pas de dommages graves[42]. Certains auteurs parlent également de régime de responsabilité stricte (*strict liability approach*). Elle est justifiée par l'idée qu'aujourd'hui, les sociétés modernes sont particulièrement dépendantes du bon fonctionnement de ces infrastructures, qui elles-mêmes reposent sur l'usage de systèmes informatiques. Or, une opération menée par des moyens non militaires (dans le sens classique du terme) tels que des cyberattaques peut causer des dégâts particulièrement importants à ces infrastructures et donc mettre à mal le bon fonctionnement d'une société. Bien qu'elle présente l'avantage de la facilité, cette approche ne devrait pas être adoptée.

A la différence de l'approche instrumentaliste, l'approche basée sur la cible risque d'inclure un trop grand nombre d'opérations. Certaines opérations, même si elles visent des infrastructures critiques, ne produisent pas d'effets de grande ampleur.

Serait par exemple qualifiée d'usage de la force une cyber-opération visant à rendre inaccessibles, au moyen d'attaques par déni de service, certains sites Internet gouvernementaux durant quelques minutes, ceux-ci fonctionnant à nouveau normalement immédiatement après. Au vu de la pratique des Etats en droit international et de l'avis de la plupart des juristes, une telle opération ne présente pas un degré suffisant de gravité pour être qualifiée d'usage de la force au sens de l'article 2(4).

De plus, il n'existe aucune définition de ce que constitue une infrastructure nationale vitale en droit international. Cela relève donc de l'appréciation de chacun des Etats. Sont généralement considérées comme infrastructures nationales vitales celles dont l'incapacité ou la destruction pourrait avoir un impact grave sur la sécurité, l'économie nationale ou la santé publique. Cela

[42] *Ibid*, p. 1041.

concerne en particulier les secteurs de l'énergie, de la fourniture d'eau, de la banque, des transports et des télécommunications, mais cette liste n'est pas restrictive. En adoptant une approche basée sur la cible, un grand nombre de cyber-attaques seraient qualifiées d'usage de la force, uniquement parce qu'elles visent un domaine qui est considéré par l'Etat victime comme étant essentiel.

La qualification d'une opération comme un usage de la force en fonction de la cible étend trop la notion d'usage de la force et présente un risque d'escalade dans les relations entre Etats.

3. L'approche basée sur les effets

Cette approche est celle favorisée par une majorité d'auteurs, mais également par certains Etats comme les Etats-Unis ou par le groupe d'experts du Manuel de Tallinn. Elle implique que lorsqu'une cyberattaque produit des effets équivalents à l'usage de la force par des moyens cinétiques (comme la destruction de biens ou des pertes en vies humaines), elle constitue un usage de la force.

Pour les rédacteurs du Manuel de Tallinn, « une cyber opération constitue un usage de la force lorsque ses dimensions et ses effets sont comparables à ceux d'une opération non-cyber atteignant le niveau d'un usage de la force »[43]. Les experts raisonnent par analogie et considèrent qu'une cyber-opération, si elle cause les mêmes effets qu'une opération cinétique qualifiée d'usage de la force, constitue également un usage de la force.

Cette méthode, basée sur les effets de l'attaque (*effect-based approach*) permet de qualifier certaines opérations d'usage de la force avec une relative certitude. Il en va notamment ainsi des opérations qui détruisent des objets ou causent la mort d'individus. De telles conséquences pourraient par exemple être atteintes par une cyberattaque causant la fusion des réacteurs d'un site nucléaire, endommageant les systèmes de contrôle aérien ou ouvrant un barrage, causant des inondations.

Elle permet également d'exclure certaines opérations, dont les conséquences sont trop faibles pour qu'elles soient qualifiées d'usage de la force. Le Manuel de Tallinn prend pour exemple une opération non destructrice, psychologique, visant à miner la confiance dans un gouvernement ou une économie. Les conséquences ne sont pas suffisantes pour qualifier la

[43] Tallinn Manual, Rule 11 – Definition of use of force: "A cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force".

cyber opération d'usage de la force. Cela ne signifie pas que l'opération est licite en droit international ; néanmoins, elle n'atteint pas le seuil de l'usage de la force.

Comme le souligne L. Simonet, la méthode basée sur les effets semble être la plus adaptée dans le cadre des cyberattaques. En effet, « l'acte d'agression informatique a ceci de particulier que sa gravité ne réside pas dans le mécanisme de sa survenance en lui-même (l'infiltration d'un virus ou d'un ver dans un réseau informatique), mais dans ses conséquences potentielles sur la vie de l'Etat et de sa population »[44].

Cette approche présente elle aussi des inconvénients, puisqu'elle attache énormément d'importance aux effets que peuvent avoir des opérations cinétiques. Elle rend mal compte de la spécificité des cyberattaques, qui peuvent causer des dommages uniques, qu'une attaque par des moyens traditionnels ne saurait atteindre. Par exemple, une attaque cinétique ne serait pas capable de fermer la bourse d'un Etat en quelques minutes et sans la moindre victime physique ; une cyberattaque le peut. Selon l'approche basée sur les effets, une telle attaque, pouvant pourtant causer des conséquences immenses, ne constituerait pas un usage de la force tel qu'envisagé dans l'article 2(4) de la Charte. De même, une cyberattaque qui échoue à produire les effets envisagés ne sera pas qualifiée d'usage de la force ; tandis qu'une attaque causant des effets non voulus pourra l'être. Ainsi, cette approche n'est pas des plus satisfaisantes en termes de dissuasion[45].

Chacune des méthodes présente des avantages et des inconvénients. Néanmoins, l'approche basée sur les effets constitue la méthode privilégiée par la majorité de la doctrine et les Etats, ainsi que le montre leur pratique (déclarations, rapports, etc.). Elle est également celle qui présente le moins d'inconvénients et semble la plus équilibrée, n'englobant ni trop, ni trop peu d'opérations.

[44] L. Simonet, « L'usage de la force dans le cyberespace et le droit international », *Annuaire français de droit international, Vol. 58,* 2012, p. 124.
[45] Nguyen, « Navigating *jus ad bellum* in the Age of Cyberwarfare" *California Law Review, Vol. 101 (4)*, 2013, p. 1122.

B. Application de l'approche basée sur les effets aux cyberattaques

Une cyberattaque constitue donc un usage de la force prohibé par l'article 2(4) lorsque ces effets équivalent à ceux d'une opération cinétique qualifiée d'usage de la force. Puisque la notion de force n'englobe pas la simple coercion politique ou économique, les cyberattaques dont les effets restent confinés au domaine économique, politique ou diplomatique ne devraient pas être qualifiées d'usage de la force. Ces actes ne sont pas nécessairement légaux en droit international, simplement, ils ouvrent à l'Etat victime un éventail de réponses différents.

Dans un premier temps, il peut être intéressant de regarder la notion d'agression armée, puisqu'un acte qualifié comme tel constitue nécessairement un usage de la force, ainsi que l'a mentionné la Cour internationale de Justice dans l'affaire *Nicaragua*[46]. Néanmoins, la plupart des cyberattaques n'atteignent pas le niveau d'une agression armée, ce qui pose la question de leur qualification comme usage de la force ou non.

1. Cyberattaques de même gravité qu'une agression armée

Dans l'affaire des *Activités militaires et paramilitaires au Nicaragua*, la Cour internationale de Justice esquisse une distinction entre « les formes les plus graves de l'emploi de la force (celles qui constituent une agression armée) et d'autres modalités moins brutales »[47]. Il semble donc exister une forme de gradation au sein même de la catégorie des actes qualifiés « d'usage de la force ».

Cette distinction ne fait pas l'unanimité parmi la doctrine ou les Etats. En particulier, à la suite de cet arrêt, les Etats-Unis ont déclaré ne pas reconnaître de différence entre un usage de la force et une attaque armée – une action qualifiée d'usage de la force ouvrant de la même manière qu'une attaque armée le droit d'un Etat à répondre par des mesures de légitime défense. D'autres auteurs considèrent la différence entre les deux concepts trop étroite pour que la définition soit opérationnelle dans les faits.

Il reste qu'une majorité des Etats et des auteurs reconnaît cette différence, et en tire la conclusion qu'une opération qualifiée d'attaque armée au sens de l'article 51 de la Charte des

[46] Activités militaires et paramilitaires au Nicaragua et contre celui-ci (Nicaragua c. Etats-Unis d'Amérique), CIJ, Recueil 1986, p.14, §191
[47] *Ibid*, §191.

Nations Unies constitue nécessairement un usage illicite de la force. En revanche, une opération qualifiée d'usage de la force ne constitue pas nécessairement une attaque armée, ouvrant le droit pour l'Etat de réagir en légitime défense.

La définition de l'agression armée – tout comme celle de l'usage de la force – reste sujet à débat en droit international. Elle sera examinée plus en détail ci-après, mais il suffit de dire ici qu'on considère généralement qu'une opération suffisamment grave et ayant pour effet de détruire des biens ou de causer des pertes en vie humaines constitue une agression armée, et donc *a fortiori*, un usage de la force.

Selon la méthode basée sur les effets, une cyberattaque dont les effets directs sont d'entraîner la destruction de biens et/ou des pertes en vies humaines constituera donc un usage prohibé de la force, et même une agression armée au sens de l'article 51.

Il convient cependant de garder en mémoire que les articles 2(4) et 51 de la Charte des Nations Unies n'opèrent pas de la même façon. L'article 2(4) pose un principe d'interdiction de l'usage de la force – qui englobe l'agression armée – et permet de déterminer qu'un Etat a violé le droit le droit international. L'article 51 pose une exception à ce principe de prohibition en autorisant un Etat à faire légalement usage de la force au titre de la légitime défense[48].

2. Cyberattaques n'atteignant pas le seuil de gravité d'une agression armée

Certaines cyber opérations constituent un usage de la force - et vont donc au-delà de la simple contrainte économique ou politique - sans être assez graves pour mériter la qualification d'agression armée. La littérature anglo-saxonne parle ainsi d'usage de la force sous le seuil de l'attaque armée (« *use of force short of an armed attack* »).

Ces actes seront qualifiés d'usage de la force au sens de l'article 2(4) en fonction des circonstances. Il en est de même des actes dans le cyberespace, néanmoins, le manque de pratique des Etats rend difficile l'appréciation de ce que constitue un usage de la force sous le seuil de l'agression armée.

[48] C Catherine Lotrionte, « Cyber Operations: Conflict Under International Law", *Georgetown Journal of International Affairs, International Engagement on Cyber 2012: Establishing Norms and Improving Security*, 2012, p. 19.

Dans un des premiers ouvrages s'intéressant avec attention à la question des attaques informatiques, M. Schmitt a développé une théorie qui reste à ce jour une des plus élaborées, et qui est reprise par une majorité de la littérature. Le Manuel de Tallinn se réfère également aux critères de Schmitt et propose de s'en servir pour imaginer comment la communauté internationale qualifierait une cyberattaque.

L'idée est d'observer des critères qualitatifs, permettant de distinguer les opérations qui seraient plutôt qualifiées de coercion économique ou politique, et celles qui atteignent le seuil de l'usage de la force. Il ne s'agit pas de critères formels et entérinés, mais seulement des indices qui influent la décision des Etats lorsqu'ils caractérisent une opération comme constituant un usage de la force. Ces critères sont entre autres la sévérité (*severity*), l'immédiateté (*immediacy*), le caractère direct de l'attaque (*directness*), son degré d'invasivité (*invasiveness*), la mesurabilité des effets (*measurability of the effects*), le caractère militaire de l'opération (*military character*), le degré d'implication d'un Etat (*state involvement*) ainsi que le caractère présumé de légalité de l'opération (*presumptive legality*).

Le critère de la sévérité est assurément le plus important. Une cyberattaque qui a pour conséquence la mort d'individus ou la destruction d'objets constitue un usage de la force, tandis qu'une attaque provoquant seulement une gêne (« *mere inconvenience* ») n'atteindra pas le seuil de l'usage de la force. Entre ces deux extrêmes, on peut considérer qu'une attaque qui a des conséquences pour les intérêts nationaux critiques tendra à être qualifiée d'usage de la force. Pour évaluer la sévérité d'une attaque, il faut prendre en compte son étendue, sa durée et son intensité.

Le critère de la sévérité n'étant en lui-même pas toujours simple à mettre en œuvre, d'autres critères influencent la décision d'un Etat de qualifier une opération comme un usage de la force. Tout d'abord, l'immédiateté de l'attaque influence sur cette décision. Plus les conséquences d'une opération se manifestent tôt, moins les Etats ont le temps de recourir à des mesures pacifiques pour limiter leurs effets néfastes. Ainsi, les Etats auront plus facilement tendance à qualifier une cyberattaque dont les résultats sont immédiats comme un usage de la force puisque la menace sera perçue comme imminente.

Doit être également pris en compte le caractère direct de l'attaque. Le caractère immédiat de l'attaque s'attache à la temporalité, tandis que le caractère direct renvoie à la causalité entre l'opération et les conséquences. Le Manuel de Tallinn détaille ainsi que dans le cadre de mesures de coercion économiques, comme des sanctions ou boycotts, les conséquences tendent à se faire sentir plusieurs semaines voire mois après la décision d'adopter des sanctions. En revanche, les opérations militaires classiques ont des effets plus instantanés – il suffit par exemple de penser à des frappes aériennes ou l'envoi de troupes au sol, dont les conséquences sont quasi-immédiates. Plus les effets d'une cyber-opération sont directs, plus celle-ci est à même d'être considérée comme un usage de la force.

Le critère d'invasivité prend en compte la nature de la cible visée et son importance pour l'Etat victime d'une cyber-opération. Plus la cible visée est sécurisée, plus l'attaque est intrusive et plus elle est vue comme une menace pour l'Etat victime, qui aura plus facilement tendance à la qualifier d'usage de la force. De plus, une opération conduite de sorte à ne viser qu'un Etat accroît le sentiment de menace ressenti par l'Etat victime, comparé à une opération visant indifféremment différents Etats.

Le critère de mesurabilité des effets dérive du fait que les Etats sont plus enclins à caractériser une opération comme un usage de la force lorsque ses conséquences sont apparentes. Toutefois, ce critère peut être difficile à appliquer dans le cyberespace. Il reste qu'une opération a plus de chances d'être qualifiée d'usage de la force si ses conséquences sont quantifiables et identifiables. Par exemple, si un Etat est en mesure de déterminer avec précision l'étendue des conséquences d'une cyber-opération, notamment la masse de données corrompues, de fichiers extraits, le nombre de serveurs touchés, etc., il lui sera plus aisé de déterminer si l'opération équivaut à un usage de la force.

Naturellement, le caractère militaire d'une cyber-opération joue également un rôle, puisque l'opération se rapproche dans ce cas d'une attaque armée, laquelle constitue un usage de la force. Une opération présentera notamment un caractère militaire lorsqu'elle est conduite par l'armée d'un Etat.

Le critère du degré d'implication de l'Etat qui lance la cyber-opération joue également un rôle. Plus l'Etat conduisant la cyber-opération est impliqué et moins il a recours à des « *proxies* », c'est-à-dire des intermédiaires, plus l'Etat victime est susceptible de qualifier l'opération d'usage de la force.

Enfin, le dernier critère à observer est celui de la légalité présumée de l'opération. Le droit international est prohibitif par nature, c'est-à-dire que ce que le droit international n'interdit pas explicitement est en principe autorisé[49]. Puisque le droit international n'interdit pas expressément et de façon générale certaines actions comme la simple pression économique, la propagande, les opérations psychologiques ou l'espionnage, celles-ci sont généralement considérées comme licites. Une cyber-opération dont les conséquences équivalent à une de ces catégories aura donc tendance à être qualifiée de licite et sera moins sujette à la qualification d'usage de la force.

Ces critères doivent être examinés ensemble, afin d'avoir une image globale et d'évaluer au mieux si une cyber-opération se rapproche plus d'une attaque armée ou de la simple coercion économique ou politique, auquel cas elle doit être exclue des frontières de l'usage de la force[50].

Afin de voir comment ces critères opèrent en réalité, il peut être intéressant de les appliquer à un cas concret. Schmitt lui-même a appliqué ces critères aux cyberattaques ayant visé l'Estonie en 2007.

Il considère que les attaques étaient sévères puisqu'elles ont visé des services dépendant du gouvernement, qui ont été sérieusement affectés. Elles ont également mis à mal différents services dans le secteur de l'économie et ont impacté la population locale. Les effets ont été immédiats, et étaient la conséquence directe des opérations par déni de service. Les attaques étaient invasives puisqu'elles visaient des systèmes pour la plupart sécurisés. Elles n'étaient pas présumées licites puisqu'elles visaient à affecter le gouvernement estonien et non à causer de simples pressions. Pris ensemble, il considère que ces critères démontrent que les attaques s'apparentaient à un usage illégitime de la force.

Néanmoins, plusieurs auteurs ont également démontré la faiblesse de ce modèle. Tout d'abord, mis à part l'accent sur le critère de sévérité, aucune indication n'est donnée sur le poids que doit avoir chacun des critères dans l'évaluation de l'opération. Surtout, les critères sont trop malléables, et peuvent conduire à deux résultats opposés.

[49] Affaire du "Lotus", Publications de la Cour permanente de justice internationale, Série A – n°10, 1927, p. 19.
[50] M.N. Schmitt, "Computer attacks and the use of force in international law: thoughts on a normative framework", *Columbia Journal of Transnational Law, Vol. 37*, 1999, p. 916.

En effet, on peut parvenir à un tout autre résultat et considérer que les attaques menées contre l'Estonie ne semblent pas avoir eu des conséquences assez importantes pour être qualifiées d'usage de la force. Bien que les conséquences aient été immédiates – les sites victimes des attaques par déni de services étaient rendus inaccessibles au moment des attaques – les conséquences furent finalement assez minimes. Aucun dommage physique à l'encontre d'individus, direct ou indirect, n'a été enregistré. Les attaques n'ont pas détruit de propriété, elles ont causé une simple gêne, qui plus est temporaire, pour un laps de temps assez court. L'on peut considérer que les conséquences directes des attaques étaient simplement l'indisponibilité des serveurs, et non les dommages économiques ou la perte de confiance dans le gouvernement. De plus, les attaques ont été opérées à distance et n'impliquaient pas la pénétration du territoire. On peut également considérer que les attaques étaient légitimes, puisqu'elles ont seulement interrompu les systèmes de communication, ce qui conformément à l'article 41 de la Charte ne constitue pas un usage de la force.

On le voit, les critères sont donc relativement maniables et sujets à des interprétations différentes en fonction des intérêts géostratégiques des Etats. De plus, l'appréciation variera énormément en fonction des capacités cyber d'un Etat et de sa dépendance aux réseaux et systèmes informatiques. En effet, plus un Etat est dépendant, plus des attaques ciblant ses réseaux et systèmes informatiques aura des conséquences directes pour son gouvernement, son économie ou sa population. Ainsi, la même cyberattaque conduite contre un Etat A ou un Etat B sera appréciée différemment en fonction de la dépendance de cet Etat aux nouvelles technologies.

En guise de conclusion, on peut noter que le modèle de Schmitt est plus nuancé que les dispositions de la Charte et permet de faire une distinction entre différentes attaques en fonction de leur intensité et prend en compte leurs effets indirects. Il constitue l'analyse la plus poussée permettant de savoir quand une cyber-opération constitue un usage de la force mais n'est pas pleinement satisfaisant puisque l'application des critères est trop subjective. De nombreux auteurs, mais aussi certains Etats proposent de redéfinir la notion de force dans le contexte cyber, afin de garantir une certaine sécurité juridique et éviter que l'évaluation de ce que constitue un usage de la force ne soit uniquement laissé à l'appréciation des Etats. Le manque de consensus présente le risque que les Etats définissent avec une certaine largesse certaines opérations comme constituant un usage de la force, et donc comporte le danger d'une escalade dans les réponses apportées par l'Etat victime.

Un cadre légal effectif pour qualifier les cyber-opérations d'usage de la force devrait prendre en compte la gravité des conséquences d'une attaque pour la souveraineté d'un Etat et la paix et la sécurité internationales. Il s'agirait également de prendre en compte les effets réversibles ou non d'une cyberattaque ainsi que la cible d'une attaque, sans pour autant appliquer l'approche basée sur la cible qui fait fi des conséquences. Une cyberattaque serait ainsi qualifiée d'usage de la force lorsqu'elle vise à causer des dommages physiques de grande ampleur et irréversibles en s'attaquant aux systèmes et réseaux informatiques dont une société dépend pour son bon fonctionnement.

Toutes les opérations n'atteignent pas le seuil de l'usage de la force tel qu'envisagé dans l'article 2(4). Toutefois, elles ne sont pas nécessairement licites en droit international. En particulier, elles peuvent contrevenir au principe de non-intervention.

