Les cyberattaques étatiques et la notion d'agression en droit international

Vladimir Szoke-Pellet

AIX-MARSEILLE UNIVERSITÉ
FACULTÉ DE DROIT ET DE SCIENCE POLITIQUE

CERIC
Centre d'Études et de Recherches Internationales et Communautaires

Unité Mixte de Recherche 7318
Droit International, Comparé et Européen
(UMR 7318 DICE)
AMU-CNRS

MÉMOIRE DANS LE CADRE DU

MASTER 2 DROIT INTERNATIONAL PUBLIC
MENTION DROIT INTERNATIONAL ET EUROPÉEN

LES CYBERATTAQUES ÉTATIQUES ET LA NOTION D'AGRESSION EN DROIT INTERNATIONAL

Sous la direction de
Monsieur le Professeur PHILIPPE Xavier

Vladimir SZOKE-PELLET

Année universitaire 2017/2018

REMERCIEMENTS

Je remercie vivement Monsieur le Professeur PHILIPPE Xavier pour ses précieux conseils, ses encouragements et sa disponibilité tout au long du présent mémoire, et en particulier lors des grandes étapes de sa rédaction.

Je remercie également mes proches pour leur disponibilité et leur aide.

SOMMAIRE

LISTE DES SIGLES ET ABREVIATIONS

A.G.N.U.	**Assemblée générale des Nations unies**
A.N.S.S.I.	**Agence Nationale de la Sécurité des Systèmes d'Information**
A.P.T.	**Attaques sophistiquées persistantes**
C.D.I.	**Commission du droit international**
C.I.C.R.	**Mouvement international de la Croix-Rouge et du Croissant-Rouge**
C.I.J.	**Cour Internationale de Justice**
C.N.U.	**Charte des Nations unies**
C.P.J.I.	**Cour Permanente de Justice Internationale**
C.S.	**Conseil de sécurité**
D.G.S.S.I.	**Direction Générale de la Sécurité des Systèmes d'Information**
D.I.H.	**Droit International Humanitaire**
F.I.I.	**Fait internationalement illicite**
N.R.B.C.	**Armes Nucléaires, Radiologiques, Biologiques et Chimiques**
N.S.A.	**National Security Agency**
O.N.U.	**Organisation des Nations unies**
OTAN	**Organisation du traité de l'Atlantique nord**

P.A.I. **Protocole additionnel I aux Conventions de Genève**

R.D.C. **République Démocratique du Congo**

S.D.N. **Société des Nations**

T.P.I.Y. **Tribunal pénal international pour l'Ex-Yougoslavie**

U.I.T. **Union internationale des télécommunications**

Introduction

1. « *La guerre n'est que la continuation des relations politiques avec d'autres moyens* ». Tel que le conceptualisait Clausewitz, les relations interétatiques ont toujours été la source de tensions entre les États. Pendant longtemps, les relations entre les États ont été gouvernées par le dogme westphalien. Ce dogme, issu du Traité de Westphalie de 1648, met en place divers principes. Il pose tout d'abord les États comme les principaux sujets du droit international, ce qui donne naissance au système interétatique moderne. Les États sont de plus égaux ce qui induit qu'ils ne reconnaissent aucune autorité supérieure, qu'ils ont une autorité exclusive sur leur sol, protégée par une obligation de non-ingérence des autres États, et qu'ils ne doivent pas disposer de forces leur permettant d'imposer leur hégémonie à l'ensemble des autres États.

2. C'est également au nom de cette souveraineté que les États peuvent s'engager dans des luttes contre d'autres États. Cet ordre westphalien fait ainsi de la guerre un mode de résolution normal des différends, qui donne la possibilité aux États d'y recourir librement pour éteindre leurs litiges. Cela érige *de facto* la guerre en un instrument nécessaire à son fonctionnement même[1]. Cette conception westphalienne permet ainsi aux États de recourir à la force afin d'asseoir leur pouvoir sur la scène internationale. Tel que l'exprime J. Lévy « *le monde prend alors la forme d'un champ de force* »[2] entre les puissants capables d'imposer leurs vues et les faibles qui les subissent.

3. *A contrario* de ce système fondé sur la guerre, l'idée de pacifier ces relations a depuis longtemps été développée. Dès le XIV^{ème} siècle, la notion de « *paix chrétienne* » a été développée par Pierre Du Bois[3]. En 1625, Hugo Grotius devient le précurseur du droit international avec l'idée d'une loi s'imposant à toutes les puissances dans leurs relations internationales dans son ouvrage *De Jure Belli ac Pacis*[4]. Son idée est que les puissances chrétiennes soumettraient leurs litiges à une puissance tierce afin que cette dernière arbitre le litige, dans le but d'éviter les guerres entre chrétiens.

---

[1] En ce sens *v*. HIRIDJEE Kévin, « *Le Modèle westphalien* », IEP Paris http://sciences-po.macrocosme.net/cr_exposes/Hiridjee_Wesphalie.pdf
[2] *Ibid*.
[3] En ce sens *v*. MARBEAU Michel, « *La Société des Nations, vers un monde multilatéral 1919-1946* », éditions Presses Universitaires François Rabelais de Tours, 2017, p. 17
[4] *Ibid*. p. 19

4. L'idée d'un système assurant la paix est donc ancien, mais ne va voir le jour que tardivement. En effet, les relations interétatiques connaissent un tournant au XX^{e} siècle. En réaction aux millions de morts de la Première Guerre mondiale, l'idée de créer un système promouvant la paix se concrétise enfin.

5. Le système westphalien ayant entrainé par sa philosophie de la guerre la sanglante « *Der des Ders* », l'idée d'une organisation de la paix avec une structure supérieure aux États, méprisée avant la guerre, est alors encensée[5]. C'est sous l'impulsion des États-Unis et des 14 points du président Wilson que les États tentent de mettre fin au système westphalien en mettant en place le système de la Société des Nations (S.D.N.) en 1919, abandonnant le système de l'équilibre des États au profit d'un système de sécurité collective.

6. La S.D.N. est ainsi la première organisation internationale ayant pour finalité le maintien de la paix. Son pacte est annexé au traité de Versailles en 1919. Elle est créée le 10 janvier 1920 avec pour objectif d'éviter une nouvelle guerre mondiale. Cependant, la S.D.N. ne connaîtra pas le succès attendu notamment en raison de ses failles, et de la défection de son principal créateur, les États-Unis.

7. En effet, les États-Unis, en première ligne pour ce projet, ne ratifieront pas le pacte de la S.D.N. Le Sénat, d'une majorité hostile au président Wilson, refusera sa ratification. Cette « *défection des États-Unis est un coup dur pour la* S.D.N. »[6]. Cela la fragilise financièrement (les États-Unis étant ses principaux contributeurs), mais aussi politiquement car son projet de parvenir à réunir tous les États est, dès le départ, mis à mal, ce qui compromet sa volonté d'universalité. Le retrait des vaincus de la Première Guerre mondiale et le contexte géopolitique entraineront l'escalade des tensions entre la Triple-Alliance (ou Triplice) et la Triple-Entente, la course à l'armement puis la Seconde Guerre mondiale.

8. L'incapacité de la S.D.N. à s'opposer aux coups de forces de l'Axe et du Japon dans les années 1930, ainsi que d'empêcher la Seconde Guerre mondiale, entrainera sa perte. Toutefois, l'idée de réglementer les recours à la force des États demeure et réapparaît à

[5] En ce sens *v*. MARBEAU Michel, « *La Société des Nations, vers un monde multilatéral 1919-1946* », éditions Presses Universitaires François Rabelais de Tours, 2017, p. 37
[6] *Ibid*. p. 64

l'issue de la Seconde Guerre mondiale. Ce projet se matérialisera enfin véritablement avec la création de l'O.N.U. dans l'immédiat après-guerre (1945), création qui reprend le projet de la S.D.N. souhaitant mettre fin au système westphalien par l'établissement d'un mécanisme de sécurité collective, tendant à interdire les recours à la force et, *de facto*, les agressions entre États.

9. Le présent mémoire s'oriente vers une réflexion sur l'évolution de la notion d'agression afin qu'elle englobe non seulement les recours à la force constitués par des attaques conventionnelles, mais aussi ceux constitués par des cyberattaques. La question centrale est donc en quoi les cyberattaques peuvent être assimilées à des recours à la force constituant des agressions, et quelles seraient les conséquences d'une telle reconnaissance. Afin de traiter cette question, nous aurons donc recours à différentes notions spécifiques aux cyberattaques.

10. Tout d'abord, le cyberespace est issu d'Internet qui est un « *ensemble de réseaux informatiques privés et publics interconnectés grâce à un protocole de communication en commun […] conçus par les milieux américains de la défense et de la recherche dans les années 1960* »[7]. A l'époque réservé au domaine militaire et appelé « *Arpanet* » [8], il a été « *dissocié de l'usage militaire en 1980* »[9] et a pris le nom d'Internet.

11. D'Internet est né le cyberespace, qui peut être analysé sous la lumière de plusieurs sens et qui sera envisagé dans ce mémoire dans le sens de réseau, c'est-à-dire « *comme cet espace virtuel des ordinateurs reliés entre eux grâce à des réseaux, constitue un environnement global qui est le siège d'évènements ayant des conséquences juridiques* »[10]. Le préfixe cyber rappelant « *tout ce qui a un lien avec les ordinateurs, l'informatique, les réseaux ou encore Internet* »[11].