Chapitre 2 : Les cyberattaques comme violation du principe de non-intervention

Ainsi qu'on l'a vu ci-haut, toutes les cyberattaques ne constituent pas un usage de la force, et encore moins une agression armée. Pour autant, ces actes ne sont pas nécessairement en conformité avec le droit international. Sont en particulier concernées les cyberattaques dont les conséquences sont d'ordres politiques ou économiques, puisque, à l'heure actuelle, le concept de « force » tel qu'employé dans l'article 2(4) de la Charte des Nations Unies exclut la contrainte économique ou politique.

Pour ces actes dont la gravité n'atteint pas le seuil de l'usage de la force, la littérature parle de « cyberattaques de faible intensité » (eng : *low-intensity cyberattacks*) ou bien de « cyberattaques non destructives » (eng : *non destructive cyberattacks*)[51]. Certains auteurs soulignent d'ailleurs que si la littérature s'est principalement intéressée à des cyber-opérations de grande ampleur, produisant des effets désastreux, celles-ci, bien que possibles, demeurent rares[52]. Au contraire, il semble que les cyberattaques de « faible intensité » vont connaître une croissance vigoureuse, puisqu'elles permettent pour un Etat d'influencer le jeu des relations internationales, sans pour autant être accusé de faire usage de la force, elles requièrent peu de ressources et réduisent le risque de représailles.

Ces attaques peuvent entrer dans une autre catégorie que celle de l'usage de la force, à savoir celle de l'intervention prohibée par le droit international. Peu d'auteurs se sont intéressés au principe de non-intervention appliqué aux cyberattaques, en comparaison avec le principe de prohibition de l'usage de la force. Généralement, le principe est évoqué rapidement comme constituant une catégorie pour les cyberattaques n'équivalant pas à un usage de la force, sans plus de réflexion sur ce qu'englobe le principe de non-intervention et comment il trouve à s'appliquer dans le contexte cyber. Pourtant, comme le souligne Russel Buchan, « le principe de non-intervention établit un cadre légal qui peut protéger les Etats des cyberattaques qui, bien qu'elles ne produisent pas de dégâts physiques et ne peuvent donc être qualifiées d'usage

[51] Voir par exemple W. Mattessich, « Digital Destruction: Applying the Principle of Non-Intervention to Distributed Denial of Service Attacks Manifesting No Physical Damage", *Columbia Journal of Transnational Law, Vol. 54 (3)*, 2016, p. 876.
[52] S. Watts, "Low intensity cyber operations and the principle of non-intervention", 2014, disponible à https://ssrn.com/abstract=2479609, p.2.

prohibé de la force, ont quand même pour effet de contraindre un Etat à adopter une conduite qu'il devrait pouvoir déterminer librement »[53].

Afin de limiter le recours à la contrainte politique ou économique ayant pour effet de porter atteinte à la souveraineté d'un Etat et sa capacité à agir en toute indépendance, le droit international a développé un principe, celui de la non-intervention dans les affaires intérieures et extérieures. Le principe a aujourd'hui acquis une valeur coutumière, ainsi que l'a rappelé à plusieurs reprises la Cour internationale de Justice[54].

Absent de façon explicite dans la Charte des Nations Unies, le principe trouve une base textuelle importante dans la Déclaration sur les relations amicales et la coopération entre Etats[55] adoptée par la résolution 2625 (XXV) de l'Assemblée Générale des Nations Unies en 1970. Elle dispose que :

> *« Aucun Etat ni groupe d'Etats n'a le droit d'intervenir, directement ou indirectement, pour quelque raison que ce soit, dans les affaires intérieures ou extérieures d'un autre Etat. En conséquence, non seulement l'intervention armée, mais aussi toute autre forme d'ingérence ou toute menace, dirigées contre la personnalité d'un Etat ou contre ses éléments politiques, économiques et culturels, sont contraires au droit international.*
>
> *Aucun Etat ne peut appliquer ni encourager l'usage de mesures économiques, politiques ou de toute autre nature pour contraindre un autre Etat à subordonner l'exercice de ses droits souverains et pour obtenir de lui des avantages de quelque ordre que ce soit. Tous les Etats doivent aussi s'abstenir d'organiser, d'aider, de fomenter, de financer, d'encourager ou de tolérer des activités armées subversives ou terroristes destinées à changer par la violence le régime d'un autre Etat ainsi que d'intervenir dans les luttes intestines d'un autre Etat ».*

[53] Russell Buchan, 'Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?', *17 Journal of Conflict & Security Law 211*, 2012, p. 226.
[54] Par exemple dans l'affaire des *Activités armées sur le territoire du Congo*, §162 ; *Activités militaires et paramilitaires au Nicaragua*, §202.
[55] Déclaration relative aux principes du droit international touchant les relations amicales et la coopération entre Etats conformément à la Charte des Nations Unies, 1970.

Ces dispositions sont reprises par la déclaration sur l'inadmissibilité de l'intervention et de l'ingérence dans les affaires intérieures des Etats[56], qui reconnaît également :

> *« Le droit des Etats et des peuples d'avoir librement accès à l'information et de développer pleinement et sans ingérence leur système d'information et de communications et de mettre leurs moyens d'information au service de leurs aspirations et intérêts politiques, sociaux, économiques et culturels ».*

La référence aux « affaire intérieures ou extérieures » permet de cerner l'étendue des activités protégées par le principe de prohibition de l'intervention. Le concept « d'affaires intérieures » dérive de la théorie du domaine réservé, c'est-à-dire des activités qui ne sont en principe pas régulées par le droit international. En d'autres termes, il s'agit des matières à propos desquelles le principe de souveraineté des Etats permet à chacun d'entre eux de se décider librement ». Il s'agit notamment « du choix du système politique, économique, social et culturel et de la formulation des relations extérieures »[57]. Si ce choix n'est plus libre en raison d'une contrainte exercée par un Etat, celui-ci viole le droit international. Il en est notamment ainsi lorsqu'il a recours à une action militaire, violant à la fois le principe de prohibition de l'usage de la force et celui du principe de non-intervention.

Les affaires « extérieures » comprennent quant à elles le choix des relations diplomatiques et consulaires, le choix d'un Etat de reconnaître un autre Etat ou son gouvernement, le choix de devenir membre d'une organisation internationale, etc.

En plus de concerner les affaires intérieures ou extérieures au sujet desquelles les Etats doivent demeurer libres de faire leur choix, le principe de non-intervention impose que la contrainte (en anglais : « *coercion* ») soit utilisée. Ce terme n'est pas défini en droit international, mais il est plus large que celui de la « force physique », et doit également inclure les actions qui visent à entraver le choix d'un Etat et le forcent à agir de telle ou telle manière. La simple « contrainte »

[56] Déclaration sur l'inadmissibilité de l'intervention et de l'ingérence dans les affaires intérieures des Etats, A/RES/36/103.
[57] Activités militaires et paramilitaires au Nicaragua et contre celui-ci (Nicaragua c. Etats-Unis d'Amérique), CIJ, Recueil 1986, p.14, §205.

à l'encontre d'individus est insuffisante, elle doit être exercée dans le but d'impacter l'Etat, et non simplement un groupe de citoyens ou une entreprise.

La contrainte doit être distinguée de la simple influence : les activités qui visent à faire adopter un comportement à un Etat ne constituent une violation du principe de non-intervention que dans la mesure où elles obligent effectivement l'Etat à adopter ce comportement, celui-ci ne doit pas disposer de marge de manœuvre.

Le principe de non-intervention a été longuement discuté et explicité dans l'arrêt de la Cour internationale de Justice sur les *Activités militaires et paramilitaires au Nicaragua*. Dans cet arrêt, le Nicaragua a notamment tenté de faire valoir que certaines mesures d'ordre économique prises par les Etats-Unis à son encontre constituaient « une forme d'intervention indirecte dans ses affaires intérieures »[58].

Comme l'a expliqué la Cour, en raison de leur gravité, les actions qui constituent un usage de la force au sens de l'article 2(4) de la Charte des Nations Unies, et *a fortiori* une agression armée constituent également une violation du principe de non-intervention[59]. On peut également conclure de cet arrêt que le fait de financer, de soutenir et d'entraîner des rebelles constitue une intervention prohibée par le droit international[60], tout comme le fait de fournir des armements ou un soutien logistique[61]. Ainsi, le fait pour un Etat de financer, entraîner et supporter un groupe d'activistes opérant à l'aide de moyens cyber ou le fait de fournir des logiciels ou une assistance logistique pourrait constituer une intervention de cet Etat ; même s'il n'agit pas directement[62].

Mais le principe de non-intervention est plus large, et englobe la coercion économique, politique et idéologique. Certains auteurs parlent également de caractère « dictatorial » des actions. Il reste que les contours exacts de ce qui est prohibé demeurent flous. Le droit international admet le jeu d'influences, mais seulement dans une certaine mesure. Le critère

[58] *Ibid*, §123.
[59] *Ibid*, §205.
[60] *Ibid*, §247.
[61] *Ibid*, §195.
[62] Aussi la position du Manuel de Tallinn 2.0, Commentary on Rule 66, §23.

central est celui de la contrainte, le fait d'imposer un certain comportement à un Etat, en dépit du droit qui lui est reconnu d'exercer sa souveraineté sur le sujet. Il y a un élément de coercion lorsqu'il ne peut être mis fin à l'intervention au bon plaisir de l'Etat victime.

Avant de donner quelques exemples de cyber-opérations pouvant être qualifiées d'interventions, il est à noter que même si le droit international tend ces dernières années à étendre ses dispositions aux acteurs non-étatiques, il n'existe pas à ce jour de textes ou de pratique des Etats qui démontre l'application du principe de non-intervention aux acteurs non-étatiques. Le principe de non-intervention ne s'applique donc que pour des actes attribuables à un Etat.

L'usage de la contrainte économique n'est pas explicitement prohibé en droit international et il n'en est pas fait mention dans la Charte des Nations Unies. Certains auteurs soulignent d'ailleurs que la contrainte économique constitue un instrument nécessaire lorsque l'autre solution à disposition d'un Etat est l'usage de la force militaire[63]. Il reste que la contrainte économique doit rester limitée et ne pas se transformer en coercion portant atteinte à la souveraineté d'un Etat.

Il faut avoir en tête que les pressions sur l'économie d'un Etat qui peuvent être exercées grâce à des moyens cyber sont d'une nature complètement différente de celles généralement adoptées. En effet, il y a peu de ressemblance entre des sanctions économiques telles qu'un embargo et une cyberattaque contre le système bancaire et financier d'un Etat.

Un exemple typique de cyberattaque pouvant être caractérisée d'intervention prohibée par le droit international est une opération visant les systèmes informatiques de la bourse d'un Etat, par exemple le New York Stock Exchange, si cette opération est conduite dans le but de forcer un Etat à adopter tel ou tel comportement. Ce scénario est régulièrement envisagé, en particulier car il pourrait être conduit sans causer de pertes en vie humaines ou la destruction de biens de façon directe, ce que ne pourrait pas nécessairement éviter une opération cinétique avec le même but. Il ne constitue pas un usage de la force ou une agression armée, puisque ses effets se cantonnent au domaine économique. En revanche, il s'agirait d'une intervention prohibée

[63] M. Gervais, "Cyberattacks and the laws of war", *Berkeley Journal of International Law, Vol. 30 (2)*, 2012, p. 551.

par le droit international, puisque la mise à mal du système économique et financier de l'Etat victime constitue une ingérence dans ses affaires intérieures.

La coercion idéologique renvoie à la tentative d'influencer sur la politique intérieure d'un Etat. Le cyberespace est particulièrement vulnérable, puisqu'Internet est un espace accessible à tous et sa structure rend la diffusion à grande échelle de messages possible à faibles coûts. Bien que la Charte des Nations Unies soit muette sur l'usage de l'instrument idéologique comme moyen de coercion, un certain nombre d'accords internationaux limitent son usage dans un but hostile[64].

Dans sa résolution 110 (II)[65], l'Assemblée Générale s'est exprimée sur la légalité du recours à la propagande. Elle condamne la propagande destinée ou de nature à provoquer ou à encourager toute menace à la paix, rupture de la paix ou acte d'agression. La pratique des Etats démontre cependant l'ineffectivité de ces déclarations. Il existe bien certains cas dans lesquels des Etats ont été condamnés pour avoir diffusé de la propagande encourageant la violence, en particulier dans le contexte du génocide.

En dehors de ces cas, le droit international semble peu enclin à définir l'usage de l'instrument idéologique comme une violation du principe de non-intervention. Ainsi, il semble qu'à ce jour, des cyberattaques visant à influencer l'opinion, par exemple en diffusant de la propagande ou en hackant les pages d'un parti pour l'associer à des positions radicales ne serait pas considérées comme une violation du principe de non-intervention, ni même comme illégales aux yeux du droit international (même si cela peut l'être en droit interne).

Toutefois, pourraient être considérée comme une intervention prohibée par le droit international des cyberattaques visant à diffuser de la propagande si la contrainte exercée sur les électeurs et le système politique de l'Etat victime est avérée. Le Manuel de Tallinn souligne que le test décisif demeure l'existence d'une contrainte[66]. Pour constituer une intervention prohibée, il doit s'agir d'actions réellement contraignantes, et non seulement des opérations visant à persuader ou influencer le choix des électeurs. Pour distinguer une action de propagande contraignante d'une action visant simplement à persuader l'audience, la littérature propose notamment de regarder si l'audience dispose de moyens alternatifs de s'informer ou si les actions de

[64] *Ibid*, p. 552.
[65] Résolution de l'Assemblée Générale des Nations Unies, 110 (II), Centième séance plénière, 21 octobre 1947.
[66] Tallinn Manual, Commentary on Rule ??, §10.

propagande restreignent l'information accessible[67]. Ainsi, de la propagande diffusée sur certains sites Internet ne constituerait pas une intervention prohibée par le droit international ; tandis que des cyberattaques visant à diffuser de la propagande dans tous les médias d'information et empêchant d'autres informations de circuler seraient qualifiées comme violant le principe de non-intervention.

Enfin, une cyberattaque visant à s'introduire dans le système informatique d'un gouvernement pour en voler des informations confidentielles avant de les diffuser publiquement ou pour les transmettre à un groupe de rebelles cherchant à faire tomber le gouvernement pourrait constituer une ingérence diplomatique[68].Toutefois, la simple intrusion dans un système pour voler des informations ne constitue pas une intervention, puisqu'aucune contrainte n'est exercée sur l'Etat victime. Il peut s'agir d'une violation de la souveraineté de cet Etat, mais l'opération ne présente pas d'élément de coercion. Le groupe d'experts du Manuel de Tallinn confirme cette analyse, et ajoute que même si l'intrusion dans un système suppose de déjouer des barrières défensives comme des pares-feux ou de « cracker » des mots de passe, il se n'agit pas d'une intervention, puisqu'il n'y a pas d'élément de contrainte[69].

Une cyber-opération peut également avoir pour effet de contraindre à la fois économiquement, idéologiquement et/ou diplomatiquement. Par exemple, dans le cas des cyberattaques ayant visé l'Estonie, les opérations de déni de services ont porté atteinte principalement à des sites médiatiques, ont diffusé des informations visant à décrédibiliser les dirigeants politiques, mais ont aussi eu pour effet de ralentir l'économie puisque de nombreux sites Internet, notamment bancaires, ont été rendus inaccessibles.

Rares sont les personnes qui qualifient les incidents en Estonie d'usage prohibé de la force. En revanche, de nombreux auteurs considèrent qu'il s'agissait d'une violation du principe de non-intervention, compte tenu de la durée (plusieurs semaines) et de la sévérité des attaques qui visaient à exercer plus qu'une influence sur le pays, en cherchant à faire pression sur le

[67] S. Watts, "Low intensity cyber operations and the principle of non-intervention", p. 14.
[68] M. Gervais, "Cyberattacks and the laws of war", *Berkeley Journal of International Law, Vol. 30 (2)*, 2012, p. 550.
[69] Tallinn Manual, commentary on Rule 10 §8.

gouvernement pour le forcer à revenir sur sa décision de retirer le mémorial soviétique[70]. Les interférences qu'elles ont causé aux communications et aux systèmes bancaires du pays ont eu un impact suffisant, en particulier compte tenu de la dépendance du pays aux nouvelles technologies[71], pour que l'on considère qu'il s'agit d'une intervention prohibée par le droit international[72]. L'opération n'a néanmoins jamais pu être qualifiée comme telle puisqu'elle n'a pas pu être attribuée à un Etat et que le principe de non-intervention ne s'applique pas, à ce jour, aux acteurs non-étatiques.

Il en va de même pour les évènements survenus en Géorgie en 2008. Les cyberattaques ayant visé les infrastructures de communications, les systèmes informatiques bancaires et médiatiques ont empêché le gouvernement géorgien de communiquer durant une période de crise. Si elles avaient été attribuées à un Etat, elles auraient très probablement été qualifiées de violation du principe de non-intervention[73].

Le principe de non-intervention permet donc de qualifier des cyber-attaques n'atteignant pas le seuil de l'usage de la force comme des actes illicites au regard du droit international. Néanmoins, compte tenu du manque de clarté attaché au principe de non-intervention, mais surtout, des problèmes d'attribution, celui-ci demeure difficile à appliquer dans le cyberespace. En effet, faute de pouvoir qualifier une opération menée par un groupe non-étatique, ou tout simplement faute de pouvoir attribuer une opération à un Etat, le principe ne peut jouer et n'ouvre pas de réponse à l'Etat victime.

De plus, certains auteurs soulignent[74] que si certaines cyber-opérations atteindront en effet le seuil de gravité d'une intervention prohibée par le droit international, beaucoup demeureront dans une zone « grise », en particulier lorsqu'elles visent des entreprises privées, mais aussi parce que ces opérations sont très localisées et n'impactent que rarement la conduite des affaires d'un Etat.

[70] R. Buchan, "Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?", *Journal of Conflict and Security Law*, 17(2), 2012, p. 225.
[71] G.D. Brown/O.W. Tullos, "On the spectrum of cyberspace operations", *Small Wars Journal*, 2016, p. 6.
[72] Mattessich, p. 895.
[73] *Ibid*, p. 6.
[74] Par exemple B.A. Walton, « Duties Owed: Low-Intensity Cyber Attacks and Liability for Transboundary Torts in International Law", *Yale Law Journal, Vol. 126 (5)*, 2017, p. 1473.

Compte tenu de ces objections pratiques à l'application du principe de non-intervention dans le cyberespace, il convient de se tourner vers un dernier concept permettant de qualifier une cyber-opération d'illicite au regard du droit international.

Chapitre 3 : Le principe de diligence dans le cyberespace

Comme on l'a vu ci-haut, un Etat peut commettre une violation du droit international lorsqu'il a recours à une cyber-attaque qui constitue un usage prohibé de la force ou constitue une intervention dans les affaires intérieures ou extérieures d'un autre Etat. Il se rend coupable de la commission d'un acte. Mais une opération est plus généralement illicite lorsqu'elle viole la souveraineté d'un Etat. L'article 2(1) de la Charte des Nations Unies dispose ainsi que « l'organisation est fondée sur le principe de l'égalité souveraine de tous ses Membres ». On peut considérer que les Etats exercent aussi leur souveraineté dans le cyberespace, en tout cas sur leur cyber-infrastructures.

C'est notamment ce qu'affirment les experts rédacteurs du Manuel de Tallinn dans leur première règle : « un Etat peut exercer le contrôle sur les cyber-infrastructures et les activités situées sur son territoire souverain »[75]. Cela signifie qu'un Etat régule de la façon dont il le souhaite l'usage et l'accès aux infrastructures situées sur son territoire. Une attaque qui viserait une cyber-infrastructure constitue une violation de la souveraineté de cet Etat.

Le Manuel de Tallinn pose pour principe qu'un Etat ne doit pas conduire de cyber opérations qui violent la souveraineté d'un autre Etat. Toutefois, cette règle s'applique seulement entre Etats, et ne joue pas à l'égard des acteurs non-étatiques, qui ne sont pas liés par l'interdiction de violer la souveraineté d'un Etat en droit international. Leurs actions ne sont pas licites pour autant, simplement, elles ne sont pas régies par le droit international, mais doivent l'être par le droit interne des Etats.

Différents Etats, notamment la France, ont exprimé le même avis dans leur prise de position sur le cyberespace[76].

Toutefois, le droit international impose aussi aux Etats d'adopter une certaine conduite, dont le non-respect constitue une violation de leur obligation par omission. Une de ses obligations a été explicité par la Cour internationale de Justice dans l'affaire du Détroit de Corfou, celle de «

[75] Tallinn Manual – Rule 1 – Sovereignty: « A State may exercise control over cyber infrastructure and activities within its sovereign territory ».
[76] Stratégie nationale de cyberdéfense, p. 100.

ne pas laisser utiliser son territoire aux fins d'actes contraires aux droits d'autres Etats ». Cette règle découle du principe cardinal de la souveraineté des Etats. Entre Etats indépendants, chacun est libre d'exercer sa souveraineté sur son territoire, mais doit se garder d'affecter la souveraineté des autres Etats. Dans son arrêt récent sur l'Affaire relative à des usines de pâte à papier sur le fleuve Uruguay, la Cour internationale de Justice a rappelé ce principe et précisé sa nature coutumière en déclarant que « le principe de prévention, en tant que règle coutumière, trouve son origine dans la diligence requise (« *due diligence* ») de l'Etat sur son territoire »[77].

La diligence due correspond à un standard de conduite attendu de la part des Etats. Bien que cette affirmation soit rendue dans le cadre de dommages causés à l'environnement d'un autre Etat, la règle est générale et devrait aussi trouver à s'appliquer aux cyber-opérations.

C'est dans cet esprit que le rapport du GGE de 2015 précise que « Les États ne devraient pas permettre sciemment que leur territoire soit utilisé pour commettre des faits internationalement illicites à l'aide des technologies de l'information et des communications »[78].

Le Manuel de Tallinn 2.0 reprend le concept de diligence due dans sa règle 6 qui dispose que « un Etat doit exercer la diligence due en n'autorisant pas à ce que son territoire ou les cyber infrastructures sous son contrôle ne soient utilisées pour des cyber opérations affectant les droits et produisant des conséquences graves à l'égard d'autres Etats »[79].

Cette situation implique 3 parties : l'Etat victime de la cyber opération ; l'Etat sur le territoire duquel elle est menée ; une partie tierce à l'origine de l'attaque, qui peut être un Etat, une entreprise, un groupe d'individus, etc. Si l'interdiction de porter atteinte à la souveraineté d'un Etat s'adresse aux seuls Etats, le principe de diligence due peut concerner des actes d'acteurs non-étatiques qui ont été rendus possibles en raison du non-respect par un Etat de son obligation d'empêcher que son territoire ne soit utilisé pour mener des cyber opérations hostiles à l'encontre d'un autre Etat.

Le niveau de gravité que les dommages causés doivent atteindre pour que l'Etat sur le territoire duquel l'opération a été menée soit en violation de son obligation de diligence due demeure controversé. Le Manuel de Tallinn emploie le terme de « conséquences graves » (eng : '*serious*

[77] Usines de pâte à papier sur le fleuve Uruguay (Argentine c. Uruguay), arrêt, C.I.J. Recueil 2010, p. 14, §101.
[78] A/70/174.
[79] Tallinn Manual 2.0, Rule 6 : "A state must exercise due diligence in not allowing its territory, or territory or cyber infrastructure under its governmental control, to be used for cyber operations that affect the rights of, and produce serious adverse consequences for, other States".

consequences') même si certains ont proposé d'abaisser ce seuil et de parler de conséquences « signifiantes » (‘*significant'* ou « substantielles » (‘*substantial'*).

Pour qu'un Etat soit en violation de son obligation de diligence, il doit avoir connaissance de ce que son territoire est utilisé à des fins hostiles envers un autre Etat. Cette condition de connaissance se mesure de façon subjective et objective, en prenant en compte les informations dont il dispose, notamment de la part de d'autres Etats ou de ses services de renseignement par exemple. Toutefois, il peut être compliqué pour l'Etat victime de démontrer qu'un Etat avait connaissance de l'utilisation qui était faite de son territoire par les auteurs d'une attaque.

Certains auteurs plaident pour une présomption de connaissance de l'Etat dont les réseaux sont utilisés à des fins hostiles de façon répétée ou lorsqu'il est possible de retracer l'origine d'une cyberattaque au territoire d'un Etat en particulier[80]. Toutefois, cette présomption peut être dangereuse. La Cour internationale de Justice a déjà identifié ce risque dans l'affaire du Détroit de Corfou, en déclarant que la connaissance n'est pas établie par le simple fait qu'une action trouve son origine dans le territoire d'un Etat[81].

Les experts du Manuel de Tallinn considèrent que si un Etat, dans les circonstances de l'espèce aurait dû savoir que son territoire était utilisé à des fins hostiles, on peut considérer qu'il en avait connaissance (théorie de la « *constructive knowledge* »). Cette connaissance présumée sera par exemple plus facile à démontrer si les cyber infrastructures utilisées pour mener la cyberattaque sont sous le contrôle de l'Etat ; elle sera plus dure à démontrer si les cyber infrastructures appartiennent à un acteur privé.

Concrètement, la connaissance pourrait aussi être présumée lorsque par exemple, le CERT[82] d'un Etat en avertit un autre quant à la conduite de cyber-opérations hostiles émanant de son territoire[83].

Il reste que le concept de diligence due n'impose pas à un Etat de prendre des mesures préventives. En particulier, la règle ne doit pas être interprétée comme imposant aux Etats de se munir de systèmes de défense empêchant toute utilisation de ses cyber infrastructures à des

[80] Voir en ce sens R. Garnett/P.Clarke, « Cyberterrorism: a new challenge for international law » in Andrea Bianchi (ed), *Enforcing International Law Norms against Terrorism*, Hart Oxford, 2004, p. 479.
[81] Affaire du Détroit de Corfou, Arrêt du 9 avril 1949, C.I.J. Recueil 1949, p. 18.
[82] *Computer Emergency Response Team*, définition donnée ci-après.
[83] J.C. Woltag, "Cyber Warfare – Military Cross-Border Computer Network Operations under international Law", Intersentia, 2014, p. 105.

fins hostiles. Cela constituerait une obligation trop lourde, qui ne peut pas être remplie par les Etats, compte tenu de la variété et de la sophistication des cyberattaques qui peuvent être entreprises.

Enfin, le manquement à l'obligation de diligence doit être distingué de l'aide ou de l'assistance d'un Etat dans la conduite d'une cyber opération. Par exemple, un Etat sera considéré comme aidant et assistant lorsqu'il met à disposition ses infrastructures pour la conduite d'une cyberattaque ; en revanche, le fait de ne pas prendre de mesures lorsque ses infrastructures sont utilisées à des fins hostiles constitue un manquement à l'obligation de diligence.

Pour se conformer à son obligation de diligence, un Etat doit, dès lors qu'il a connaissance de l'utilisation hostile qui est faite de son territoire, prendre les mesures à sa disposition pour y mettre fin.

Compte tenu de la difficulté de traiter toutes les menaces cyber, il serait déraisonnable d'imposer aux Etats une obligation de prévention. De plus, l'obligation de vigilance impose de prendre des mesures pour mettre fin à un acte hostile, ce qui signifie que l'acte est en cours ou imminent. Il serait contradictoire d'attendre d'un Etat qu'il prenne des mesures contre des opérations cyber futures et hypothétiques.

L'Etat doit prendre les mesures à sa disposition, c'est-à-dire les mesures qu'il peut raisonnablement mettre en œuvre. Ainsi, la conformité avec l'obligation de diligence s'analyse plutôt comme une obligation de moyens que comme une obligation de résultat. Dans le contexte cyber, cela signifie notamment que l'on n'attendra pas d'un Etat dont les capacités cyber sont peu développées les mêmes mesures que d'un Etat disposant de techniques de pointe. Néanmoins, cela ne doit pas servir d'excuses à des pays dont les capacités sont moins développées pour se dédouaner. Désormais, il semble que la mise en place de régulation minimes, l'instauration d'un CERT[84] et la désignation d'un contact constitue un standard minimum de sécurité dans le domaine cyber[85].

[84] Un CERT (*Computer Emergency Response Team*) constitue une structure permanente d'alerte et d'assistance pour les administrations et entreprises. Elle a pour mission à la fois de conseiller et d'alerter sur les vulnérabilités des systèmes et réseaux informatiques, mais également de venir en aide aux opérateurs lorsque ceux-ci font face à des cyber-incidents. Aujourd'hui, la plupart des Etats ont mis en place un CERT, et les différents CERT coopèrent et procèdent à des échanges d'informations grâce au FIRST (*Forum of Incidents Response and Security Teams*).
[85] J.C. Woltag, "Cyber Warfare – Military Cross-Border Computer Network Operations under international Law", Intersentia, 2014, p.106.

Ainsi, un Etat ne peut laisser des cyberattaques qui trouvent leur origine sur son territoire se produire s'il en a connaissance. Les experts n'ont toutefois pas réussi à trouver un consensus sur l'étendue de l'obligation imposée aux Etats. Si un Etat a par exemple connaissance des actions d'un groupe d'hacktivistes, et qu'il peut prendre des mesures pour l'empêcher de lancer des cyberattaques qui produiraient un effet négatif sur le territoire d'un autre Etat, sa défaillance constitue un acte international illicite. En revanche, il est compliqué d'étendre l'obligation à des mesures de prévention, pour faire en sorte que de telles situations ne se produisent pas, compte tenu des spécificités du cyberespace. En effet, même la mise en œuvre de moyens techniques ou de renseignement ne peut suffire à prévenir toutes les actions des individus ou groupes d'individus.

Le concept de diligence est certes intéressant, puisqu'il permet, comme on le verra dans la seconde partie de ce travail, d'adopter des mesures pour se protéger contre une menace ou une attaque cyber même lorsque l'auteur n'est pas identifié avec certitude ou lorsque l'opération ne peut être attribuée directement à un Etat. Néanmoins, il suppose tout de même de pouvoir identifier avec une certitude relative de quel territoire la cyberattaque émane. Cela reste techniquement compliqué, requiert du temps et des ressources ; et la possibilité d'une erreur d'identification n'est pas à exclure. Surtout, il faut pouvoir prouver que l'Etat sur le territoire duquel les cyber opérations ont pris place avait connaissance de ces actions et n'a pas pris les mesures qu'un autre Etat prendrait raisonnablement dans les mêmes circonstances. Or, à ce jour, les mesures qu'un Etat doit raisonnablement prendre vis-à-vis du cyberespace sont plutôt floues[86].

Ces différents développements ont permis de conclure quand une cyberattaque est illicite au regard du droit international. En fonction de sa gravité, elle pourra être caractérisée d'usage de la force ou de violation du principe de non-intervention. Le recours au principe de diligence permet également de classifier les cyberattaques menées par des acteurs non-étatiques non pas

[86] Geiss/Lahmann, "Freedom and security in cyberspace: shifting the focus away from military responses towards non-forcible countermeasures and collective threat prevention" *in Peacetime Regime for State Activities in Cyberspace, K. Ziolkowski (ed.), 2013,* p. 653.

comme internationalement illicites en soi, mais de caractériser le comportement d'un Etat qui les laisse se produire comme illicite.

Cela nous amène maintenant à nous poser la question de savoir quelles réponses un Etat peut prendre lorsqu'il est victime d'une cyberattaque.

Seconde partie - Licéité des réponses aux cyber-attaques

Un Etat victime d'une cyberattaque doit pouvoir se défendre. Le droit international offre ainsi différentes possibilités pour rétablir le *statu quo ante*, c'est-à-dire pour revenir à une situation licite au regard du droit international. Le but est de mettre fin à l'acte illicite, et non de « punir » l'Etat qui est à l'origine dudit acte.

La France a notamment rappelé dans sa stratégie nationale de cyberdéfense « sa position en faveur de la reconnaissance claire et univoque de la licéité des moyens de réponse à une cyberattaque, qu'ils impliquent un recours à la force (légitime défense) ou non (contre-mesures, mesures de rétorsion, etc.) »[87]. Elle parle également de « mécanismes exceptionnels d'autoprotection », ce qui peut être compris comme faisant référence à l'état de nécessité[88].

La littérature s'est principalement tournée vers le droit de légitime défense, qui est reconnu comme étant du droit international coutumier, mais également codifié dans l'article 51 de la Charte des Nations Unies. Néanmoins, le recours à la légitime défense n'est pas la seule réponse possible, et ne constitue pas toujours la plus adaptée dans le cyberespace. Il convient d'analyser quelles autres mesures sont à la disposition des Etats victimes d'une cyberattaque.

Toutefois, avant d'envisager de prendre des mesures contre un Etat, encore faut-il savoir contre quel Etat ces mesures doivent être dirigées. On touche alors au problème de l'attribution des cyberattaques, qui constitue un préalable à la mise en œuvre de la plupart des réponses licites en droit international.

[87] Stratégie nationale de cyberdéfense, parue le 29 juin 2018, p. 103.
[88] F. Delerue, « Le droit international dans la 'stratégie nationale de la cyberdéfense' », *IRSEM*, 2018, p. 4.

Chapitre 1 : L'attribution des cyber-attaques comme condition préalable à l'adoption de réponses licites en droit international

I. L'attribution d'un comportement en droit international

La plupart des réponses licites en droit international face à un acte hostile nécessitent de pouvoir au préalable attribuer ledit acte à un Etat. En effet, le droit international se préoccupe des relations entre Etats, mais n'a pas vocation à régler les crimes commis par les individus (mis à part les plus graves, qui peuvent être incriminés par le droit pénal international, comme le génocide ou les crimes contre l'humanité).

L'Etat est une fiction juridique et ne peut en tant que tel pas agir « physiquement ». On peut toutefois lui attribuer le comportement de certains individus ou groupes d'individus. Les règles relatives à l'attribution d'un comportement à un Etat ont été rassemblées dans le Projet d'articles relatif à la responsabilité des Etats. Bien que n'ayant pas le statut de droit conventionnel, ces règles ont été adoptées par une résolution de l'Assemblée générale des Nations Unies[89] et l'on considère qu'elles reflètent globalement le droit international coutumier applicable.

Différents comportements peuvent être attribués à un Etat. Tout d'abord, « le comportement de tout organe de l'Etat est considéré comme un fait de l'Etat d'après le droit international ». La notion d'organe dans le droit international de la responsabilité des Etats est conçue de façon large et s'entend de « toutes les personnes ou entités qui entrent dans l'organisation de l'État et qui agissent en son nom »[90]. Ainsi, les services militaires, des agences ou les services de renseignement d'un Etat sont considérés comme des organes étatiques dont la conduite est attribuable à l'Etat.

Un comportement sera également attribué à un Etat lorsqu'il est le fait d'une personne ou entité qui n'est pas un organe de l'Etat « mais qui est habilitée par le droit de cet Etat à exercer des prérogatives de puissance publique ». Cette règle permet d'englober les entités « paraétatiques

[89] A/RES/56/83.
[90] Commentaire de la Commission du droit international sur l'article 4 du projet d'articles relatif à la responsabilité de l'Etat pour internationalement illicite, §1.

» telles que des institutions publiques ou des entreprises publiques ou privées que le droit interne d'un Etat habilite à exercer des prérogatives de puissance publique.

Enfin, le comportement d'une personne ou d'un groupe de personnes est attribuable à un Etat s'il « agit en fait sur les instructions ou les directives ou sous le contrôle de cet Etat »[91]. Cette règle permet ainsi d'attribuer des actes commis par des personnes ou entités privées à un Etat. Il peut s'agir par exemple d'une entreprise employée par un Etat et exécutant ses ordres. Néanmoins, le degré de contrôle que doit exercer l'Etat sur les activités des individus ou de l'entité n'est pas précisé, ce qui a donné lieu à des nombreux débats.

La Cour internationale de Justice a été confrontée à ce problème dans l'affaire des *Activités militaires et paramilitaires au Nicaragua*. Elle a déclaré que, pour qu'un comportement soit attribué à un Etat, celui-ci doit avoir le « contrôle effectif des opérations ». Le fait qu'un Etat ait exercé le contrôle effectif sur des actes est déterminé au cas par cas, mais cela implique qu'il ait donné des orientations précises à un groupe de personnes, qui agit dépendamment de ses instructions et ne bénéficie pas d'une marge de manœuvre sur les opérations concrètes. L'Etat conserve la mainmise sur les opérations et peut décider d'y mettre fin. Des indications globales ne suffisent pas à établir le contrôle effectif.

On oppose souvent au standard de contrôle effectif celui du « contrôle global » adopté par la Chambre d'appel du Tribunal pénal international pour l'ex-Yougoslavie (TPIY) dans l'affaire *Tadic*[92]. Pour qu'un acte soit attribuable à un Etat, celui-ci n'a pas besoin de donner des ordres concrets et directs relatifs aux opérations en question ; le fait d'organiser et de coordonner les opérations est suffisant. Néanmoins, cette affaire concernait l'application du droit international humanitaire et surtout, s'intéressait à des questions de responsabilité pénale individuelle et non pas à la responsabilité des Etats. De plus, la Chambre d'appel a précisé que le standard valait dans le cas de groupes « structurés et hiérarchisés » tels que des milices et non pour des groupes non-étatiques moins structurés.

Ainsi, la majorité de la doctrine considère que le « contrôle » mentionné dans l'article 8 des articles sur la responsabilité des Etats s'entend du « contrôle effectif », tel que précisé par la Cour internationale de Justice dans l'affaire *Nicaragua*.

[91] Projet d'articles sur la responsabilité de l'Etat pour fait internationalement illicite, Article 8.
[92] Affaire IT-94-1, *Le Procureur* c. *Tadić* (1999) *I.L.M.*, vol. 38, p. 1518.

Enfin, un comportement peut être attribué à un Etat « si, et dans la mesure où, cet État reconnaît et adopte ledit comportement comme étant sien ». Cette règle a notamment été appliquée dans l'arrêt de la Cour internationale de Justice dans l'affaire du *Personnel diplomatique et consulaire*[93]. La Cour a considéré que l'Iran était responsable des actions des preneurs d'otages à l'ambassade compte tenu de l'approbation donnée par le chef du gouvernement et différents organes de l'Etat et de leur décision de ne pas mettre fin à la prise d'otages. Cette règle demeure d'application stricte : les conditions de reconnaissance et d'adoption sont cumulatives, et requièrent plus qu'un simple soutien ou une approbation tacite.

L'application de ces règles peut sembler simple à première vue, mais il convient d'analyser si elles sont adaptées au cyberespace.

II. L'attribution d'une cyberattaque à un Etat

Il faut avant tout rappeler certains points quant aux caractères uniques du cyberespace qui rendent la question de l'attribution particulièrement épineuse.

Techniquement, il peut être compliqué de retracer l'origine d'une cyber-attaque. Celles-ci se caractérisent généralement par leur vitesse. Or, une fois qu'une cyber-attaque arrive à son terme, il est plus compliqué de retracer son origine (*back-tracking*). L'auteur d'une cyber-attaque peut employer des méthodes dites de « *spoofing* » lui permettant de masquer son identité ou de prendre l'identité d'un autre. Certains malwares sont également conçus pour cacher leurs traces et s'auto-détruire après avoir infecté les systèmes, de telle sorte qu'il est impossible de les analyser *a posteriori*[94]. Enfin, dans certains cas, notamment lors d'attaque par déni de services distribués, l'auteur de la cyber-attaque agit à travers des ordinateurs infectés à distance, les *botnets*. L'identification est donc compliquée par le fait que l'attaque émane en apparence d'ordinateurs, localisés dans tel ou tel Etat, mais qui sont en réalité contrôlés à l'insu de leurs propriétaires par les « maîtres », localisés dans un autre Etat.

De même, une cyberattaque sera parfois élaborée à partir d'outils informatiques, mais diffusée manuellement, par exemple à l'aide de l'introduction d'une clé USB contenant un logiciel

[93] Personnel diplomatique et consulaire de l'ambassade des Etats-Unis à Téhéran, arrêt, C.I.J. recueil 1980, p. 3.
[94] Par exemple le virus Flame, voir l'article du Point « Stuxnet. Duqu. Et maintenant Flame. Ces virus relancent le débat sur le déploiement des cyberattaques » du 11 juin 2012.

infecté dans des systèmes informatiques. Il n'est alors pas possible de retracer l'origine de la cyberattaque par des moyens informatiques.

Néanmoins, l'identification de l'auteur d'une cyberattaque n'est pas impossible, et de plus en plus d'acteurs – qu'il s'agisse d'Etats ou d'entreprises privées – disposent de capacités techniques avancées permettant de remonter à l'origine d'une cyber opération. Dans le cas de logiciels introduits manuellement, comme cela fût le cas pour Stuxnet, on peut chercher à déterminer l'auteur en analysant la structure du logiciel, les codes utilisés ou encore à l'aide de renseignements humains.

Après être « techniquement » remonté à la source de l'attaque, il s'agit de savoir si le comportement est attribuable à un Etat.