[7] BAUDIN Laura, « *Les cyberattaques dans les conflits armées* », éditions L'Harmattan, 2014, p. 16
[8] MULLET-FEUGA Philippe, « *Cyberespace, nouvelles menaces et nouvelles vulnérabilités* », éditions sécurité globale, 2017/I n°9, pp. 83-95 § 1
[9] *Ibid*.
[10] TRUDEL Pierre, « *Droit du cyberespace* », éditions Thémis, 1997, p. 1-15
[11] BAUDIN Laura, « *Les cyberattaques dans les conflits armées* », éditions L'Harmattan, 2014, p. 22

12. C'est dans le cyberespace qu'ont lieu les cyberattaques. Le terme de cyberattaque, parfois appelée attaque cybernétique, est « *l'association de cyberespace et attaque* »[12]. Ce sont donc des attaques qui ont lieu dans le cyberespace. Les cyberattaques peuvent être lancées par des personnes publiques ou privées. Les cyberattaques étatiques sont les cyberattaques lancées par des États contre d'autres acteurs (autres États, entreprises, particuliers) et peuvent être définies comme « *une agression contre les systèmes qui organisent, qui dirigent* »[13]. Ce sont donc des « *offensives attribuables à un État et menées contre les réseaux informatiques d'un autre pays afin d'occasionner des perturbations dans le fonctionnement des activités et services publics ou privés de l'État cible* »[14]. Les cyberattaques ont pour but de « *perturber, neutraliser, détruire ou contrôler de façon malveillante l'infrastructure informatique de la cible ou d'en détruire l'intégrité des données ou voler des informations protégées* »[15].

13. Les cyberattaques étatiques, menées par les États, entrent dans une logique de cyberguerre. La cyberguerre est définie par « *le département de la Défense américain comme un conflit armé conduit totalement ou partiellement par des moyens cyber, des opérations militaires menées pour interdire à l'ennemi l'utilisation efficace des systèmes du cyberespace et de ses armes au cours d'un conflit* »[16]. Toutefois, la cyberguerre est généralement « *dépourvue d'acceptation juridique* »[17] et fait référence à des « *situations de fait dans lesquelles l'outil informatique est utilisé aux fins de créer un dommage dans une sphère internationale* »[18]. Dans son sens « *entendu stricto sensu la cyberguerre devrait n'être que virtuelle, ne faire appel qu'à des armes électroniques et n'être conduite que dans une sphère immatérielle* »[19]. Toutefois, la cyberguerre est « *la conduite, dans un contexte de conflit armé, d'activités militaires à l'aide de moyens et de méthodes numériques dans le cyberespace* ». Dès lors, « *en l'absence de conflit*

---

[12] AKOTO Evelyne, « *Les cyberattaques étatiques constituent-elles une agression en droit international public ?* » : Première partie. Revue de droit d'Ottawa - Ottawa Law Review, Faculty of Law, Common Law Section, University of Ottawa, 2015, 46 (1), pp.1. http://www.rdoolr.uottawa.ca/subsite/olr/ <hal-01244603> p. 3
[13] BAUDIN Laura, « *Les cyberattaques dans les conflits armées* », éditions L'Harmattan, 2014, p. 22
[14] AKOTO Evelyne, « *Les cyberattaques étatiques constituent-elles une agression en droit international public ?* » : Première partie. Revue de droit d'Ottawa - Ottawa Law Review, Faculty of Law, Common Law Section, University of Ottawa, 2015, 46 (1), pp.1. http://www.rdoolr.uottawa.ca/subsite/olr/ <hal-01244603> p. 3
[15] *Ibid*.
[16] BAUD Michel, « *La cyberguerre n'aura pas lieu, mais il faut s'y préparer* », éditions Politique étrangère, 2012, p. 305-316, § 5
[17] BORIES Clémentine, « *Appréhender la cyberguerre en droit international. Quelques réflexions et mises au point* », éditions La revue des Droits de l'Homme, juin 2014, § 5
[18] *Ibid*.
[19] *Ibid*.

armé opposant deux États, toute cyberattaque opposant lesdits États est considérée avoir lieu en temps de paix, et n'est donc pas un acte de guerre »[20].

14. Un acte de cyberguerre *« peut consister dans une opération menée dans le cadre d'un conflit armé* »[21] mais aussi « *en dehors de tout conflit armée* »[22], se trouvant souvent en dehors des situations de guerre ou de paix, « *somewhere between* »[23]. L'hypothèse « *la plus communément admise* »[24] d'un acte de cyberguerre est « *une attaque électronique commanditée par des autorités étatiques soucieuses de porter atteinte aux intérêts d'une puissance étrangère* »[25].