Conformément à l'article 4 du projet d'articles sur la responsabilité des Etats, une cyberattaque sera attribuable à un Etat si elle est le fait d'un de ses organes ; ou le fait d'organes qu'elle a autorisé à exercer des prérogatives de puissance publique, conformément à l'article 5. Ce sera le cas de cyberattaques conduites par les services militaires ou de renseignement par exemple. L'on sait également que certains Etats ont créé des unités spécialisées dans le domaine cyber, rattachés au gouvernement, dont les actions seraient également imputables à l'Etat. Un Etat ne peut se dédouaner de sa responsabilité en argumentant que ses organes ont agi au-delà de leurs fonctions ; le droit international considère que l'Etat est responsable même lorsque ses organes agissent *ultra vires*.

Il reste que la plupart des cyber-opérations, si ce n'est toutes, ne sont pas conduites publiquement par les organes d'un Etat. Généralement, l'auteur d'une cyber-opération cherche à masquer son identité. Les Etats n'échappent pas à cette affirmation et chercheront le plus souvent à rester anonyme afin d'éviter toute forme de réponse de la part de l'Etat victime. Dans ce cas, l'article 8 du projet d'articles relatif à la responsabilité des Etats trouve à s'appliquer. Si les auteurs d'une cyberattaque agissent sur les instructions ou directives ou sous le contrôle d'un Etat, leur comportement sera attribué à cet Etat. Dans le cyberespace, l'usage de « *proxies* » ne constitue donc pas un obstacle à la mise en jeu de la responsabilité d'un Etat.

La règle a notamment été adaptée dans le Manuel de Tallinn (2.0) qui dispose que « les cyber-opérations conduites par un acteur non-étatique sont attribuables à un Etat lorsqu'elles sont

engagées sur les instructions ou sous la direction ou le contrôle de cet Etat ». Il s'agit par exemple d'entreprises privées qui seraient engagées pour mener des cyber-opérations hostiles ou le fait pour un Etat d'encourager ses ressortissants à s'engager dans de telles opérations et à leur fournir les moyens techniques pour le faire.

Dans sa stratégie nationale de cyberdéfense, la France a rappelé que la responsabilité d'un Etat pour un fait internationalement illicite peut être engagée par les actes de ses organes mais aussi ceux « d'acteurs non-étatiques si l'Etat exerce une forme de contrôle sur les auteurs de l'attaque ». Néanmoins, comme le note Delerue, on peut regretter le manque de précision « sur le niveau de contrôle que devrait exercer l'Etat pour que les actes d'un acteur privé lui soient attribuables »[95].

Il a été avancé par certains auteurs que le test du contrôle « général » était préférable dans le cas des cyber-activités, en raison de la difficulté technique à identifier les auteurs. Il serait trop facile pour les Etats de se dédouaner de leur responsabilité dans le cadre de cyber-attaques si le standard de l'arrêt Nicaragua était utilisé ; il faudrait placer le curseur de responsabilité dès qu'un Etat exerce le contrôle global sur les attaques. D'autres avancent au contraire qu'en raison des problèmes d'identification, le test du contrôle effectif est préférable, puisqu'il permet de ne pas accuser trop rapidement un Etat d'être derrière telle ou telle attaque. Cela est particulièrement important dans le cyberespace, compte tenu de la facilité pour l'auteur d'une attaque de se retrancher derrière les ordinateurs de d'autres individus ou de faire croire à tort que tel ou tel groupe ou Etat est à l'origine de l'opération. Il semble donc qu'il faille privilégier le standard du contrôle effectif lorsque l'on cherche à savoir quel degré de contrôle est nécessaire pour que le comportement d'un groupe d'individus ou d'une entité soit attribuable à un Etat.

Enfin, une cyberattaque pourra être attribuée à un Etat si celui-ci reconnaît et adopte ces actions comme étant les siennes. Concrètement, si un groupe d'individus s'engage dans des cyberattaques à l'encontre d'un Etat A, et que l'Etat B approuve tacitement ces attaques, elles ne lui sont pas pour autant attribuables. En revanche, s'il met à disposition ses services (de renseignement, militaires ou sa division cyber) à ce groupe afin de l'aider à perpétrer les

[95] François Delerue, « le droit international dans la 'stratégie nationale de la cyberdéfense' », *Institut de recherche stratégique de l'école militaire (IRSEM*), Note de recherche n°58, 2018, p.3.

attaques ou pour le protéger contre des contre-opérations, alors, l'on considère qu'il a fait sien ces actes et qu'ils lui sont donc attribuables, tout comme s'il les approuve explicitement.

Il reste encore une question à laquelle il faut répondre, à savoir le degré de certitude nécessaire pour attribuer un acte à un Etat. Il s'agit d'une question de preuve, qui est particulièrement importante lorsque l'on analyse l'attribution des cyberattaques.

Aucun seuil n'est précisément fixé par le droit international ou les articles relatifs à la responsabilité des Etats. Néanmoins, un standard développé par le Tribunal arbitral pour l'Iran et les Etats-Unis (Iran-United States Claims Tribunal – IUSCT) dans une décision de 1987 est généralement repris par la doctrine[96]. Le Tribunal a déclaré que pour attribuer un acte à un Etat, il est nécessaire d'identifier avec une « certitude raisonnable » les auteurs et leur lien avec l'Etat.

Ainsi, le Manuel de Tallinn mentionne que le simple fait qu'une cyber-opération soit lancée ou trouve son origine dans les cyber-infrastructures d'un Etat ne constitue pas une preuve suffisante pour attribuer l'opération à cet Etat, même si cela peut constituer un indice quant à l'association de l'Etat avec ladite opération. Un tel indice reste insuffisant, et il faudra d'autres éléments pour corroborer l'affirmation selon laquelle tel ou tel Etat est responsable d'une cyber-opération.

Comme le souligne Geiss[97], il semble que plus l'acte en question est grave – et ouvre donc la possibilité de réponses plus violentes – plus le standard de preuve requis est élevé. Ainsi, un Etat qui en accuse un autre d'avoir commis un acte équivalant à une agression armée devra prouver avec plus de certitude ses allégations que s'il faisait valoir que l'Etat a seulement commis une violation minime de sa souveraineté.

Il convient maintenant de se tourner vers les réponses qu'offre le droit international à l'Etat victime d'une cyberattaque, en présumant que ces attaques sont attribuables ou imputables à un Etat.

---

[96] Yeager v. Iran, *IUSCT*, Case N. 10199, §37.

[97] Geiss/Lahmann, "Freedom and security in cyberspace: shifting the focus away from military responses towards non-forcible countermeasures and collective threat prevention" *in Peacetime Regime for State Activities in Cyberspace, K. Ziolkowski (ed.), 2013,* p. 624.

Chapitre 2 : Les réponses disponibles contre une cyberattaque équivalant à un usage prohibé de la force

Le droit international propose aux Etats victime d'un acte hostile, conduit par des moyens cyber ou non, un éventail de réponses. Celles-ci varient en fonction de la gravité de l'acte. Nous nous intéresserons dans un premier temps aux réponses disponibles contre une cyberattaque équivalant à un usage prohibé de la force.

Lorsqu'une cyberattaque atteint le niveau de gravité d'une agression armée, l'Etat victime est en droit, sous certaines conditions, de recourir à la légitime défense. Ces cas constituent une exception, et la plupart du temps, l'Etat ne sera autorisé qu'à recourir à des contre-mesures ou à plaider sur la base de l'état de nécessité, là encore, sous certaines conditions, qui seront examinées ci-après.

Un Etat peut également avoir recours au système de sécurité collective mis en place par la Charte des Nations Unies et faire appel au Conseil de Sécurité pour prendre des mesures.

La Charte des Nations Unies fait du principe de prohibition de l'usage de la force un des piliers des relations entre les Etats. Le principe est également reconnu en droit international coutumier et une partie toujours plus grande de la communauté internationale tend à lui reconnaître le caractère de *jus cogens*.

Il reste que la Charte elle-même prévoit des exceptions au principe de prohibition de l'usage de la force dans deux cas. Le Conseil de sécurité peut, conformément aux articles 39 et suivants, prendre des mesures à l'encontre d'un Etat lorsqu'il existe une menace contre la paix, une rupture de la paix ou un acte d'agression, y compris des mesures militaires. La seconde exception est celle de l'exercice du droit de légitime défense.

I. Le recours à la légitime défense

Le droit pour un Etat de recourir à la légitime défense est codifié dans l'article 51, qui dispose que :

> *« 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 ».*

Le droit de légitime défense est également reconnu comme droit coutumier, ainsi que l'a réaffirmé la Cour internationale de Justice dans l'arrêt sur les *Affaires militaires et paramilitaires au Nicaragua*, qui existe à côté de la norme de l'article 51 et dont le contenu n'est pas nécessairement identique[98]. Cette affirmation est renforcée par le texte même de l'article 51 qui parle d'un droit « naturel » (en anglais « *inherent right* »).

Il est donc possible de faire usage de la force en réponse à une agression armée. Puisque le droit international ne s'intéresse pas aux moyens par lesquels il est fait usage de la force – armes traditionnelles, chimiques, biologiques ou cyber – il est donc *a priori* possible de recourir à des cyberattaques en réponse à une agression armée[99]. Cela amène à se poser plusieurs questions : qu'est-ce qu'une agression armée ? Une cyberattaque peut-elle être qualifiée d'agression armée ? Peut-on répondre à une agression armée menée par des moyens traditionnels à l'aide de moyens cyber ? Si oui, à quelles conditions ?

A. Agression armée dans le cyberespace

1. La notion d'agression armée en droit international

La notion « d'agression armée » au sens de l'article 51 ne bénéficie pas d'une définition dans la Charte. En revanche, d'autres documents nous donnent des indications sur la façon dont le terme doit être interprété, ainsi que la Cour internationale de Justice ou la pratique des Etats.

A partir de 1967, les Etats ont cherché à adopter une définition de l'agression non pas au sens de l'article 51 de la Charte, mais plutôt de l'article 39, qui prévoit que le Conseil de Sécurité

[98] Activités militaires et paramilitaires au Nicaragua et contre celui-ci (Nicaragua c. Etats-Unis d'Amérique), fond, Arrêt, C.I.J. Recueil 1986, p. 14. §176.
[99] Voir par exemple Y. Dinstein, "Computer network attacks and self-defense" in *Computer Network attacks and international law*, Naval War College, 2002, p. 103.

peut constater l'existence « d'une menace contre la paix, d'une rupture de la paix ou d'un acte d'agression » et prendre des mesures pour y remédier. La confusion vient de la rédaction de la Charte en français, qui utilise le terme « d'agression » dans l'article 39 (*aggression* en anglais ; *agresion* en espagnol) ; et « d'agression armée » à l'article 51, là où le texte anglais emploie le terme « *armed attack* » et le texte espagnol « *ataque armado* ».

Les débats ont finalement abouti à l'adoption d'une résolution en 1974[100] qui définit l'agression (au sens de l'article 39) comme

> *« L'emploi de la force armée par un Etat contre la souveraineté, l'intégrité territoriale ou l'indépendance politique d'un autre Etat, ou de toute autre manière incompatible avec la Charte des Nations Unies ».*

Il est également précisé que l'emploi de la force armée doit revêtir une certaine gravité. Sont ensuite donnés certains exemples de ce que peut constituer une agression. Juridiquement non-contraignante, on peut lui attribuer le caractère de *soft-law*, puisque les Etats dans leur pratique internationale se réfèrent pour une grande partie à cette résolution. L'agression armée au sens de l'article 51 ne correspond pas exactement à cette définition mais la résolution permet de donner une orientation importante sur ce que constitue une attaque armée.

Dans l'arrêt des *Activités militaires et paramilitaires au Nicaragua*, la Cour souligne que l'agression armée constitue une des « formes les plus graves » de l'usage de la force[101]. Pour qu'une opération soit qualifiée d'agression armée, il faut se référer à ses « effets et ses dimensions ». Dans le cadre de cet arrêt, la Cour explique par exemple qu'un « simple incident de frontières » ne saurait être qualifié d'agression armée[102]. De la même manière, la fourniture d'armements ou le soutien logistique et financier à un groupe ne suffit pas à caractériser l'agression armée – bien que cela puisse constituer un usage de la force au sens de l'article 2(4) ou au moins une violation du principe de non-intervention[103].

La notion d'agression armée tend ainsi à être interprétée de façon restrictive. Cela est justifié par le fait qu'une agression armée ouvre le droit pour un Etat d'avoir recours à la force en

[100] AG/Res/3314 (XIX).
[101] Activités militaires et paramilitaires au Nicaragua et contre celui-ci (Nicaragua c. Etats-Unis d'Amérique), fond, Arrêt, C.I.J. Recueil 1986, p. 14. §191.
[102] *Ibid*, §195.
[103] *Ibid*, §242.

réponse. Puisque la Charte des Nations Unies vise en premier lieu à prévenir et à éviter toute violence et escalade dans les relations entre Etats, il est justifié que seules les attaques les plus graves ouvrent le droit de recourir à la force[104].

Au vu de la pratique des Etats, l'on peut considérer que sera qualifié d'agression armée un acte ayant pour effet d'entraîner la destruction de biens ou des pertes en vies humaines, généralement opéré par des moyens militaires, même si ce dernier critère doit être interprété de façon souple. Ainsi, le seul recours aux armes ou à des techniques militaires ne suffit pas ; par exemple, une attaque lancée dans une zone vide et dénuée de population ne sera pas qualifiée d'agression armée au sens de l'article 51 de la Charte, puisqu'il lui manque le caractère de gravité généralement associé à la destruction de biens et aux pertes en vies humaines. Dans sa stratégie nationale de cyberdéfense, la France parle ainsi d'agression armée lorsqu'il y a « des pertes en vies humaines substantielles ou des dommages physiques aux biens considérables »[105].

Le critère « d'effets et de dimensions » n'étant pas toujours simple à pratiquer, certains auteurs proposent d'avoir recours au concept d'infrastructures vitales ou critiques (*critical infrastructure*) comme indice pour la qualification d'agression armée[106]. Ce concept est utilisé par de nombreux pays, en particulier dans les discussions concernant la cybersécurité des Etats. Bien que les interprétations varient quant à ce que recoupe le concept d'infrastructures vitales, on peut les définir comme des infrastructures essentielles au fonctionnement d'un Etat et de son économie. Cela inclut les télécommunications, le secteur de l'énergie, de la banque, de la finance, du transport, de l'alimentation et des ressources en eau ou encore des services de secours et de santé publique. L'incapacité ou la destruction des systèmes informatiques dans ce secteur peuvent avoir un impact sur la sécurité, l'économie ou la santé d'une nation et de ses citoyens.

Bien que le critère semble à première vue intéressant et facilement transposable pour déterminer si un acte constitue une agression armée, il risque d'étendre indûment la notion d'agression

[104] N. Melzer, « Cyberwarfare and international law », *UNIDIR*, 2011, p. 12
[105]SGDSN, « Stratégie nationale de cyberdéfense », *Editions Economica*, 2018, p. 100. ; passage souligné par l'auteur.
[106] N. Melzer, "Cyberwarfare and international law", *UNIDIR*, 2011, p.14 ; M. Benatar, "The use of cyberforce: need for legal justification ?", *Göttingen Journal of International Law* 1, 2009, p. 393.

armée, qui est censée être réservée pour les actes les plus graves. Certes, le fait qu'une attaque vise une infrastructure considérée comme vitale pour la sécurité ou l'économie d'un Etat peut constituer un indice quant à sa gravité ; mais cela ne doit pas remettre en cause l'exigence de pertes en vie humaines ou de destruction de biens pour la qualification d'agression armée[107]. Le fait qu'aucun consensus n'existe au sein de la communauté internationale quant à ce qui constitue une infrastructure nationale vitale augmente trop le risque d'abus dans la caractérisation d'attaques comme agressions armées.

Enfin, il semble qu'un acte ne sera qualifié d'agression armée que si les conséquences graves qui lui sont associées – destruction de biens et/ou pertes en vies humaines – revêtent un lien causal direct. Une opération qui résulte *in fine* dans la perte en vie humaines ou des dégâts causés à des biens mais seulement de façon indirecte ne satisferait pas à la définition de l'agression armée.

Dans plusieurs affaires, les Etats ont eu recours à la théorie de l'accumulation d'évènements (ou « *pin prick theory* ») pour justifier le recours à la légitime défense. Selon cette théorie, certains actes pris individuellement n'équivalent pas à une agression armée, mais considérés ensemble, ils atteignent un degré de gravité suffisant pour justifier le recours à la force de l'Etat victime.

La Cour internationale a été confrontée à l'argument dans l'affaire des *Activités militaires et paramilitaires au Nicaragua*. Il était question de savoir si différentes incursions sur le territoire du Honduras et du Costa Rica, attribuables au gouvernement du Nicaragua, pouvaient constituer une agression armée. La Cour est restée évasive en déclarant ne disposer que de « très peu d'informations sur les circonstances de ces incursions ou les motifs qui ont pu les inspirer, de sorte qu'il est difficile de décider si à des fins juridiques, elles peuvent être considérées soit ensemble soit isolément comme une agression armée »[108]. Sans affirmer explicitement que des actes pris ensemble puissent constituer une agression armée, la Cour ne l'a néanmoins pas écarté.

[107] F. Dittmar, „Angriffe auf Computernetzwerke", *Schriften zum Völkerrecht, Band 159, Duncker und Humboldt*, 2005, p.156.
[108] Activités militaires et paramilitaires au Nicaragua et contre celui-ci (Nicaragua c. Etats-Unis d'Amérique), fond, Arrêt, C.I.J. Recueil 1986, p. 14, §231.

L'argument fût à nouveau avancé par les Etats-Unis dans l'Affaire des *Plates-formes pétrolières*[109]. Encore une fois, la Cour rejette la qualification d'agression armée dans le cas présent, faute de preuves suffisantes, mais elle admet implicitement que des actes « même pris conjointement » puissent être qualifiés d'attaque armée déclenchant le droit de légitime défense[110]. La France a admis explicitement reconnaître la théorie de l'accumulation, notamment dans sa stratégie de cyberdéfense[111].

Le texte de l'article 51 ne fait pas référence à l'origine de l'agression armée et déclare seulement que les Etats ont un droit naturel de légitime défense lorsqu'ils font l'objet d'une agression armée. Au contraire, l'article 2(4) pose une interdiction à destination des Etats de recourir à la force. De la même façon, le texte de la résolution 3314 définit l'agression comme étant le fait d'un Etat. Il faut toutefois garder en tête que la définition de l'agression renvoie au terme de l'article 39, et non de l'article 51 (*armed attack*/agression armée).

Comment l'agression armée est-elle à interpréter dans ce contexte ? Doit-elle émaner d'un Etat, puisqu'elle constitue également un usage illicite de la force au sens de l'article 2(4), ou l'article doit-il être considéré indépendamment, de sorte qu'une agression armée au sens de l'article 51 puisse être le fait d'un groupe non-étatique ?

Si à l'époque de la rédaction de la Charte, il semblait peu probable qu'une opération de la gravité d'une agression armée soit le fait d'un groupe non-étatique, il s'agit désormais d'une réalité en droit international. En particulier depuis les attaques du 11 septembre, les groupes terroristes internationaux ont prouvé qu'ils étaient capables de coordonner des opérations de la même manière qu'un Etat, posant la question de leur qualification comme agression armée au sens de l'article 51 de la Charte.

Dans son arrêt sur les *Activités militaires et paramilitaires au Nicaragua*, la Cour a précisé qu'une agression armée n'est pas nécessairement le fait des forces armées régulières d'un Etat, mais peut aussi s'entendre de « l'envoi par un Etat ou en son nom de bandes ou de groupes armés, de forces irrégulières ou de mercenaires qui se livrent à des actes de force armée contre

[109] Plates-formes pétrolières (République Islamique d'Iran c. Etats-Unis d'Amérique), arrêt, C.I.J. Recueil 2003, p.161.
[110] *Ibid*, §64.
[111] SGDSN, « Stratégie nationale de la cyberdéfense », *Editions Economica*, 2018, p. 101.

un autre Etat d'une gravité telle qu'ils équivalent entre autres à une véritable agression armée accomplie par des forces régulières, ou au fait de s'engager d'une manière substantielle dans une telle action »[112]. Ainsi, si un Etat exerce le contrôle sur un groupe d'individus qui commet des actes atteignant le seuil de gravité de l'agression armée, cet acte sera attribuable à l'Etat commanditaire.

En dehors de ces cas aisément solubles, la question de savoir si un acte attribuable uniquement à un groupe non-étatique peut constituer une agression en droit international demeure controversée. Traditionnellement, le droit de légitime défense tel qu'envisagé par la Charte mais aussi par le droit coutumier ne s'entendait que d'une riposte contre un acte d'un Etat. De plus, la Cour internationale de Justice dans un avis de 2004 a déclaré que « L'article 51 de la Charte reconnaît ainsi l'existence d'un droit naturel de légitime défense en cas d'agression armée par un Etat contre un autre Etat »[113]. De même, dans son arrêt sur l'*Affaire des activités armées sur le territoire du Congo*, la Cour semble exclure la qualification d'agression armée puisque les opérations n'étaient pas le fait des forces armées de la RDC ; il manquait des éléments de preuve concernant « l'implication directe ou indirecte du Gouvernement de la RDC »[114].