15. La cyberguerre doit être distinguée « *de l'action d'un individu ou d'un groupe d'individus dont l'objectif, peut être l'enrichissement personnel (cybercriminalité) ou la revendication (cyberhacktivisme)* »[26] car la cyberguerre est « *une opération coordonnée, menée au travers du cyberespace par un groupe ayant des objectifs définis, au moyen de système d'information et de communication* »[27].

16. La cyberguerre est également à distinguer de la guerre dite classique, ou encore conventionnelle, qui « *met en œuvre de part et d'autre des armées nationales en uniforme sous la forme d'unités terrestres, maritimes et/ou aériennes*[28]. A l'inverse, la notion de guerre non conventionnelle recouvre « *l'emploi de moyens dits aujourd'hui asymétriques : techniques de guérilla (résistance, insurrection), ou actions de terrorisme, emploi de missiles balistiques, d'armes chimiques, voire biologiques ou nucléaires, ou encore de cyberattaques* »[29].

---

[20] AKOTO Evelyne, « *Les cyberattaques étatiques constituent-elles une agression en droit international public ?* » : Première partie. Revue de droit d'Ottawa - Ottawa Law Review, Faculty of Law, Common Law Section, University of Ottawa, 2015, 46 (1), pp.1. http://www.rdoolr.uottawa.ca/subsite/olr/ <hal-01244603> p. 9
[21] BORIES Clémentine, « *Appréhender la cyberguerre en droit international. Quelques réflexions et mises au point* », éditions La revue des Droits de l'Homme, juin 2014, § 5
[22] *Ibid*.
[23] *Ibid*.
[24] *Ibid*.
[25] *Ibid*.
[26] BAUD Michel, *« La cyberguerre n'aura pas lieu, mais il faut s'y préparer* », éditions Politique étrangère, 2012, p. 305-316, § 5
[27] *Ibid*. § 6
[28] TERTRAIS Bruno, « *La guerre* », éditions Presses Universitaires de France, 2010, p. 7
[29] *Ibid*.

17. Le système de l'Organisation des Nations unies (O.N.U.), créée en 1945 pour éviter tout nouveau conflit, a pour but premier de maintenir la paix et la sécurité internationales[30]. Ce système repose sur la Charte des Nations unies (C.N.U.). Celle-ci précise sa primauté et celle des décisions de son organe central, le Conseil de sécurité, sur les autres traités en ses articles 25 et 103.

18. Afin de maintenir et promouvoir la paix, le mécanisme des Nations unies proscrit à travers la C.N.U. le recours à la force entre États[31] et les oblige à régler leurs différends de manière pacifique[32]. Les États doivent respecter la souveraineté des autres États et ne pas s'ingérer dans leurs affaires intérieures, ni recourir à la force contre eux. Le recours à la force est confié à l'O.N.U. à travers le mécanisme de sécurité collective. Selon ce mécanisme, tout recours à la force est proscrit entre États, et seul le Conseil de sécurité est à même de l'autoriser car celui-ci a pour charge principale de veiller au maintien de la paix et de la sécurité internationales. La seule autre exception à l'interdiction du recours à la force est la possibilité de recourir à la légitime défense en cas d'agression. Tout recours à la force est prohibé et serait considéré par le Conseil de sécurité, comme une menace ou une rupture de la paix, voire comme une agression d'un État contre un autre, ce qui entrainerait sa réaction au moyen du chapitre VII de la Charte des Nations unies. Les États ont donc l'interdiction de s'ingérer ou de recourir à la menace ou l'emploi de la force entre eux.

19. Toutefois, lors de la rédaction de la C.N.U. en 1945, le recours à la force et l'agression ont été envisagés sous leur seule forme connue à l'époque, sa forme classique, c'est-à-dire physique, au moyen de forces conventionnelles tels que des hommes, des chars, des avions, des navires etc…

20. Mais, avec l'évolution des technologies et le développement d'Internet, les États ont développé de nouvelles formes de recours à la force à l'encontre d'autres États, qui sont réalisées de manière dématérialisée (à travers l'utilisation du cyberespace), mais n'en demeurent pas moins susceptibles d'entraîner des conséquences similaires. Cette nouvelle pratique est une faille dans le système de l'O.N.U. prohibant de tels

[30] Charte des Nations unies, article 1er
[31] *Ibid*. article 2 § 4
[32] *Ibid*. article 2 § 3

agissements car ils n'existaient pas encore lors de la rédaction de la Charte et ne sont donc pas pris en compte par le droit international moderne développé depuis l'avènement des Nations unies, et dont la prohibition du recours à la force et des agressions interétatiques est la pierre angulaire[33]. En effet, les États contournent cette prohibition et utilisent de plus en plus les cyberattaques pour s'attaquer à d'autres États, en complément ou à la place des moyens conventionnels. Les cyberattaques sont donc un nouveau moyen pour les États de contourner cette interdiction du recours à la force et de réaliser de tels actes contre les autres États sans être sanctionnés.