Toutefois, les attentats du 11 septembre contre les Etats-Unis marquent un tournant. Le Conseil de Sécurité, dans une résolution adoptée au lendemain des attentats[115], qualifie les évènements comme « une menace à la paix et à la sécurité internationale ». Quelques jours plus tard, le Conseil adopte une nouvelle résolution[116] qualifiant les actes terroristes en général de menace à la paix et à la sécurité internationale et réaffirme le droit de légitime défense dans ce contexte.

Le gouvernement américain s'est à l'époque déclaré prêt à engager des actions contre des « organisations et des Etats dans le cadre de [notre] droit de légitime défense »[117]. De la même façon, suite aux attentats perpétrés par le groupe Daech en France en 2015, le gouvernement de

[112] Activités militaires et paramilitaires au Nicaragua et contre celui-ci (Nicaragua c. Etats-Unis d'Amérique), fond, Arrêt, C.I.J. Recueil 1986, p. 14, §195.
[113] Conséquences juridiques de l'édification d'un mur dans le territoire palestinien occupé, avis consultatif, CIJ, Recueil 2004, p.136, §139. Souligné par l'auteur.
[114] Activités armées sur le territoire du Congo (République démocratique du Congo c. Ouganda), arrêt, C.I.J. Recueil 2005, p. 168, §146.
[115] SC/Res/1368.
[116] SC/Res/1373.
[117] Lettre datée du 7 octobre 2001, adressée au Président du Conseil de sécurité par le Représentant permanent des États-Unis d'Amérique auprès de l'Organisation des Nations Unies, S/2001/946.

l'époque a fondé la légalité de frappes aériennes sur le territoire syrien sur le droit de légitime défense conformément à l'article 51 de la Charte des Nations Unies[118].

Ces argumentations ont été critiquées par de nombreux auteurs, faute d'une base juridique certaine. L'on pourrait argumenter que la pratique des Etats a enrichi le texte de la Charte, mais la question demeure épineuse et la possibilité de caractériser un acte d'un groupe non-étatique d'agression armée déclenchant le droit de légitime défense demeure contesté au sein de la communauté internationale.

En conclusion, on peut définir l'agression armée comme un usage de la force armée contre un Etat, ayant pour conséquences la destruction de biens ou des pertes en vies humaines, ou des effets d'une gravité semblable, constitué par un ou plusieurs actes commis par un Etat et, dans certaines circonstances, des groupes non-étatiques.

2. Cyberattaques équivalant à une agression armée

Maintenant que nous avons mieux cerné ce que recoupe la notion d'agression armée, il convient d'examiner si une cyberattaque peut être qualifiée comme telle.

L'article 51 ne fait référence à aucune arme en particulier ; il semble donc qu'il n'y ait pas de différence selon que l'attaque soit menée par des moyens traditionnels ou des moyens cyber[119]. C'est également la conclusion que tirent les rédacteurs du Manuel de Tallinn, qui proposent d'employer les critères de dimension et d'effets pour savoir quand une cyberattaque équivaut à une agression armée. La règle 13 est formulée de la façon suivante : « Un Etat qui est la cible d'une cyber opération d'un niveau équivalent à une attaque armée peut exercer son droit naturel de légitime défense. La question de savoir si une cyber opération atteint le niveau d'une agression armée dépend de ses dimensions et de ses effets »[120].

---

[118] Voir par exemple la Déclaration de M. Manuel Valls, Premier ministre, et l'intervention de M. Jean-Yves Le Drian, ministre de la défense, sur l'engagement des forces aériennes en Syrie, à l'Assemblée nationale le 15 septembre 2015 : « Nous devons mieux identifier et localiser le dispositif de Daech pour être en mesure de le frapper sur le sol syrien et d'exercer ainsi - je veux le souligner tout particulièrement - notre légitime défense, comme le prévoit l'article 51 de la Charte des Nations unies ».

[119] M. Roscini, « World Wide Warfare - *Jus ad bellum* and the Use of Cyber Force », *Max Planck Yearbook of United Nations Law, Vol. 14*, 2010, p. 106.

[120] Tallinn Manual, Rule 13: « A State that is the target of a cyber operation that rises to the level of an armed attack may exercise its inherent right of self-defence. Whether a cyber operation constitutes an armed attack depends on its scale and effects ».

Le groupe a majoritairement écarté l'approche instrumentaliste selon laquelle une attaque armée doit nécessairement être menée au moyen d'une arme militaire et reprend à son compte les conclusions de la Cour internationale de Justice dans son avis sur la *Licéité de la menace ou de l'emploi d'armes nucléaires*. Le choix des moyens est indifférent à la qualification d'agression armée. Le groupe souligne que l'emploi d'armes chimiques, biologiques ou radiologiques n'a jamais fait obstacle à la qualification d'agression armée, quand bien même il ne s'agit pas de moyens cinétiques ; et qu'il devrait en être de même pour le recours à des moyens cyber[121]. Ce n'est pas la dénomination d'un appareil, ni son usage normal qui en fait une arme, mais l'intention avec laquelle il est utilisé et son effet. Ainsi, l'usage de n'importe quel appareil qui résulte en des pertes en vies humaines et/ou la destruction de biens doit être considéré comme remplissant les conditions d'une agression armée[122].

En pratique, une cyber-attaque causant une gêne importante, sans pour autant aller jusqu'à entraîner la destruction de biens ou des pertes en vie humaines pourrait constituer un usage de la force, mais ne sera pas qualifié d'agression armée. Seule une cyberattaque atteignant ces effets sera à même d'être qualifiée d'agression armée et de déclencher le droit de l'Etat victime à recourir à l'usage de la force en légitime défense.

Il s'agit également de la vue adoptée par les Etats-Unis. Daniel Silver, ancien Conseiller général de la CIA et de la NSA a ainsi déclaré qu'une cyberattaque constitue une agression armée « si les conséquences prévisibles de l'attaque sont de causer des dommages physiques ou des dommages aux biens et seulement si la gravité de ces conséquences ressemble aux conséquences associées à la coercion armée »[123].

Ainsi, une cyberattaque menée contre les systèmes de contrôle aérien visant à causer des crashs serait regardée comme une agression armée puisqu'une telle attaque a pour conséquences prévisibles des pertes en vies humaines et la destruction de biens.

[121] Tallinn Manual, Commentary on Rule 13, §3.
[122] Karl Zemanek, "Armed attack", in Rüdiger/Wolfrum (ed.), *Max Planck Encyclopedia of Public International Law*, 2013, § 21.
[123] Daniel B. Silver, "Computer Network Attacks as a Use of force under Article 2(4) of the United Charter", in M. Schmitt/BT O'Donnell (eds), *Computer Network Attacks and international Law*, 2002, p.90: "only if its foreseeable consequence is to cause physical injury or property damage and, even then, only if the severity of those foreseeable consequences resembles the consequences that are associated with armed coercion."

La question de savoir si une cyberattaque constitue une agression armée au sens de l'article 51 lorsque ses conséquences ne sont pas de nature physique est controversée. Par exemple, une cyberattaque visant des centres financiers ne résultera pas directement en des dommages physiques sur des biens ou des individus, même s'ils peuvent indirectement se manifester en raison des cyberattaques. Pour les tenants d'une approche basée sur la cible de l'attaque, à partir du moment où une cyberattaque vise une infrastructure dite critique et cherche à la rendre hors d'usage, elle peut être qualifiée d'agression armée, qu'elle donne lieu ou nom à des dommages physiques.

Néanmoins, comme expliqué ci-haut, l'approche basée sur les cibles présente plusieurs inconvénients, qui se manifestent également lorsque l'on cherche à qualifier une cyber-opération d'agression armée. Elle risque d'englober trop d'opérations dont les conséquences ne sont pas suffisamment graves et directes. Une cyberattaque dont les conséquences directes seraient seulement économiques par exemple ne devrait pas être qualifiée agression armée et ne doit pas permettre de réponse en légitime défense de la part de l'Etat victime.

La théorie de l'accumulation des effets est particulièrement intéressante dans le cadre du cyberespace. De nombreuses attaques, en particulier les attaques par déni de service, ne peuvent pas individuellement causer de dommages sérieux. Toutefois, une série de cyberattaques dirigées contre un même Etat et menées de façon coordonnée peuvent être considérées collectivement et ainsi atteindre le seuil d'une agression armée au sens de l'article 51, alors même que prises individuellement, elles seraient considérées comme de trop faible ampleur. Les experts du Manuel de Tallinn ont également adopté cette position en considérant que si les attaques avaient la même origine ou étaient menées de concert, elles peuvent atteindre le seuil d'agression armée considérées collectivement[124].

A titre d'illustration, on peut imaginer une cyberattaque visant à interrompre le fonctionnement d'une centrale électrique. Si cela constitue probablement un usage prohibé de la force, on peut douter que les Etats aillent jusqu'à qualifier la cyberattaque d'agression armée justifiant le recours à la légitime défense. En revanche, une série de cyberattaque visant à mettre hors d'usage tous les sites de production électrique d'un Etat seraient sûrement considérées comme

[124] Tallinn Manual, Commentary on Rule 13, §8.

une attaque armée puisque les conséquences cumulées sont particulièrement graves et ont le potentiel pour causer la destruction de biens ou des pertes en vies humaines.

La question de l'origine de l'agression armée mérite d'être éclaircie. Il semble aujourd'hui inévitable de reconnaître qu'une agression armée peut être le fait d'un acteur non-étatique, en particulier compte tenu de l'essor des opérations hostiles dans le cyberespace. Sans parler de la question de l'attribution d'actes de groupes non-étatiques à un Etat, il est probable que des groupes indépendants parviennent à mener des cyberattaques entraînant la destruction de biens et la mort d'individus qui comme telles ont le potentiel d'être qualifiées d'agression armée au sens de l'article 51. C'est également la conclusion à laquelle est parvenue une majorité des experts du Manuel de Tallinn, bien qu'aucun consensus n'ait été trouvé. Si une cyberattaque menée par un groupe d'individus est similaire dans son étendue et ses effets à une attaque classique et si elle vise un Etat, elle peut être qualifiée d'agression armée et déclencher le droit de l'Etat victime à réagir en légitime défense[125].

Dans le cadre des attaques ayant visé l'Estonie en 2007, le gouvernement a renoncé à caractériser les attaques d'agression armée au sens de l'article 51 mais a également renoncé à activer la clause de l'article 5 du Traité de l'Atlantique Nord qui prévoit qu'une attaque armée contre un des Etats membres de l'OTAN constitue une attaque armée contre tous les membres, déclenchant la possibilité pour les Etats d'avoir recours à l'emploi de la force dans le cadre du droit de légitime défense individuel et collectif tel que reconnu par l'article 51. Cela semble en accord avec les critères d'ampleur et d'effets : les attaques n'ont finalement occasionné qu'une « gêne » et n'ont causé aucun dommage affectant des biens ou des individus. Même prises dans leur globalité, de façon agrégée, les cyberattaques n'ont pas atteint un seuil de gravité suffisant pour déclencher le droit de légitime défense.

La question a été en revanche plus débattue s'agissant du virus Stuxnet ayant visé l'Iran. Certes, le virus n'a pas causé de destruction ou de pertes en vies humaines et a seulement handicapé le bon fonctionnement des centrales visées. Néanmoins, certains auteurs, y compris au sein des rédacteurs du Manuel de Tallinn[126], considèrent que le degré de sophistication du virus était tel

[125] Michael N. Schmitt, "International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed", *Harvard International Law Journal, Vol. 54*, 2012, p. 24.
[126] Tallinn Manual, Commentary on Rule 13, §13.

qu'il équivalait à une arme militaire de pointe. De plus, l'attaque visait ce que l'on peut considérer comme étant une infrastructure critique pour la sécurité nationale. Toutefois, dans un souci de cohérence avec les objectifs de la Charte, l'emploi de *Stuxnet* ne devrait pas être qualifié d'agression armée. Bien que le logiciel ait eu le potentiel d'infliger des dommages sévères et graves, ces conséquences ne se sont pas produites. Etendre la qualification d'agression armée a des faits « ayant le potentiel de » mais qui ne causent pas de pertes en vies humaines ou de dégâts substantiels reviendrait à trop étirer la notion et présente un risque d'escalade si des mesures incluant l'usage de la force sont prises en réponse.

Même si aucune attaque à ce jour n'a été qualifié d'agression armée permettant à un Etat de prendre des mesures de légitime défense, ce scénario n'est pas totalement surréaliste. Les développements qui suivent s'intéressent ainsi à l'exercice du droit de légitime défense dans le cyberespace.

B. Légitime défense dans le cyberespace

1. L'exercice de la légitime défense en droit international

L'article 51 de la Charte des Nations Unies consacre le droit de légitime défense, qui existe également au rang de droit international coutumier. L'idée qui sous-tend le concept de légitime défense est la protection de l'ordre juridique international, en permettant à un Etat de prendre les mesures nécessaires pour mettre fin à une attaque, même si ces mesures requièrent d'employer la force. L'emploi de la force est ici justifié par les actions illégales de l'Etat à l'origine de l'attaque et par la nécessité pour l'Etat victime d'y mettre fin[127]. La littérature fait souvent remonter la consécration du droit de légitime défense en tant que droit international coutumier à l'Affaire Caroline en 1837.

A l'époque, un mouvement d'indépendance canadien se battait contre les Britanniques. Bien que les Etats-Unis soient officiellement neutres dans ce conflit, certains citoyens apportaient leur aide aux rebelles canadiens, notamment à l'aide de navires, dont le *Caroline*. Celui-ci fût détruit et brulé par l'armée britannique, tuant au passage le capitaine, un citoyen américain. Cet incident est à l'origine d'une crise diplomatique entre les Etats-Unis et le Royaume-Uni, qui donnera lieu à une correspondance entre l'ambassadeur britannique et le secrétaire d'Etat

[127] N. Melzer, "Cyberwarfare and international law", *UNIDIR*, 2011, p. 12.

américain de l'époque, Daniel Webster. En réponse à l'argument des britanniques selon lequel ils auraient agi en légitime défense, Webster répondit dans une formule célèbre que l'Etat qui s'en prévaut doit pouvoir prouver que « la nécessité de légitime défense était instantanée, irrésistible, ne laissant aucun choix dans les moyens ni de moment de délibération »[128].

Cette formule va poser les bases des modalités de mise en œuvre du droit de légitime défense en réponse à une agression armée. Une fois constatée l'agression armée, l'Etat qui souhaite réagir en faisant usage de la force doit respecter deux exigences : sa réponse doit être nécessaire et proportionnelle. Il existe également une dimension temporelle : l'agression armée doit être en cours ou imminente.

a. Nécessité et proportionnalité

L'exigence de nécessité signifie que le recours à la force en légitime défense doit viser à mettre fin à une agression armée en cours ou imminente. L'Etat victime n'a à sa disposition aucune mesure alternative pacifique moins grave et suffisante pour défendre sa souveraineté.

L'exigence de proportionnalité postule que les actes entrepris en réponse à une agression doivent être proportionnés à celle-ci et ne pas aller au-delà de ce qui est nécessaire pour faire cesser l'attaque dont l'Etat est victime. Cette exigence vise à s'assurer que la légitime défense n'est pas un prétexte pour à son tour agresser un Etat ou que les mesures prises ne soient en réalité des mesures de représailles. L'acte de légitime défense ne doit pas être disproportionné au regard du danger actuel ou imminent auquel fait face l'Etat qui s'engage dans l'opération.

Ces exigences valent à titre de droit international coutumier et ont également été rappelées par la Cour internationale de Justice dans l'affaire du *Nicaragua*[129] ainsi que celle des *Plateformes pétrolières*[130].

[128] En anglais : "instant, overwhelming, and leaving no choice of means, and no moment for deliberation".
[129] *Activités militaires et paramilitaires au Nicaragua et contre celui-ci (Nicaragua c. Etats-Unis d'Amérique), fond, arrêt, C.I.J. Recueil 1986*, p. 14, §176.
[130] *Plates-formes pétrolières (République Islamique d'Iran c. Etats-Unis d'Amérique), arrêt, C.I.J. Recueil 2003,* p. 161, §43 ; §74.

b. Imminence et droit de légitime défense anticipée

L'article 51 de la Charte des Nations Unies fait référence à une situation dans laquelle un Etat « est l'objet d'une agression armée ». Cela signifie que l'agression est en cours. Cette même exigence se retrouve dans la formule Webster qui estime que le besoin de se défendre pour l'Etat victime doit être « instantané ».

Il est en revanche des cas où un Etat sait qu'une attaque armée va être lancée de façon imminente, mais celle-ci n'a pas encore eu lieu. Une partie de la doctrine internationale considère que dans ce cas, il n'est pas raisonnable pour un Etat d'attendre la survenance de l'agression et qu'il peut d'ores et déjà agir en légitime défense. On parle alors de légitime défense anticipée (*anticipated self-defence*).

D'autres auteurs, comme Dienstein, proposent une vision nuancée et considèrent qu'un Etat peut agir en légitime défense contre une opération qui a été lancée, mais qui n'a pas encore atteint sa cible et parle de « légitime défense interceptive » (« *interceptive self-defence* »).

Le cas de la légitime défense anticipée n'est pas envisagé explicitement par l'article 51. Une autre partie de la doctrine internationale demeure hostile à cette théorie et maintient que la légitime défense n'est possible qu'une fois que l'agression armée a effectivement été lancée. La Cour internationale de Justice n'a pas tranché la question, et a même explicitement évité d'y répondre dans l'affaire des *Activités militaires et paramilitaires au Nicaragua*[131]. Toutefois, l'idée de légitime défense anticipée est défendue par de plus en plus d'Etats, en premier lieu les Etats-Unis qui l'ont inscrit dans leur stratégie nationale de défense dès 2002[132].

La France, plutôt hostile à cette doctrine dans un premier temps, semble avoir changé d'avis. Elle a ainsi admis dans sa stratégie nationale de cyberdéfense qu'elle pourrait exceptionnellement avoir « recours à la légitime défense en réponse à une agression armée non encore déclenchée mais sur le point de l'être, de façon imminente et certaine, pourvu que l'impact potentiel de cette agression soit suffisamment grave »[133].

[131] *Activités militaires et paramilitaires au Nicaragua et contre celui-ci (Nicaragua c. Etats-Unis d'Amérique), fond, arrêt, C.I.J. Recueil 1986*, p.14, §194.
[132] The National Security Strategy of the United States of America, 2002.
[133] Stratégie nationale de cyberdéfense, p.102.

La légitime défense anticipée ne trouve certes pas d'appui textuel. Néanmoins, en faisant application de l'article 31 de la Convention de Vienne sur l'interprétation des traités, une disposition ne doit pas être prise au sens littéral si le résultat est absurde ou déraisonnable. Or, attendre qu'une attaque se produise pour réagir en légitime défense va à l'encontre même du principe de légitime défense, qui vise à éviter la survenance et la poursuite d'actes hostiles dans les relations internationales. En effet, il semble qu'aucun Etat ne soit prêt à laisser se dérouler une agression armée contre son territoire s'il est certain qu'elle va avoir lieu et qu'elle risque de mettre en péril son existence.

Le droit de recourir à la légitime défense anticipée n'est donc pas clairement entériné, mais la pratique de certains Etats tend à montrer que, sous certaines conditions, il peut être exercé.

En revanche, ce que certains appellent « légitime défense préventive », c'est-à-dire l'exercice de la légitime défense contre des opérations potentielles demeure rejetée par une majorité de la communauté internationale. Etendre la légitime défense à des cas dans lesquels une agression armée pourrait être lancée, sans que cela ne soit certain, étendrait trop le concept de légitime défense et présente un risque pour la paix et la sécurité internationale.

L'acte hostile doit être imminent et, pour reprendre les termes de la formule Webster, ne pas laisser de place aux délibérations. L'exigence d'imminence doit être combinée à celle d'immédiateté de la réponse, c'est-à-dire que l'emploi de la force au titre de la légitime défense doit présenter une connexité temporelle avec l'acte d'agression armée.

c. Légitime défense collective

La légitime défense peut être exercée collectivement, ainsi que le précise l'article 51 de la Charte des Nations Unies. Cela est également une règle de droit coutumier. Pour qu'un Etat exerce la légitime défense au nom d'un autre, il doit y avoir été invité par l'Etat victime de l'agression armée. Il n'existe pas de règle permettant à un Etat de prendre des mesures au titre de la légitime défense pour un autre Etat si celui-ci n'en a pas fait la requête. Cela peut être le fait d'un accord préalable, comme dans le traité de l'Atlantique Nord, ou d'un accord *ad hoc*. L'exercice du droit de légitime défense collectif est également soumis aux conditions de nécessité, de proportionnalité, d'imminence et d'immédiateté.

d. Exercice de la légitime défense sur le territoire d'un autre Etat

Les Etats ont le devoir de respecter la souveraineté des autres Etats. Néanmoins, dans certains cas, un Etat victime d'une cyberattaque équivalente à une agression armée peut vouloir prendre des mesures qui ont une incidence sur le territoire d'un autre Etat, en particulier lorsque l'agression armée est le fait d'un groupe non-étatique. L'Etat victime doit en premier lieu demander l'aide ou le consentement de l'Etat sur le territoire duquel il envisage de prendre des mesures. Si celui-ci décline, deux interprétations sont possibles.