21. Par conséquent, étant donné que les cyberattaques permettent aux États de remplir les mêmes objectifs que des attaques conventionnelles, cela indique qu'elles servent la même logique d'attaque. La pratique actuelle des États démontre de plus qu'elles sont véritablement utilisées comme des armes par les États[34]. Enfin, les conséquences peuvent être aussi graves que des attaques conventionnelles. Il est vrai qu'aucune cyberattaque n'a permis encore à ce jour de causer de tels dégâts mais cet état de fait provient surtout du manque de moyen des États à lancer de tels actes. Or, les États ont décidé de développer leurs connaissances et leurs capacités en la matière, comme en témoigne la création de nombreux programmes de défenses cybernétiques, ainsi que l'insertion des cyberattaques dans les tactiques de combat des États. Il est donc à craindre que le développement des armes cybernétiques entraine à terme des cyberattaques à même d'entraîner les mêmes conséquences que des attaques conventionnelles, voire pire, car les cyberattaques brouillent la distinction entre civils et militaires.

22. C'est pourquoi ce mémoire se positionne en faveur d'une règlementation portant sur l'utilisation des cyberattaques, calquée sur celle existant déjà pour les attaques conventionnelles tout en tenant compte des spécificités des cyberattaques. Selon ce mémoire, il apparaît donc nécessaire de condamner l'utilisation des cyberattaques quand celles-ci correspondent à une utilisation illicite, contraire aux règles et principes du droit international, notamment quand elles constituent des recours à la force, et en particulier quand ces derniers ont atteint le seuil de gravité permettant leur qualification en agression voire en agression armée.

---

[33] C.I.J., « *Activités armées sur le territoire du Congo* », REC. 2005, § 148

[34] BAUDIN Laura, « *Les cyberattaques dans les conflits armées* », éditions L'Harmattan, 2014, p. 9-10 (préface)

23. Si le Droit International Humanitaire (D.I.H.) permet d'appliquer un standard de règles (en attendant une meilleure réglementation) pour les cyberattaques lancées lors des conflits armés, il faut toutefois dès aujourd'hui se pencher sur la création d'un corps de règles spécifiques aux cyberattaques, applicables en temps de guerre comme en temps de paix. En effet, les cyberattaques peuvent être utilisées au sein d'un conflit déjà existant, en complément des forces conventionnelles, mais elles peuvent aussi être utilisées à leur place, ce qui en temps de paix, selon leurs conséquences, peut être considéré comme une agression.

24. Il est nécessaire, à cette fin, d'adopter une vision évolutive de la notion d'agression afin de pouvoir prendre en compte ce nouveau danger pour la paix et la sécurité internationales que sont les cyberattaques. Cela appelle donc à une extension de la notion d'agression afin qu'elle puisse englober, en plus des attaques conventionnelles, les cyberattaques. Or, cela est un défi auquel seuls les juristes peuvent apporter une solution car se pose alors la question de déterminer en quoi les attaques conventionnelles et les cyberattaques sont similaires au point d'être regroupées au sein de la même notion et de pouvoir recevoir la même qualification juridique d'agression, dans le but de répondre à cette nécessité du droit international d'être toujours à même d'encadrer les agissements des États. Ce mémoire se positionne donc en faveur d'une extension de la notion d'agression étant donné que les cyberattaques étatiques peuvent être des recours à la force constituant des agressions, et qu'il est nécessaire que le droit international prenne en compte ce constat.

25. La méthode utilisée est une méthode comparative entre, d'une part, les recours à la force conventionnels que la notion d'agression actuelle appréhende et, d'autre part, les nouveautés que constituent les cyberattaques que la nouvelle notion d'agression doit aussi traiter.

26. Pour ce faire, seront traités tout au long du mémoire ce qui est perçu par le droit comme une agression, la réalité en pratique et les conséquences juridiques d'une agression, avec une mise en perspective de ce que ce régime juridique impliquerait pour les cyberattaques, notamment au vu de leur pratique actuelle mais aussi en tenant compte de la potentielle pratique future que les États sont en train de développer.

27. C'est ainsi que le présent mémoire entend démontrer le besoin de reconnaître que les cyberattaques peuvent être des recours à la force constituant des agressions, afin de fournir un encadrement juridique à ces nouvelles pratiques étatiques.

28. Ce mémoire traitera spécifiquement des cyberattaques étatiques. Il n'abordera pas la question des cyberattaques orchestrées par des particuliers, sauf dans le cas où elles sont attribuables à un État. Toute cyberattaque menée par une personne privée et non attribuable à un État selon les règles du droit international public ne sera traité dans ce mémoire. Dans le même esprit il ne sera pas fait mention de la cybercriminalité, du cyberhacktivisme ou du cyberterrorisme en particulier, mais uniquement des cyberattaques attribuables à un État de manière générale, soit des cyberattaques étatiques.

29. Ce mémoire traitant des cyberattaques étatiques et de leurs conséquences, ne sera pas abordée la question de la responsabilité individuelle pénale des personnes privées responsables de cyberattaques. Il ne sera fait mention des personnes privées que pour leur rôle dans la perpétration de cyberattaques étatiques dans le cadre de l'attribution de cyberattaques, pour engager la responsabilité internationale de l'État responsable.

30. Ce mémoire s'attachera exclusivement à la question de l'agression, à la mise en perspective de sa pratique et de son régime juridique avec les cyberattaques afin de fournir un aperçu des règles générales qu'il serait souhaitable d'appliquer afin d'en règlementer leur utilisation. L'objectif de ce mémoire est de démontrer que les États peuvent réaliser des agressions par le biais des cyberattaques, et qu'il faut donc étendre la notion d'agression à ces dernières. Son but n'est pas de traiter la totalité du régime juridique en la matière. Bien qu'il se situe entre le *jus ad bellum* et le *jus in bello*, le *jus in bello* ne sera ici abordé que pour démontrer qu'un encadrement juridique est possible et nécessaire en ce qui concerne le *jus ad bellum*, ou qu'il peut permettre d'aider à la mise en place du *jus ad bellum* notamment dans les ripostes aux cyberattaques. Ce mémoire n'a pas pour objectif de traiter des cyberattaques dans les conflits armés, seulement de leur recours en tant qu'arme pour réaliser des agressions. Il ne sera fait mention du D.I.H. et des conflits armés que pour étayer la thèse selon laquelle les cyberattaques sont de nouvelles armes aux mains des États, pouvant réaliser des agressions par leur biais.

31. De même, ce mémoire aborde un certain nombre de points juridiques extrêmement controversés en ce qui concerne l'agression. Il n'a cependant pas pour ambition de parvenir à trancher ces débats doctrinaux ô combien épineux, mais de transposer les règles juridiques applicables aux agressions via des moyens conventionnels à celles réalisées par des cyberattaques. Les éléments indéterminés en matière d'agression conventionnelle telle que la question du seuil de gravité entre l'agression et l'agression armée seront donc transposés tels quels, selon les règles du droit international public, et directement appliqués aux cyberattaques. Il sera fait de même avec tous les points discutés en doctrine : la position de référence qui sera donnée pour chaque controverse sera, dans les cas où elle existe, la position appliquée par la Cour Internationale de Justice (C.I.J.). Dans les cas où celle-ci a pris une position nuancée, il sera fait mention de la doctrine dominante en adéquation avec les différentes possibilités proposées.

32. Enfin, ce mémoire n'a pas pour but de déterminer si une cyberattaque est une agression en droit international selon la résolution 3314 de l'Assemblée Générale des Nations unies tel que l'a analysé Evelyne Akoto dans son article « *Les cyberattaques étatiques constituent-elles des actes d'agression en vertu du droit international public* »[35], mais du fait que les cyberattaques doivent être considérées comme des agressions au vu de leur pratique qui entre en contradiction avec les principes et les règles du droit international public. Ce mémoire s'oriente donc en faveur d'une extension de la notion d'agression au vu de la pratique des États en violation du droit international public, et tente d'en tirer les conséquences concernant la responsabilité internationale et les mesures possibles en riposte. La résolution 3314 ne sera abordée qu'à l'appui de cette argumentation, afin de justifier cette extension de la notion d'agression.

33. Après avoir étudié au cours de mon cursus universitaire les cyberattaques en droit international, je me suis rendu compte du manque flagrant de règles spécifiques en la matière et de la stratégie des États d'en profiter pour contourner le droit international de manière de plus en plus récurrente.