L'Etat victime peut recourir à l'argument selon lequel l'Etat en question n'est pas capable (il ne dispose par exemple pas des compétences techniques) ou ne souhaite pas prendre les mesures nécessaires pour mettre fin à l'agression armée, ce qui autorise l'Etat victime à prendre des mesures qui, dans un autre contexte, pourraient être considérées comme violant la souveraineté de cet Etat. Une seconde option considère que même dans le cadre de la légitime défense, le principe de souveraineté des Etats ne saurait souffrir d'exception. Il faudrait dans ce cas se tourner vers une autre base légale, l'état de nécessité constituant *a priori* la solution la plus satisfaisante[134]. Il n'existe actuellement pas de consensus au sein de la communauté internationale sur la question.

2. L'exercice de la légitime défense dans le cyberespace

Lorsque la force est employée à l'aide de moyens cyber en réponse à une agression armée, au titre de la légitime défense, les conditions détaillées ci-haut doivent être respectées de la même manière que si la réponse était menée par des moyens traditionnels. Ainsi, des cyber opérations équivalant à un usage de la force ne seront légitimes que si elles sont nécessaires et proportionnées.

L'emploi de la force cyber en réponse à une agression armée ne sera légitime que s'il vise à mettre fin à l'agression et qu'il n'existe aucune mesure pacifique permettant à l'Etat victime de se défendre suffisamment, ou que celles-ci ont été mises en œuvre sans succès[135]. Ainsi, si un Etat peut se défendre grâce à des mesures de cyber protection passives telles que des pares-

[134] O. Barat-Ginies, « Existe-t-il un droit international du cyberespace ? », *La découverte*, 2014/1 n° 152-153, p. 209.
[135] Y. Dienstein, "Computer Network Attacks and Self-defence", *International Law Studies*, Vol. 76, p. 109.

feux ; ou des mesures actives en-deçà du seuil de l'usage de la force, il n'est pas fondé à avoir recours à la force au titre de la légitime défense.

L'exigence de proportionnalité vient limiter l'étendue, la durée et l'intensité de l'emploi de la force à ce qui est requis pour mettre fin à l'agression armée[136]. Cela ne signifie pas que la force employée doit être de même ampleur ou de même nature que l'acte qui a donné lieu à la situation de légitime défense. En effet, un Etat peut avoir besoin de mettre plus en œuvre pour se défendre contre une agression ; ou au contraire, un emploi de la force minime peut suffire à mettre fin à l'agression armée. De plus, rien n'impose que l'Etat victime réponde par les mêmes moyens : il est possible de répondre à une attaque cinétique par des moyens cyber, et vice versa, tant que les modalités conditionnant l'exercice de la légitime défense sont respectées[137]. Dans certains cas, on peut même imaginer que les Etats devront prendre des mesures cyber lorsqu'ils veulent exercer leur droit de réponse en légitime défense puisque celles-ci sont susceptibles de mettre fin à l'agression armée en causant moins de dommages que des mesures « traditionnelles ».

Même si le droit n'est pas totalement fixé sur la question, une majorité d'auteurs semble considérer que l'accumulation d'actes hostiles, ne constituant pas indépendamment une agression armée, mais atteignant ce seuil lorsque considérés cumulativement peut donner lieu à un acte unique de légitime défense. Par exemple, une cyber-campagne constituée de multiples attaques par déni de service distribués qui n'équivalent pas à eux seuls à une agression armée peuvent, ensemble, être qualifiés comme tel. L'Etat victime pourra y répondre en lançant contre l'Etat responsable une cyber-offensive unique[138].

L'exercice de la légitime défense suppose en outre que l'agression armée a déjà produit ses effets ou que ceux-ci sont en train de se déployer. Le recours à la force est donc légitime lorsqu'une cyberattaque a déjà produit des effets équivalant à une agression armée ou lorsque ceux-ci se déploient actuellement.

[136] Tallinn Manual, Commentary on Rule 14, §5.
[137] H.H. Koh, "International law in cyberspace", *Harvard International Law Journal*, Volume 54, 2012, p. 4.
[138] Y. Dienstein, "Computer Network Attacks and Self-defence", *International Law Studies,* Vol. 76, p. 109.

Le critère d'imminence de l'attaque doit être interprété avec une certaine souplesse dans le cadre des cyberattaques puisqu'un Etat victime d'une cyber opération peut avoir besoin d'un certain temps pour mettre en œuvre des mesures de légitime défense. De plus, si l'agresseur utilise des bombes logiques, les dommages peuvent se produire bien après que l'opération ait été lancée[139].

Parfois, une opération n'équivaut pas en elle-même à une attaque armée, mais elle vise à préparer une agression armée future, éventuellement au moyen de cyber-opérations. L'exemple type est celui d'une cyberattaque qui vise à mettre hors d'usage les systèmes de contrôle aérien avant de lancer une campagne d'attaques aériennes[140].En ce cas, certains auteurs soutiennent que la légitime défense est possible, de façon anticipée, lorsque trois critères sont réunis : l'opération informatique fait partie d'une opération globale équivalant à une agression armée ; l'opération informatique est une étape irrévocable d'une attaque imminente et probablement inévitable ; l'Etat qui se défend réagit de façon anticipée à l'attaque armée durant la dernière fenêtre de tir. Selon la théorie de la dernière fenêtre de tir (« *last feasible window of opportunity standard* »), un Etat peut agir en légitime défense anticipée contre une attaque armée lorsque l'attaquant est clairement engagé dans le lancement de l'attaque et l'Etat victime va perdre l'opportunité de se défendre effectivement si elle n'agit pas (à un instant T). Le point déterminant est de savoir si le fait de ne pas agir à tel moment T résulte en l'incapacité pour l'Etat de se défendre effectivement une fois l'attaque lancée.

La question de la légitime défense anticipée viendra nécessairement à se poser dans le cadre des cyberattaques, notamment lorsque celles-ci constituent une opération préalable à l'emploi de la force par des moyens traditionnels. L'intrusion d'un virus ou la pénétration d'un réseau n'équivaut pas à une agression armée. La possibilité de répondre à la cyberattaque dépend des circonstances et des informations dont dispose l'Etat, mais il faut que cette première étape indique que l'attaque va se produire avec certitude, et non qu'il s'agisse d'une simple possibilité[141]. Ce critère est déterminant. Pour reprendre l'exemple du Manuel de Tallinn, l'insertion d'une bombe logique dans un système ne sera qualifiée d'attaque armée imminente

139 M. Roscini, « World Wide Warfare - Jus ad bellum and the Use of Cyber Force », *Max Planck Yearbook of United Nations Law, Vol. 14,* 2010, p. 120.
140 Tallinn Manual, Commentary on Article 15, §1.
141 Y. Dienstein, "Computer Network Attacks and Self-defence", *International Law Studies,* Vol. 76, p. 111.

que si les conditions pour son activation sont réunies et que la bombe va effectivement être activée de façon imminente. En revanche, la simple insertion de la bombe logique dans un réseau, laissant la possibilité à son propriétaire de la déclencher ou non ne satisfait pas à la condition d'imminence, il y a encore trop d'incertitude concernant le lancement ou non de l'attaque. L'Etat victime ne peut alors se défendre que durant sa dernière fenêtre de tir, lorsque le fait de ne pas se défendre constitue un réel risque. Il reste que la distinction n'est pas toujours simple à mettre en œuvre en pratique. Il suffit par exemple de penser à Stuxnet, dont les experts croyaient au début qu'il s'agissait d'un logiciel visant à espionner le complexe industriel iranien, sans se douter de ses capacités destructrices.

De plus, certains auteurs considèrent que la formule Webster aménage un champ d'appréciation trop large aux Etats dans leur choix d'employer des mesures au titre de la légitime défense anticipée dans le cadre du cyberespace, ce qui peut mener à des situations d'abus[142]. Les conditions « instant, overwhelming and leaving no choice of means » seraient formulées trop largement pour limiter de façon objective l'appréciation des cyberattaques[143]. Pour limiter les risques d'abus, il faudrait restreindre la légitime défense aux cas dans lesquels une agression armée s'est ou se produit.

Le fait qu'un Etat hostile soit en capacité de lancer des cyber-attaques ne constitue aucunement une raison pour employer la force sous couvert de légitime défense. L'Etat victime doit d'abord venir à la conclusion que la menace s'est transformé en une réelle décision d'attaquer. Il doit également avoir épuisé les autres recours à sa disposition, notamment diplomatiques et éventuellement informer le Conseil de Sécurité de la situation. S'il prend des mesures alors qu'une cyberattaque est seulement possible, il se trouve en violation des règles relatives à la prohibition de l'usage de la force puisqu'à ce jour, la légitime défense préventive n'est pas reconnue en droit international.

Le recours à la légitime défense doit respecter une condition d'immédiateté, c'est-à-dire que l'emploi de la force en légitime défense doit survenir immédiatement après l'agression armée. Ce critère vise à éviter les mesures de représailles. Le critère doit néanmoins être appliqué avec

[142] Voir par exemple S. Schmahl, « Cybersecurity » in Dethloff/Nolte/Reinisch, „Freiheit und Regulierung in der Cyberwelt", *Berichte der Deutschen Gesellschaft für Internationales Recht*, Band 47, C.F. Müller, 2016p. 172.
[143] Dittmar, « Angriffe auf Computernetzwerke *Ius ad bellum* und *ius in bello*", Schriften zum Völkerrecht, Band 159, Duncker & Humboldt, 2004, p.161.

une certaine souplesse dans le contexte cyber, en prenant en compte la proximité entre l'agression et la réponse, le temps nécessaire pour mettre en œuvre les mesures de légitime défense et pour identifier l'auteur de l'attaque. Le Manuel de Tallinn prend également en compte les cas de « cyber-campagnes » qui voient se succéder plusieurs vagues de cyberattaques. Un Etat peut avoir recours à la légitime défense après que les attaques l'ayant visé soient terminées si celles-ci risquent de se reproduire.

Enfin, les mesures de légitime défense ne sont justifiées que tant que l'agression armée persiste ou s'il est certain que d'autres agressions vont suivre.

Au sujet des articles 2(4) mais aussi de l'article 51 de la Charte des Nations Unies, la Cour internationale de Justice a déclaré dans son avis relatif à la *Licéité de la menace ou de l'emploi des armes nucléaires* que « ces dispositions ne mentionnent pas d'armes particulières. Elles s'appliquent à n'importe quel emploi de la force, indépendamment des armes employées »[144].

Ainsi, il semble que rien ne fasse obstacle à l'emploi d'armes traditionnelles en réponse à une attaque armée menée par des moyens cyber, et inversement ; il est possible de répondre par des moyens cyber à une agression armée menée par des moyens traditionnels, à conditions que les règles strictes de légalité de l'usage de la force en légitime défense soient respectées.

On peut souligner l'argument selon lequel une réponse par des moyens cyber est potentiellement moins destructrice qu'une attaque menée par des moyens traditionnels. L'argument est réversible et un emploi de la force par des moyens cyber peut s'avérer plus catastrophique ; mais dans ce cas, il ne répondra pas aux exigences de légalité de la légitime défenses examinées ci-dessus.

II. Les réponses institutionnelles – Rôle du Conseil de sécurité

Un Etat victime d'une agression peut prendre des mesures sur la base de la légitime défense jusqu'à ce que le Conseil de Sécurité « ait pris les mesures nécessaires pour maintenir la paix et la sécurité internationales », conformément à l'article 51 de la Charte. Le Conseil de sécurité dispose également de prérogatives pour faire face aux cyberattaques, qu'elles atteignent le degré d'une agression armée ou non.

[144] Licéité de la menace ou de l'emploi d'armes nucléaires, avis consultatif, C.I.J. Recueil 1996, p. 226, §39.

En effet, l'article 39 permet au Conseil de Sécurité de constater « l'existence d'une menace contre la paix, d'une rupture de la paix ou d'un acte d'agression » et de prendre des mesures impliquant ou non l'usage de la force pour maintenir ou rétablir la paix et la sécurité.

L'agression est définie comme « l'emploi de la force armée par un Etat contre la souveraineté, l'intégrité territoriale ou l'indépendance politique d'un autre Etat ou de toute autre manière incompatible avec la Charte des Nations Unies »[145]. Ainsi, une cyberattaque analogue à l'emploi de la force armée pourra être caractérisée de rupture de la paix ou d'acte d'agression.

Mais conformément à l'article 39, le Conseil de Sécurité est également compétent en cas de menace de rupture de la paix. L'emploi de la force armée n'est pas nécessaire pour qu'il y ait une situation de menace de la paix. Le Conseil de sécurité dispose d'un large pouvoir d'appréciation et donc, de nombreuses cyberattaques – qu'elles atteignent le niveau de gravité de l'usage de la force ou non - pourraient être qualifiées de menace à la paix et autoriser le Conseil de Sécurité à adopter des mesures sur la base des articles 41 et 42 de la Charte des Nations Unies. C'est également la conclusion à laquelle sont parvenus les experts du Manuel de Tallinn (2.0) qui prévoient que le Conseil de sécurité peut déterminer qu'une cyber-opération constitue une menace ou une rupture de la paix ou un acte d'agression et peut autoriser l'adoption de mesures non-violentes – y compris cyber – en réponse. Si celles-ci sont inadéquates, le Conseil peut préconiser l'adoption de mesures incluant l'usage de la force, y compris par des moyens cyber[146].

A ce jour, aucune cyber-opération n'a été décrite par le Conseil de sécurité comme constituant une menace ou une rupture de la paix. Néanmoins, deux menaces ont été labellisées par le Conseil de sécurité comme tel, à savoir le terrorisme international[147] et la prolifération des armes de destruction massive[148]. Il est donc pensable que le Conseil de sécurité déclare certains types de cyber-opérations comme constituant une menace ou une rupture de la paix *in abstracto*,

[145] Définition de l'agression adoptée en Annexe de la résolution 3314 (XXIX) de l'Assemblée Générale, 1974.
[146] Tallinn Manual 2.0, Rule 76 – United Nations Security Council: "Should the United Nations Security Council determine that a cyber operation constitute a threat to peace, breach of the peace, or act of aggression, it may authorise non-forceful measures, including cyber operations, in response. If the Security Council considers such measures to be inadequate, it may decide upon forceful measures, including cyber measures".
[147] SC Res. 1373, UN Doc. S/RES/2001 du 28 septembre 2001.
[148] SC Res. 1540, UN Doc. S/RES/1540 du 28 avril 2004.

par exemple les cyber-opérations de grande ampleur visant des infrastructures nationales vitales pour la population civile.

Le Conseil de Sécurité pourrait également adopter une résolution imposant aux Etats de prendre des mesures dans leur droit interne pour criminaliser les cyberattaques ou pour mettre sur pied des unités dédiées à empêcher de telles opérations d'être menées sur le territoire, de la même façon qu'il a adopté des résolutions pour lutter contre le terrorisme international.

Le Conseil de sécurité, une fois avoir déclaré l'existence d'une menace ou d'une rupture de la paix ou d'un acte d'agression, peut prendre des mesures n'incluant pas l'usage de la force au titre de l'article 41 de la Charte. Ces mesures incluent l'interruption des relations économiques, diplomatiques, mais surtout « l'interruption complète ou partielle des communications ferroviaires, maritimes, aériennes, postales, télégraphiques, radioélectriques et des autres moyens de communication ». Il semble donc que le Conseil de Sécurité puisse prendre pour mesure l'interruption des communications cyber avec un Etat ou un groupe non-étatique.

Si les mesures pacifiques de l'article 41 ne sont pas efficaces, le Conseil de Sécurité peut décider d'avoir recours à des mesures incluant l'usage de la force au titre de l'article 42 de la Charte. Il peut également le faire à l'aide de moyens cyber.

Cela ouvre donc de nouvelles possibilités pour le Conseil de Sécurité lorsqu'il est confronté à une situation de menace ou de rupture de la paix. Désormais, des mesures cyber peuvent être prises en plus des classiques sanctions économiques ou de la rupture des relations diplomatiques[149]. On peut par exemple imaginer un blocus informatique, ou en anglais « *infoblockade* » qui viserait à sanctionner un Etat en le coupant de tout accès aux réseaux des autres Etats. Schmitt souligne également que l'adoption de cyber-mesures, capables d'obtenir certains résultats sans victimes, peut à terme représenter une étape idéale entre l'adoption de mesures pacifiques de l'article 41 et l'adoption de mesures incluant l'usage de la force de l'article 42[150].

[149] Dittmar, "Angriffe auf Computernetzwerke *Ius ad bellum* und *ius in bello*", Schriften zum Völkerrecht, Band 159, Duncker & Humboldt, 2004, p. 184.
[150] M.N. Schmitt, "Computer Network attack: the normative software", *Yearbook of International Humanitarian Law, Vol. 4,* 2001, p. 70.

Néanmoins, il faut garder en tête que le processus de décision au sein du Conseil de sécurité reste lent. De plus, figurent en tant que membres permanents avec un droit de véto les Etats-Unis, la Chine et la Russie qui, malgré leurs dénégations, sont parmi les puissances les plus enclines à avoir recours à des cyberattaques[151].

[151] L. Simonet, "L'usage de la force dans le cyberespace », *Annuaire français de droit international, Vol. 58*, 2012, p. 131.

Chapitre 3 : Les réponses disponibles contre les cyber-attaques n'équivalant pas à une agression armée

Ainsi qu'on l'a vu, le recours à la légitime défense est certes possible, mais demeure très encadré. De plus, il n'est pas nécessairement adapté dans le cyberespace, compte tenu de la rapidité avec laquelle les cyber-opérations sont menées et les ressources dont un Etat à besoin pour identifier la source de l'attaque et l'attribuer à un Etat. Enfin, le fait qu'aucune cyber-attaque n'ait été qualifiée d'agression armée à ce jour démontre que la plupart d'entre elles n'atteignent pas le seuil de gravité nécessaire pour avoir recours à la force armée en réponse. Toutefois, il est difficile de concevoir qu'un Etat victime de cyber-attaques n'ait pas d'autres solutions. C'est pourquoi il faut analyser les réponses que propose le droit international face à ces cyberattaques de plus faible intensité.

Il s'agit en premier lieu de l'adoption de contre-mesures ainsi que du concept de l'état de nécessité.

I. Les contre-mesures

Il est admis en droit international qu'un Etat victime d'un acte international illicite puisse recourir à des contre-mesures.

Les contre-mesures sont des actes n'impliquant pas l'usage de la force pris en réponse à un acte illégal commis par un autre Etat dans le but de l'amener à se conformer avec ses obligations en droit international. Ces actes sont normalement illégaux, mais l'Etat victime est autorisé à y recourir pour mettre fin au comportement illégal d'un autre Etat. En cela, les contre-mesures diffèrent de ce que l'on appelle les mesures de rétorsion, qui bien que non-amicales, sont licites en toutes circonstances.

1. Le régime des contre-mesures en droit international

Pour être licites, les contre-mesures doivent répondre à certaines conditions : elles doivent être prises en réponse à la commission d'un acte international illicite par un Etat et respecter certaines limitations.

Les contre-mesures sont des actes en principe illicites au regard du droit international, mais dont l'illicéité est exclue lorsqu'elles visent à mettre fin à la commission d'un acte international lui-même illicite. Pour qu'un acte soit illicite au regard du droit international, il doit être attribuable à un Etat et constituer la violation d'une obligation internationale de cet Etat, que celle-ci soit issue d'un traité ou du droit international coutumier. Il peut notamment s'agir d'opérations violant le principe de non-intervention comme vu ci haut. L'espionnage par exemple ne donne pas droit à un Etat d'adopter des contre-mesures, puisque ce n'est pas illicite aux yeux du droit international. L'usage de la force, qu'il atteigne ou non le seuil de l'agression armée constitue également de façon évidente un acte international illicite.

Il peut aussi s'agir d'un acte violant la souveraineté d'un Etat ou un le manquement d'un Etat à son obligation de diligence.