[35] AKOTO Evelyne, « *Les cyberattaques étatiques constituent-elles une agression en droit international public ?* » : Première partie. Revue de droit d'Ottawa - Ottawa Law Review, Faculty of Law, Common Law Section, University of Ottawa, 2015, 46 (1), pp.1. http://www.rdoolr.uottawa.ca/subsite/olr/ <hal-01244603> p. 1

34. Après avoir mis en corrélation l'absence de droit en la matière, qui tranche avec le recours aux cyberattaques de plus en plus récurrent, et l'absence de condamnation des États en raison certes de difficultés d'attribution, mais également de règles juridiques qui ne prennent pas en compte les cyberattaques, il m'a semblé opportun de rédiger un mémoire proposant non pas de créer un corpus de règles spécifiques aux cyberattaques (bien que cela sera un jour nécessaire), mais d'encourager la transposition des règles et principes du droit international existant aux cyberattaques, afin que les nouvelles technologies ne permettent pas aux États de contourner leurs obligations et les interdits qu'elles leurs posent. J'ai donc débuté mes recherches au cours desquelles j'ai pu constater que de nombreux auteurs cités dans le présent mémoire envisageaient que les cyberattaques puissent être des agressions. La problématique de ce mémoire porte donc sur la question centrale suivante :

Les cyberattaques étatiques justifient-elles une extension de la notion d'agression en droit international dans laquelle elles seraient incluses ?

35. Le présent mémoire traitera donc dans une première partie des similarités qu'il existe entre une attaque conventionnelle et une cyberattaque, et *de facto* la possibilité pour l'une comme pour l'autre d'être un recours à la force constituant une agression, ce qui va en faveur de l'extension de la notion d'agression. La deuxième partie, quant à elle, abordera les différentes conséquences qui naîtraient de cette extension de la notion d'agression aux cyberattaques, que ce soit en matière de responsabilité internationale de l'État ou au sujet des différentes mesures qui pourraient être prises en riposte.

Partie I : Le besoin d'extension de la notion d'agression.

Dans cette partie, nous allons faire un état des lieux de l'agression et des cyberattaques en droit international et dans la pratique des États. Au vu du constat qui en sera tiré, nous aborderons ensuite le besoin de faire évoluer la notion d'agression en droit international afin de l'étendre aux cyberattaques étatiques.

Chapitre 1 : Les règles juridiques consacrées par le droit international et les pratiques des États.

Dans ce chapitre, nous verrons la situation actuelle de l'agression et des cyberattaques, c'est-à-dire si le droit international prévoit un encadrement juridique pour elles, et où en est la pratique des États, aussi bien en matière d'agression qu'en matière de cyberattaque.

Section 1 : État des lieux juridique et pratique de l'agression.

Au sein de cette section, il sera spécifiquement question de l'encadrement juridique et de la pratique étatique de l'agression.

Paragraphe 1 : Les règles juridiques de l'agression en droit international.

Dans ce paragraphe seront traitées les règles juridiques internationales en matière d'agression.

36. Le système actuel des Nations unies est le fruit d'une longue évolution. Déjà, en 1919 soit au lendemain de la Première Guerre mondiale, le Pacte Drago-Porter avait prohibé la guerre d'agression. Puis, en 1929, le Pacte Briand-Kellog avait interdit les guerres défensives. Ce fut enfin la Charte de San Francisco en 1945 qui prohiba la menace et l'emploi du recours à la force.

37. Le système des Nations unies repose donc sur cette interdiction de la guerre entre les États afin de maintenir la paix et la sécurité internationales. Les menaces de recours à

la force, l'emploi de la force ainsi que les agressions sont donc prohibés au sein de ce système de sécurité collective dont le Conseil de sécurité est la pierre angulaire[36]. Il est le seul à pouvoir autoriser un recours à la force[37], hormis l'unique exception de la légitime défense. Toute attaque qui aurait lieu en dehors des cas d'autorisation du Conseil de sécurité et des situations de légitime défense serait donc considérée comme un recours à la force illicite et donc comme une agression d'un État contre un autre État.

38. Il est important de souligner une nuance dans l'agression. Un recours à la force d'un État contre un autre État peut entrainer la qualification d'agression de cet acte. Un recours à la force armée sera également qualifié d'agression. Toutefois, tous les recours à la force, même armée, ne sont pas des agressions et seule « *la forme la plus grave et la plus dangereuse de l'emploi illicite de la force* »[38] entraîne la qualification d'agression. Il faut que les recours à la force armée atteignent une certaine intensité, un simple incident de frontière n'étant pas considéré comme une agression[39]. En revanche, seuls les recours à la force armée les plus graves ouvrent la voie de la qualification d'agression armée. Il existe donc deux seuils dans la qualification des recours à la force. Une certaine intensité du recours à la force ou du recours à la force armée est requise pour dépasser le premier seuil. Celui-ci ouvre la voie de la qualification d'agression. Puis, une intensité encore plus élevée est demandée afin d'atteindre le second seuil, comprenant seulement les recours à la force armée les plus graves et qui permet la qualification d'agression armée. Le présent mémoire tend à démontrer qu'une cyberattaque peut être similaire à un recours à la force et, ainsi, constituer une agression au sens de l'article 39 de la C.N.U. Il n'a pas pour but de démontrer que les cyberattaques peuvent constituer un des recours à la force les plus graves, c'est-à-dire constituant une agression armée au sens de l'article 51 de la C.N.U., bien que cette hypothèse soit soulevée au cours du mémoire pour envisager la possibilité de recourir à la légitime défense en riposte à une cyberattaque étatique constituant une agression. [40]