Les contre-mesures sont soumises à certaines limitations. Tout d'abord, elles doivent être prises dans le but de faire cesser le comportement illicite de l'Etat qui a violé ses obligations en droit international. Elles ne doivent pas avoir de caractère punitif, et ne peuvent en principe pas être déployées si le comportement illicite a cessé. Elles doivent également permettre de revenir au *statu quo*, et donc, en principe, être réversibles.

Les contre-mesures ne doivent pas porter atteinte au principe de prohibition de l'usage de la force. En effet, un Etat n'est autorisé à utiliser la force que sur autorisation du Conseil de sécurité ou lorsqu'il est victime d'une agression, dans les strictes conditions imposées pour l'exercice du droit de légitime défense. L'article 50 du projet d'articles sur la responsabilité des Etats prévoit aussi qu'elles ne peuvent aller à l'encontre de certaines règles cardinales, en particulier les règles protégeant les droits humains fondamentaux, les règles du droit humanitaire, et les normes impératives de droit international (*jus cogens*). Enfin, elles ne sauraient libérer un Etat de ses obligations quant à la résolution pacifique des différends ou aux règles concernant les agents diplomatiques.

Il est généralement admis au titre du droit coutumier que les contre-mesures doivent respecter une condition de proportionnalité. Cela est repris par les articles sur la responsabilité des Etats, qui disposent à l'article 51 que « Les contre-mesures doivent être proportionnelles au préjudice subi, compte tenu de la gravité du fait internationalement illicite et des droits en cause ». La

condition de proportionnalité ne signifie pas réciprocité, l'Etat qui adopte des contre-mesures n'a pas l'obligation d'adopter le même comportement international illicite que celui qu'il entend faire cesser. Les contre-mesures ne doivent pas non plus nécessairement être de même nature, c'est-à-dire qu'il est possible de répondre à un acte international illicite par des cyber contre-mesures ; ou de répondre à des cyberattaques illicites par des moyens « traditionnels » tels que le non-respect d'un traité conclu avec l'Etat fautif. Simplement, la contre-mesure a plus de chance d'être considérée comme proportionnelle si elle est identique à l'acte international illicite[152].

D'autres conditions sont fixées dans le projet d'articles sur la responsabilité de l'Etat pour fait internationalement illicite, notamment procédurales. L'Etat victime de l'acte international illicite doit demander à l'Etat qui en est à l'origine d'y mettre fin et de se conformer à ses obligations. Si cela est insuffisant, il doit faire part de son intention d'adopter des contre-mesures.

Contrairement à la légitime défense, il n'existe pas de notion de « contre-mesures collectives » qui permettrait à un Etat ne disposant pas des compétences techniques nécessaires de faire appel à des alliés pour l'aider[153]. Ainsi, si les contre-mesures peuvent être un moyen efficace de mettre fin à des cyberattaques pour un pays disposant de capacités cyber avancées, elles seront moins efficaces pour un Etat disposant de peu de moyens[154].

De plus, il n'existe pas aujourd'hui de règle cristallisée en droit international qui permette à un Etat de demander à un autre d'exercer des contre-mesures en son nom. Dans le cadre de la légitime défense, la Cour internationale de Justice a admis qu'un Etat puisse avoir recours à la force, sur la base de la légitime défense, en lieu et place de l'Etat victime de l'agression armée, si ce dernier a explicitement demandé au premier de le faire. Une telle possibilité n'existe pas s'agissant des contre-mesures, et il n'est pas démontré que la pratique des Etats ait entendu créer cette règle.

[152] M.N. Schmitt, "'Below the threshold' cyber operations: The Countermeasures Response Option and International Law, *Virginia Journal of International Law, Vol. 54 (3)* 2014, p. 724.
[153] *Ibid*, p. 731.
[154] S. Li, "When does internet denial trigger the right to armed self-defence", *Yale Journal of International Law*, Volume 38, 2013, p. 213.

Enfin, il n'existe pas d'équivalent à la légitime défense anticipée s'agissant des contre-mesures, puisque celles-ci doivent être prises en réponse à un acte international illicite. Il n'est pas possible de prendre des contre-mesures prospectives[155].

Toutefois, dans certains cas, un Etat peut « prendre les contre-mesures urgentes qui sont nécessaires pour préserver ses droits »[156]. Des contre-mesures peuvent alors être adoptées, sans qu'elles fassent l'objet d'une annonce, afin de prendre l'Etat en faute « par surprise » et l'obliger à se conformer à ses obligations et à mettre fin au comportement illicite. Pour autant, cela ne remet pas en cause la nécessité d'attribuer l'acte à un Etat, simplement, l'Etat victime de l'acte illicite peut exceptionnellement se dispenser des conditions procédurales de négociation et d'annonce[157].

De telles contre-mesures urgentes pourraient par exemple être prises par un Etat qui fait l'objet d'une cyberattaque contre les systèmes informatiques des banques situées sur son territoire. Pour mettre fin à ce comportement, cet Etat décide d'employer des mesures équivalentes et d'attaquer à son tour par des moyens cyber les systèmes informatiques des banques situées sur le territoire de l'autre Etat. S'il annonçait son intention, l'Etat à l'origine de cette situation pourrait mettre à l'abri les actifs financiers dont il dispose et se prémunir contre ces attaques, qui seraient *in fine* ineffectives.

Les rédacteurs du Manuel de Tallinn considèrent également qu'un Etat peut prendre des contremesures, de nature cyber ou non, en réponse à la violation d'une obligation internationale qui lui est due par un autre Etat[158]. Ils soulignent toutefois que les contremesures ne peuvent être prises qu'à l'encontre d'un Etat. Les contremesures ne constituent pas une réponse possible face à un acteur non-étatique, hormis lorsque ses actions sont attribuables à un Etat. Toutefois, ces actions ne sont pas forcément licites, en particulier au regard du droit interne de l'Etat victime.

[155] M.N. Schmitt, "'Below the threshold' cyber operations: The Countermeasures Response Option and International Law, *Virginia Journal of International Law, Vol. 54 (3)* 2014, p. 715.
[156] Article 52 (2) du projet d'articles sur la responsabilité des Etats.
[157] Geiss/Lahmann, "Freedom and security in cyberspace: shifting the focus away from military responses towards non-forcible countermeasures and collective threat prevention" *in Peacetime Regime for State Activities in Cyberspace, K. Ziolkowski (ed.), 2013,* p. 634.
[158] Tallinn Manual 2.0., Rule 20: "A State may be entitled to take countermeasures, whether cyber in nature or not, in response to a breach of an international legal obligation that it is owed by another State".

2. *Les cyber-contre-mesures*

Que peuvent constituer concrètement des contre-mesures dans le cyberespace ? Il est admis que les Etats disposent de défenses passives telles que des pares-feux pour se protéger des cyberattaques. Si un Etat est victime d'une cyber-opération, il peut, sous le régime des contre-mesures, être autorisé à mettre en œuvre des défenses dites « actives », qui visent à mettre hors d'usage l'auteur des attaques[159] ou bien mettre en œuvre des attaques réciproques afin d'inciter l'Etat à l'origine de l'attaque à mettre fin à son comportement. De façon plus radicale, un Etat victime d'une cyberattaque illégale pourrait couper l'accès à ses serveurs et systèmes informatiques jusqu'à ce que les cyberattaques prennent fin.

Il reste néanmoins de nombreux obstacles à l'utilisation des contre-mesures dans le cyberespace. Tout d'abord, pour être efficace, la contre-mesure doit mettre suffisamment sous pression l'Etat à l'origine de l'acte illicite. Or, dans le contexte cyber, il est très facile pour un Etat qui se sait visé par une contre-mesure de prendre ses dispositions pour se protéger, en particulier si l'Etat victime annonce son attention de recourir à des contre-mesures. De plus, les cyber-contre-mesures présentent le risque d'affecter d'autres Etats que celui ayant commis un acte internationalement illicite. Par exemple, une contre-mesure dont l'objet est de désactiver des systèmes et réseaux informatiques risque d'impacter des acteurs qui ne sont en rien responsables et ainsi, de rendre l'Etat en premier lieu victime finalement à son tour responsable d'un acte international illicite vis-à-vis d'un Etat tiers[160]. Enfin, un problème majeur du régime applicable aux contre-mesures est qu'elles ne peuvent être adoptées que si un Etat a commis un acte international licite ; elles n'apportent donc aucune réponse à des actes causés par des groupes non-étatiques et supposent de pouvoir attribuer l'acte international illicite à un Etat.

Un Etat victime d'une cyberattaque conduite par un groupe non-étatique a néanmoins à sa disposition d'autres possibilités, à savoir l'exercice du droit de légitime défense lorsque ces attaques atteignent le seuil d'une agression armée ; ou l'invocation de l'état de nécessité.

[159] O.A. Hathaway/ R. Crootof, "The Law of Cyber-Attack", *California Law Review, Vol. 100,* 2012, p. 858.
[160] O.A. Hathaway/ R. Crootof, "The Law of Cyber-Attack", *California Law Review, Vol. 100,* 2012, p. 859.

II. Actions prises sur la base de l'état de nécessité

Bien que ce concept soit peu utilisé par les Etats, le droit coutumier reconnaît qu'un Etat puisse avoir recours à des mesures en principe illégales, mais dont l'illicéité est écartée lorsqu'il se trouve en état de nécessité. Le projet d'articles sur la responsabilité des Etats prévoit également ce cas de figure et explicite les conditions de sa mise en œuvre.

Un Etat peut violer ses obligations en droit international lorsque cela constitue « le seul moyen de protéger un intérêt essentiel contre un péril grave et imminent » et à la condition de ne pas porter « gravement atteinte à un intérêt essentiel » d'un ou plusieurs Etats.

Les actions qu'un Etat peut prendre sur la base de l'état de nécessité diffèrent des contre-mesures en ce qu'elles n'ont pas besoin de répondre à un acte internationalement illicite d'un autre Etat. Elles ne sont pas dirigées contre un Etat en particulier et peuvent être entreprises même lorsque les évènements qui menacent l'Etat ne sont pas attribuables à un autre Etat. Elles peuvent également constituer des mesures violant les droits d'Etats non-responsables, à la condition de ne pas sérieusement porter atteinte à leurs intérêts.

Comme pour la plupart des règles, celles relatives à l'état de nécessité sont aussi applicables dans le cyberespace. Il s'agit d'un remède particulièrement intéressant lorsque l'on prend en compte le fait que les autres réponses disponibles pour les Etats – légitime défense ou contre-mesures – requièrent de pouvoir identifier et d'attribuer les cyberattaques[161]. Ainsi, le Manuel de Tallinn a adopté une disposition selon laquelle « un Etat peut agir sur la base de l'état de nécessité en réponse à des actes qui représentent un péril grave et imminent à ses intérêts essentiels, de nature cyber ou non, lorsque cela constitue pour lui le seul moyen de les protéger »[162]. Ils soulignent que la nature et l'étendue précise de l'état de nécessité demeurent controversés, mais que le seuil à atteindre pour que l'état de nécessité soit caractérisé est extrêmement haut et qu'il ne peut être invoqué que dans des cas exceptionnels. La notion d'intérêt essentiel est vague, et ne fait pas l'objet d'une définition universelle. L'état de nécessité est donc à examiner au cas par cas et varie en fonction de l'Etat concerné.

[161] Geiss/Lahmann, "Freedom and security in cyberspace: shifting the focus away from military responses towards non-forcible countermeasures and collective threat prevention" *in Peacetime Regime for State Activities in Cyberspace, K. Ziolkowski (ed.), 2013*, p. 644.

[162] Tallinn Manual 2.0., Rule 26 : « A state may act pursuant to the plea of necessity in response to acts that present a grave and imminent peril, whether cyber in nature or not, to an essential interest when doing so is the sole means of safeguarding it".

L'observation de la pratique des Etats montre qu'un intérêt essentiel peut être la protection de l'environnement ou la protection de la population civile contre une attaque terroriste par exemple. Il semble que la protection d'infrastructures vitales nationales (*critical infrastructures*) – telles que des centrales électriques ou nucléaires par exemple – face à des cyberattaques puisse constituer un intérêt essentiel.

Le simple fait qu'une cyber opération vise ce qu'un Etat considère comme un intérêt essentiel ne suffit pas à invoquer l'état de nécessité, puisque le dommage potentiel doit être suffisamment grave. Il ne doit pas nécessairement être de nature physique, mais une simple disruption mineure ne suffit pas ; le péril doit être à même de porter fondamentalement atteinte aux intérêts de l'Etat concerné. Le groupe d'experts donne l'exemple d'une cyberattaque visant les réseaux électriques ou visant à causer une catastrophe environnementale ou porter atteinte au système bancaire d'un Etat, impactant sévèrement sa sécurité, son économie, la santé publique de ses habitants ou l'environnement.

Le fait qu'un Etat puisse prendre des mesures sur la base de l'Etat de nécessité indépendamment d'un comportement internationalement illicite d'un autre Etat est particulièrement intéressant dans le contexte cyber. En effet, il constitue une option lorsqu'un Etat est victime d'une cyber opération qui est le fait d'un acteur non-étatique comme un groupe d'activistes, une entreprise ou des terroristes et qui atteint le seuil de gravité décrit ci-dessus.

Il reste néanmoins que l'état de nécessité est circonscrit à des opérations exceptionnelles, et ne peut être envisagé comme « stratégie » de défense face aux cyberattaques[163]. De plus, parce que les actions basées sur l'état de nécessité évitent à un Etat d'avoir à attribuer les actions dont il est victime, elles présentent le risque d'être utilisées abusivement.

[163] Geiss/Lahmann, "Freedom and security in cyberspace: shifting the focus away from military responses towards non-forcible countermeasures and collective threat prevention" *in Peacetime Regime for State Activities in Cyberspace, K. Ziolkowski (ed.), 2013,* p. 645.

Conclusion – vers un droit international du cyberespace ?

Au vu de ces développements, on peut se demander si les règles actuelles sont adaptées et suffisantes compte tenu de l'importance croissante des cyberattaques. Certes, le cyberespace n'est pas un espace de « non-droit », néanmoins, l'on voit que l'application par analogie de règles pensées pour réguler les conflits terrestres, maritimes ou aériens n'est pas toujours simple. Les propositions créatives de certains auteurs d'avoir recours à des concepts peu exploités en droit international – comme le principe de diligence ou l'état de nécessité – démontre que le cadre normatif actuel n'est pas tout à fait adapté.

En effet, les réponses aux cyberattaques demeurent limitées, en particulier par le problème d'identification et d'attribution des cyberattaques. De plus en plus d'acteurs non-étatiques sont susceptibles d'y avoir recours, ainsi que les Etats, et le recours à la légitime défense ou à des contre-mesures ne peut s'opérer que sous des conditions strictes. Le recours à l'état de nécessité, même s'il est intéressant, semble trop restreint puisqu'il ne concerne que des situations exceptionnelles. Cela laisse donc les Etats dans une situation délicate, puisqu'ils ne peuvent recourir à l'usage de la force ou à des contre-mesures tant qu'ils n'ont pas pu attribuer une cyberattaque à un Etat.

Face à ces problématiques, différentes possibilités existent pour faire évoluer le droit et fournir aux Etats des réponses adaptées.

Certains considèrent que le droit international ne nécessite pas d'être formellement modifié pour s'adapter dans le cyberespace et s'en remettent plutôt à la pratique des Etats pour déterminer le droit applicable. Il s'agit d'une position minoritaire ; une majorité des Etats et de la littérature propose d'adopter un traité visant à réguler le comportement des Etats dans le cyberespace. Il reste à savoir si ce traité doit consister en des normes de droit international, applicables à tous les membres, comme pour les Conventions de Genève par exemple, ou si ce traité doit fonctionner sur le même modèle que la Convention de Budapest qui impose aux Etats d'adapter leur droit interne et d'adopter des dispositions. D'autres propositions visent à promouvoir l'adoption de codes de conduite par les Etats, formellement non contraignants.

Pour une partie de la littérature, il n'est pas besoin d'adopter de nouvelles normes relatives au cyberespace, ou du moins pas tout de suite. Certains recommandent d'attendre que le droit évolue grâce à la pratique des Etats[164]. Néanmoins, cette approche présente plusieurs défauts. Tout d'abord, même si la création d'une règle coutumière peut se faire instantanément (*instant custom*) en théorie, la plupart des règles coutumières se forment après un certain laps de temps. Il faudrait donc probablement attendre des années avant de disposer d'un corps de règles constituant une « pratique générale acceptée comme étant le droit »[165]. Enfin, compte tenu des différents intérêts qu'ont les Etats dans le cyberespace, il est peu probable d'arriver à un corps uni de règles, acceptées par une majorité de la communauté internationale.

Ce problème n'est pas absent de l'idée de rédiger un traité, néanmoins, la rédaction de celui-ci supposerait la mise en place de comités de rédactions, formés de représentants de chacun des Etats, dont le but est de trouver une solution médiane satisfaisante pour la majorité de la communauté internationale.

Il semble que l'adoption d'un traité doive combiner deux volets, droit international et droit domestique. L'adoption d'un traité serait tout d'abord l'occasion d'adopter une définition commune de ce que constitue une cyberattaque pour mettre fin à l'incertitude qui règne aujourd'hui. Il serait également l'occasion de rappeler que le droit international s'applique dans le cyberespace. L'interdiction de faire usage de la force dans le cyberespace devrait constituer un des piliers du texte. Si aucune définition du terme « force » ne peut être trouvé, le traité pourrait toutefois contenir une liste d'exemples d'actes que les Etats peuvent qualifier d'usage de la force, en reprenant la méthode utilisée dans la définition de l'agression[166]. Cela permettrait notamment de faire transparaître la vision selon laquelle il y a usage de la force lorsque des infrastructures nationales vitales sont visées. Les Etats devraient également s'engager à ne pas chercher à déstabiliser un autre Etat, par exemple en s'attaquant à son économie ou en diffusant de la propagande à grande échelle.

Un autre volet du texte devrait imposer aux Etats signataires d'adapter leur législation interne pour mieux prendre en compte la menace cyber. Concrètement, il s'agirait de pénaliser les comportements hostiles dans le cyberespace qui sont le fait d'acteurs non-étatiques, mais aussi

[164] Comité international de la Croix rouge par exemple.
[165] Pour reprendre les termes de l'article 38 du Statut de la Cour internationale de Justice.
[166] A/RES/3314.

d'encourager la coopération, les échanges d'informations entre les Etats, notamment dans le cadre de leurs enquêtes après avoir été victime d'une cyberattaque.

Il s'agit là des mêmes recommandations que celles formulées par le rapport du GGE de 2015. Plusieurs Etats ont déclaré vouloir continuer à travailler au niveau international sur la base des précédents rapports du GGE. Malgré l'échec du dernier groupe de travail en 2017, les règles édictées dans les rapports précédents devraient continuer à être reconnues par la communauté internationale. On peut toutefois noter les reproches adressés au GGE par certains Etats, qui critiquent son manque de représentativité, notamment des pays en voie de développement[167]. Un sixième groupe a été instauré, dont la mission est de parvenir à adopter un nouveau rapport d'ici 2021[168].

En parallèle, un groupe de travail intergouvernemental – *Open-ending Working Group (OEWG*) a été mis en place en décembre 2018[169]. Il a pour mission de développer des règles, normes et principes relatifs aux comportements des Etats dans le cyberespace, mais aussi de discuter de leur mise en œuvre et d'étudier la possibilité d'établir une institution permanente en charge de ces questions. Il est ouvert à tous les pays qui souhaitent s'impliquer dans les discussions, mais devrait aussi se réunir avec les représentants d'ONG, d'entreprises du secteur privé ou d'académiques. Son rapport devrait être présenté à l'Assemblée générale en automne 2020.

L'adoption d'un traité n'est pas exempte de reproches. Tout d'abord, il faut prendre en compte les Etats qui décideront de ne pas se joindre aux négociations ou de ratifier le traité et qui agiront donc en « loup solitaire » dans le cyberespace, risquant de mettre à mal le système en place. De plus, comme avec toutes les nouvelles technologies, les règles risquent de devenir rapidement obsolètes. C'est pourquoi la rédaction d'un traité doit être suffisamment précise pour adresser tous les problèmes que posent les cyberattaques, sans pour autant risquer de devenir inapplicables en raison de l'avancement de la technologie.

Certains avancent qu'il est peu probable que les Etats possédant les capacités cyber les plus puissantes acceptent de rédiger un traité venant réguler leur comportement dans le cyberespace.

[167] AG/DSI/3613.
[168] Institué par la résolution A/RES/73/226.
[169] A/RES/73/27.

Pourtant, comme le souligne Hollis[170], le droit international tel qu'il s'applique aujourd'hui par analogie aux cyber-opérations est plutôt restrictif. Or, dans monde dans lequel les Etats voisins ne constituent plus la menace première, mais plutôt les acteurs non-étatiques comme les groupes terroristes, les Etats pourraient au contraire voir un intérêt dans la rédaction de normes internationales régulant leur comportement dans le cyberespace, si celles-ci adressent le problème des acteurs non-étatiques.

Il est peu probable que l'adoption d'un traité modifie le comportement des acteurs non-étatiques, qui continueront à utiliser des moyens cyber pour mener des opérations hostiles. Néanmoins, un traité peut constituer une bonne base pour la coopération entre Etats et pour faciliter la poursuite des auteurs.

La rédaction d'un traité présente avant tout le désavantage de durer longtemps, d'autant plus dans un domaine comme le cyberespace où les grandes Nations cherchent à défendre leurs intérêts et à imposer leur vision. Preuve en est, la dernière réunion du Groupe gouvernemental d'experts mis en place au niveau des Nations en 2017 n'a pas pu déboucher sur l'adoption d'un rapport car les Etats n'ont pas réussi à se trouver d'accord.

C'est pourquoi certains Etats proposent plutôt d'adopter des codes de conduite non contraignants[171]. Les règles contenues dans ces codes de conduite peuvent, à terme, se cristalliser en droit international coutumier et donc acquérir la même force que du droit conventionnel.

C'est notamment la position de la France qui souhaite promouvoir au niveau international des mesures de confiance. Ces mesures viseraient à mettre en place une autorité compétente pour traiter les attaques visant les systèmes d'information et pour renforcer l'échange d'informations entre les Etats lorsque des poursuites sont engagées.

Pour l'auteur de ce mémoire, il convient de se lancer dans ces trois voies simultanément. Les Etats devraient poursuivre leurs efforts, éventuellement au sein des Nations Unies, pour rédiger un traité adressant les principaux problèmes dans le cyberespace, en particulier le traitement des cyberattaques issues de groupes non-étatiques et la problématique de l'attribution. En même temps, un droit coutumier va se former progressivement, à mesure que les cyber-attaques se

[170] D.B. Hollis, "Why states need an international law for information operations", *Lewis & Clark Law Review*, Vol. 11, 2007, p. 1039.
[171] Internationale Sicherheit und Völkerrecht im Cyberespace.

multiplient, et la pratique des Etats viendra enrichir les normes applicables dans le cyberespace. Enfin, l'instauration de codes de conduite, de façon temporaire, permet de donner un cadre, qui, bien que non normatif, est à même d'inciter les Etats à se conduire de façon pacifique dans le cyberespace.

Bibliographie

Livres

- **Dethloff/Nolte/Reinisch**, „Freiheit und Regulierung in der Cyberwelt“, *Berichte der Deutschen Gesellschaft für Internationales Recht*, Band 47, C.F. Müller, 2016.
- Heather Harrison **Dinniss**, “Cyber Warfare and the Laws of War”, Cambridge Studies in International and Comparative Law, Cambridge University Press, 2012.
- Falko **Dittmar**, „Angriffe auf Computernetzwerke – *Ius ad bellum* und *ius in bello*“, Schriften zum Völkerrecht, Band 159, Duncker & Humboldt, 2004.
- Louis **Gautier – Secrétaire Général de la défense et de la sécurité nationale (SGDSN)**, « Stratégie nationale de la cyberdéfense », *Editions Economica*, 2018.
- Frauke **Lachenmann**/Rüdiger **Wolfrum**, « The Law of Armed Conflict and the Use of Force”, *The Max Planck Encyclopedia of Public International Law*, 2017.
- Georg **Nolte**/Albrecht **Randelzhofer**, « Ch. VII, Actions with respect to threats to the peace, breaches of the peace, and acts of aggression, Article 51” in *The Charter of the United Nations: a commentary*, Volume II (3rd edition), 2012.
- **Tallinn Manual** on the international law applicable to cyberwarfare, Prepared by the International Group of Experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence, *Cambridge University Press*, 2013.
- **Tallinn Manual** (2.0) on the international law applicable to cyber operations, second edition, prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence, *Cambridge University Press*, 2017.
- Walter Gary **Sharp**, “Cyberspace and the use of force”, *Ageis Research Corp.*, 1999.
- Thomas **Rid**, “Cyber War will not Take Place”, *Oxford University Press*, 2013.
- Johann-Christoph **Woltag**, “Cyber Warfare – Military Cross-Border Computer Network Operations under international Law”, Intersentia, 2014.

Périodiques et Articles

- Henry **Bakis**, « Fragilité du géocyberespace à l’heure des conflits cybernétiques », *Netcom*, 2013.
- Michel **Baud**, « La cyberguerre n’aura pas lieu, mais il faut s’y préparer », *Institut français des relations internationales – Politique étrangère*, 2012/2 Eté, p. 305 à 316.

- Alexis **Bautzmann**, « Vers un droit international du cyberspace ? », *Revue internationale et stratégique*, 2001/2 n°42, pp. 171 à 175.
- Marco **Benatar**, "The use of cyber force: need for legal justification?", *Göttingen Journal of international Law 1*, p. 375-396, 2009.
- Clémentines **Bories**, « Appréhender la cyberguerre en droit international. Quelques réflexions et mises au point », *La Revue des droits de l'homme*, 2014.
- Gary **Brown**, Gary and Keira **Poellet**. "The Customary International Law of Cyberspace." *Strategic Studies Quarterly*, vol. 6, no. 3, 2012, pp. 126–145, disponible sur *JSTOR*, www.jstor.org/stable/26267265.
- Gary D. **Brown** and Owen W. **Tullos**, "On the spectrum of Cyberspace Operations", *Small Wars Journal*, 2012.
- Russel **Buchan**, "Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?", *Journal of Conflict and Security Law*, 17(2), pp. 212-227, 2012.
- Hakan Selim **Canca**, "Prohibition against the use of force and the coercive uses of the cyberspace", *Journal of Naval Science and Engineering, 2017, Vol. 13, No.1, pp.60-72.*
- Myriam Dunn **Cavelty**, "Cyberwar: concept, status quo, and limitations", *CSS Analysis in Security Policy – ETH Zürich*, N° 71, 2010.
- Yoram **Dienstein**, "Computer Network Attacks and Self-defence", *International Law Studies*, Vol. 76, pp. 99-119.
- James P. **Farwell** and Rafal **Rohozinski**, "Stuxnet and the Future of Cyber War", *Survival, Vol. 53 (1),* March 2001, pp. 23-40.
- Lieutenant Colonel Patrick W. **Franzese**, "Sovereignty in Cyberspace: can it exist?", *The Air Force Law Review*, Vol. 64, pp. 1-42, 2009.
- Robin **Geiss** et Henning **Lahmann**, Freedom and Security in Cyberspace: Shifting the Focus Away from Military Responses Towards Non-Forcible Countermeasures and Collective Threat-Prevention (January 1, 2014). K. Ziolkowski (ed.), Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy, Tallinn 2013. Available at SSRN: https://ssrn.com/abstract=2462950
- Michael **Gervais**, "Cyber Attacks and the laws of war", *Berkeley Journal of international Law*, Vol. 30 Issue 2, pp. 525-579, 2012.
- Oriane Barat-**Ginies**, « Existe-t-il un droit international du cyberespace ? », *La découverte*, 2014/1 n° 152-153, pp. 201-220.

- Jack **Goldsmith**, “How cyber changes the laws of war”, *The European Journal of international Law*, Vol. 24, No. 1, pp. 129-138, 2013.
- Lawrence T. **Greenberg**, Seymour E. **Goodman** and Kevin J. **Soo Hoo**, “Information Warfare and international Law”, *National Defense University Press*, 1998.
- Oren **Gross**, “Cyber Responsibility to protect: legal obligations of states directly affected by cyber-incidents”, *Cornell International Law Journal, Vol. 48*.
- Samuli **Haataja**, “The 2007 cyber-attacks against Estonia and international law on the use of force: an informational approach”, *Journal Law, innovation and Technology, Volume 9, 2017 - Issue 2,* pp. 159-189.
- Oona A. **Hathaway**, Rebecca **Crootof**, Philip **Levitz**, Haley **Nix**, Aileen **Nowlan**, William **Perdue**, Julia **Spiegel**, “The Law of Cyber-Attack”, *California Law Review*, Vol. 100, pp. 819-885, 2012.
- Duncan B. **Hollis**, « Why States need an International Law for information operations”, *Lewis & Clark Law Review,* Vol. 11, pp. 1023-1061, 2007.
- Christopher C. **Joyner** and Catherine **Lotrionte**, “Information Warfare as international Coercion: elements of a legal framework”, *European Journal of International Law*, Vol. 12, 2001, pp. 825-865.
- Olivier **Kempf**, “Cyberstratégie à la française », *Revue internationale et stratégique,* 2012/3, n°87, pages 121 à 129.
- Hongju **Koh**, "International Law in Cyberspace", *Harvard International Law Journal*, Volume 54, 2012.
- Sheng **Li**, “When Does Internet Denial Trigger the Right of Armed Self-Defense?”, *Yale Journal of International Law,* Volume 38, pp. 179-215, 2013.
- Catherine **Lotrionte**, « Cyber Operations: Conflict Under International Law”, *Georgetown Journal of International Affairs*, International Engagement on Cyber 2012: Establishing Norms and Improving Security (2012), pp. 15-24.
- Catherine **Lotrionte**, “Reconsidering the consequences for State-sponsored Hostile Cyber Operations under International Law”, *The Cyber Defense Review*, Vol. 3, No. 2, pp. 73-114, 2018.
- Barbara **Louis-Sidney**, « La dimension juridique du cyberespace », *Revue internationale et stratégique*, 2012/3 n°87.

- William **Mattessich**, "Digital Destruction: Applying the Principle of Non-Intervention to Distributed Denial of Service Attacks Manifesting No Physical Damage", *Columbia Journal of Transnational Law*, Vol. 54 (3), 2016, pp. 874-896.
- Nils **Melzer**, "Cyberwarfare and international law", *United Nations Institute for Disarmament Research (UNIDIR)*, 2011.
- Reese **Nguyen**, "Navigating Jus Ad Bellum in the Age of Cyber Warfare", *California Law Review, Vol. 101 (4)*, 2013.
- Julien **Nocetti**, « Géopolitique de la cyber-conflictualité », *Revue politique étrangère – IFRI*, 2018.
- Mary Ellen **O'Connell**, „Cyber security without cyberwar", *Journal of Conflict & Security Law* (2012), Vol. 17 No. 2, 187–209.
- Bradley **Raboin**, "Corresponding Evolution: International Law and the Emergence of Cyber Warfare", *Journal of the National Association of Administrative Law Judiciary*, Vol. 31, Issue 2, pp. 603-668, 2011.
- John **Richardson**, "Stuxnet as Cyberwarfare: Applying the law of war to the virtual battlefield", Available at SSRN: https://ssrn.com/abstract=1892888 or http://dx.doi.org/10.2139/ssrn.1892888, 2011.
- Thomas **Rid**, "Cyber War will not take place", *Journal of Strategic Studies*, Vol. 35, No. 1, 5–32, February 2012.
- Michael **Robinson**, Kevin **Jones**, Helge **Janicke**, "Cyberwarfare: Issues and challenges", *Computers and security*, Vol. 49, March 2015, pp. 70-94.
- Marco **Roscini**, "World Wide Warfare – *Jus ad bellum* and the use of cyber force", Max Planck Yearbook of United Nations Law, Volume 14, 2010, p. 85-130.
- Marco **Roscini**, "*Cyber operations as a use of force*", in Research Handbook on International Law and Cyberspace, Edward Elgar Publishing, 2015, 233-254.
- Scott J. **Shackelford**, « From Nuclear War to Net War: Analogizing Cyber Attacks in International Law », *Berkeley Journal of international Law*, Vol. 27, pp. 192-251, 2009.
- Christian **Schaller**, „Internationale Sicherheit und Völkerrecht im Cyberspace – für klarere Regeln und mehr Verantwortung", *Stiftung Wissenschaft und Politik*, 2014.
- Michael N. **Schmitt**, "Computer Network Attack and the use of force in international law: thoughts on a normative Framework", *Columbia Journal of Transnational Law, Vol. 37*, 1999.

- Michael N. **Schmitt**, "International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed", *Harvard International Law Journal*, Vol. 54, 2012.
- Michael N. **Schmitt**, "Below the Threshold" Cyber Operations: The Countermeasures Response Option and International Law", *Virginia Journal of International Law*, Vol. 54:3, pp. 697-732.
- Michael N. **Schmitt**, "Rewired Warfare: rethinking the law of cyberattacks", *International Review of the Red Cross, Vol. 96* (893), 2014, pp. 189-206.
- Daniel B. **Silver**, "Computer Network Attack as a Use of force under Article 2(4) of the United Nations Charter" in M. Schmitt/BT O'Donnell (eds), *Computer Network Attacks and international Law,* 2002, pp. 73-97.
- Loïc **Simonet**, « L'usage de la force dans le cyberespace et le droit international », *Annuaire français de droit international*, volume 58, 2012. pp. 117-143.
- Matthew J. **Sklerov**, "Solving the dilemma of State Response to Cyberattacks: a justification for the Use of Active Defences against States who neglect their duty to prevent", *Military Law Review, Vol. 201, 2009*, pp. 1-86.
- Eric **Talbot-Jensen**, "Computer attacks on critical national infrastructure: a use of force invoking the right of self-defence", *Stanford Journal of international law*, 2002.
- Major Graham H. **Todd**, "Armed Attack in Cyberspace: Deterring Asymmetric warfare with an asymmetric definition", *The Air Force Law Review,* Vol. 64, pp. 65-102, 2009.
- Jozef **Valuch**, Tomáš **Gábriš**, Ondrej **Hamuľák**, "Cyber-attacks, informations attacks and postmodern warfare*", Baltic Journal of Law & Politics 10:1 (2017*), pp. 63–89.
- Beatrice A. **Walton**, "Duties Owed: Low-Intensity Cyber Attacks and Liability for Transboundary Torts in International Law", *Yale Law Journal,* Vol. 126, pp. 1460-1519, 2017.
- Sean **Watts**, "Low intensity cyber operations and the principle of non-intervention", *Baltic Yearbook of international Law*, Vol. 14(1), 2015.
- Matthew C. **Waxman**, "Cyber-attacks and the use of force: back to the future of Article 2(4)", *Yale Journal of International Law, Vol. 36*, 2011.
- Li **Zhang**, « A chinese perspective on cyber war », *International Review of the Red Cross*, Volume 94, 2012.

Rapports

- **Comité international de la Croix Rouge** (ICRC), « International humanitarian law and the challenges of contemporary armed conflicts", 31st international Conference, 2011.
- **Cooperative Cyber Defence Centre of Excellence** (CCDCOE), "Cyber Attacks Against Georgia: Legal Lessons Identified", 2008.
- **Cooperative Cyber Defence Centre of Excellence** (CCDCOE), "International Cyber incidents – Legal considerations", 2010.
- Paul **Cornish**, David **Livingstone**, Dave **Clemente** and Claire **Yorke**, "On Cyber Warfare", *A Chatam House Report*, November 2010.
- François **Delerue**, « le droit international dans la 'stratégie nationale de la cyberdéfense' », *Institut de recherche stratégique de l'école militaire (IRSEM*), Note de recherche n°58, 2018.
- **Deutscher Bundestag, Wissenschaftliche Dienste**, "Anwendbarkeit des humanitären Völkerrechts auf Computernetzwerkoperationen und digitale Kriegsführung (*Cyber Warfare*) », WD 2 - 3000 - 038/15, 2015.
- **Sénat**, Rapport d'information fait au nom de la commission des Affaires étrangères, de la défense et des forces armées sur la cyberdéfense, par M. Roger **Romani**, Annexe au procès-verbal de la séance du 8 juillet 2008.
- **Sénat, R**apport d'information n° 681 (2011-2012) de M. Jean-Marie **Bockel**, fait au nom de la commission des affaires étrangères, de la défense et des forces armées, déposé le 18 juillet 2012
- Robert K. **Knake**, "Untangling Attribution: Moving to Accountability in Cyberspace", Before the Subcommittee on Technology and Innovation, Committee on Science and Technology, *United States House of Representatives, 2nd* Session, *111th* Congress, 2010.
- **ICRC Expert Meeting**, "The potential human cost of Cyber Operations", 14-16 novembre 2018.
- **The White House**, International Strategy for Cyberspace – Prosperity, Security and Openness in a networked World, May 2011.

Jurisprudence

Arrêts et avis de la CPJI et de la CIJ

- CPJI, Affaire du « Lotus », Publications de la Cour permanente de Justice internationale, Série A – n°10, 7 septembre 1927.
- CIJ, Affaire du Détroit de Corfou (fond), Recueil des arrêts, avis consultatifs et ordonnances 1949, p. 4, Arrêt du 9 avril 1949.
- Affaire relative au personnel diplomatique et consulaire des Etats-Unis à Téhéran (Etats-Unis d'Amérique c. Iran), Recueil des arrêts, avis consultatifs et ordonnances 1980, p. 3, Arrêt du 24 mai 1980.
- CIJ, Affaire des activités militaires et paramilitaires au Nicaragua et contre celui-ci (Nicaragua c. Etats-Unis d'Amérique), Recueil des arrêts, avis consultatifs et ordonnances 1986, p. 14, Arrêt du 27 juin 1986.
- CIJ, Licéité de la menace ou de l'emploi d'armes nucléaires, Recueil des arrêts, avis consultatifs et ordonnances 1996, p. 226, Avis consultatif du 8 juillet 1996.
- Affaire des plates-formes pétrolières (République islamique d'Iran c. Etats-Unis d'Amérique), Recueil des arrêts, avis consultatifs et ordonnances 2003, 161, Arrêt du 6 novembre 2003.
- CIJ, Conséquences juridiques de l'édification d'un mur dans le territoire palestinien occupé, Recueil des arrêts, avis consultatifs et ordonnances 2004, p. 136, Avis consultatif du 9 juillet 2004.
- CIJ, Affaire des activités armées sur le territoire du Congo (République démocratique du Congo c. Ouganda), Recueil des arrêts, avis consultatifs et ordonnances 2005, p. 168, Arrêt du 19 décembre 2005.
- CIJ, Affaire relative à des usines de pâte à papier sur le fleuve Uruguay (Argentine c. Uruguay), Recueil des arrêts, avis consultatifs et ordonnances 2010, p. 14, Arrêt du 20 avril 2010.
- CIJ, Conformité au droit international de la déclaration unilatérale d'indépendance relative au Kosovo, Recueil des arrêts, avis consultatifs et ordonnances 2010, p. 403, Avis consultatif du 22 juillet 2010.

Tribunal pénal international pour l'ex-Yougoslavie

- TPIY, Chambre d'appel, *Affaire Tadic*, 2 octobre 1995.

Iran-US Claims Tribunal (IUSCT)

- *Yeager v. Iran*, Case N. 10199, 1987.

Articles de presse

- Pierre **Alonso** et Amaelle Guiton, « Cyberguerre : la diplomatie en quête d'un déclic », **Libération**, 11 novembre 2018. Disponible à : https://www.liberation.fr/planete/2018/11/11/cyberguerre-la-diplomatie-en-quete-d-un-declic_1691476.
- Baudouin **Eschapasse**, « Cyberguerre : les grandes manœuvres ont commencé … », **Le Point**, 23 avril 2019. Disponible à : https://www.lepoint.fr/high-tech-internet/cyberguerre-les-grandes-manoeuvres-ont-commence-23-04-2019-2309133_47.php.
- Anaïs **Bouniol**, « Stuxnet. Duqu. Et maintenant Flame. Ces virus relancent le débat sur le déploiement des cyberattaques », **Le Point**, 11 juin 2012. Disponible à : https://www.lepoint.fr/monde/ou-s-arretera-la-cyberguerre-11-06-2012-1471968_24.php#xtmc=stuxnet&xtnp=1&xtcr=6.
- John **Markoff**, "Before the Gunfire, Cyberattacks", **The New York Times**, 12 août 2008. Disponible à : https://www.nytimes.com/2008/08/13/technology/13cyber.html.
- « Telegram victime d'une cyberattaque venant de Chine »**, Les Echos**, 13 juin 2019. Disponible à : https://www.lesechos.fr/monde/asie-pacifique/telegram-victime-dune-cyberattaque-venant-de-chine-1028958.

Divers

- Michael N. **Schmitt** - Responding to Cyber Operations. Security Summit 2018, disponible à l'adresse suivante : https://vimeo.com/261517670.
- Déclaration de M. Manuel Valls, Premier ministre et M. Jean-Yves Le Drian, ministre de la défense, sur l'engagement des forces aériennes en Syrie, à l'Assemblée nationale le 15 septembre 2015, à retrouver sur http://discours.vie-publique.fr/notices/153002296.html.

Table des matières