---

[36] En ce sens *v*. COT Jean-Pierre, PELLET Alain, FORTEAU Mathias, « *La Charte des nations unies commentaire article par article* », éditions Economica (3ème édition), 2005, p. 1131

[37] En ce sens *v*. Charte des Nations unies, chapitre VII

[38] COT Jean-Pierre, PELLET Alain, FORTEAU Mathias, « *La Charte des nations unies commentaire article par article* », éditions Economica (3ème édition), 2005. p. 217

[39] C.I.J. « *Affaire du temple de Préah Vihéar* » (Cambodge *c.* Thaïlande), Fond, Arrêt du 15 juin 1962 : Recueil 1962, p. 6

[40] En ce sens *v*. AKOTO Evelyne, « *Les cyberattaques étatiques constituent-elles une agression en droit international public ?* » : Première partie. Revue de droit d'Ottawa - Ottawa Law Review, Faculty of Law, Common Law Section, University of Ottawa, 2015, 46 (1), pp.1. http://www.rdoolr.uottawa.ca/subsite/olr/ <hal-01244603>

39. Lorsque les État réalisent une agression, cela est susceptible de déclencher des réactions de l'État victime, du Conseil de sécurité voire de l'ensemble de la communauté internationale si ce dernier donne son autorisation.

40. Si le Conseil de sécurité a souvent qualifié des attaques, prenant la forme de recours à la force, de menace à la paix ou de rupture de la paix, il n'a jamais qualifié ces situations d'agression. Pour autant, même s'il choisit délibérément une autre terminologie, il s'applique à sanctionner tous les cas de recours à la force constitutif d'une agression étatique. La résolution 3314 de l'A.G.N.U. a d'ailleurs précisé que l'emploi de la force armée est bien constitutif d'une agression quand bien même le Conseil de sécurité ne l'établirait pas au vu des autres circonstances pertinentes[41]. En d'autres termes, quand bien même le Conseil de sécurité décide, souvent pour des raisons politiques, de ne pas qualifier la situation d'agression mais de rupture de la paix, juridiquement, un recours à la force est une agression.

41. Cependant, il est important de souligner que l'agression en elle-même n'a pas été clairement définie en droit international et ceci parce que le fait de définir cette notion entraînerait une limitation inéluctable de sa capacité d'appréciation[42]. Or, les Nations unies préfèrent garder cette notion d'agression la plus large possible, afin que le Conseil de sécurité conserve son pouvoir discrétionnaire en la matière.

42. Pour autant, bien qu'elle ne soit pas définie conventionnellement, l'agression est bel et bien prohibée en droit international. Le Tribunal de Nuremberg constatait en 1945 que « *les guerres et invasions d'agression ont de tout temps constitué une violation du droit international, même si des sanctions spécifiques ne faisaient pas partie des règles de l'époque* ».[43]

43. Le Tribunal annonçait le prélude de la mise « *hors la loi* »[44] des actes d'agression par le système des Nations unies. La prohibition des agressions est posée par l'article 2 paragraphe 4 de la C.N.U. qui dispose que « *les membres de l'organisation*

[41] A.G.N.U résolution A/RES/3314 (XXIX), article 2
[42] En ce sens *v*. COT Jean-Pierre, PELLET Alain, FORTEAU Mathias, « *La Charte des nations unies commentaire article par article* », éditions Economica (3ème édition), 2005, p. 1133
[43] KAMTO Maurice, « *L'agression en droit international* », éditions Pédone, 2010, p. 6
[44] En ce sens *v*. C.I. J. « *Barcelona Traction, Light and Power Company* », Limited, arrêt, C.I.J. Recueil 1970, p. 3. § 34, p. 32

s'abstiennent, dans leurs relations internationales, de recourir à la force ou à l'emploi de la force, soit contre l'intégrité territoriale ou l'indépendance politique de tout l'État, soit de manière incompatible avec les buts des Nations unies ». La Cour Internationale de Justice a elle-même reconnu la valeur coutumière de ce principe dans l'affaire des Activités militaires et paramilitaires au Nicaragua et contre celui-ci de 1986[45]. Ce principe interdit tout recours à la force, de la simple menace du recours à la force à l'agression d'un État contre un autre État.[46] Une différence est cependant faite entre les recours à la force, les agressions, et les agressions armées. La C.I.J. elle-même a précisé cela dans l'affaire des Activités militaires et paramilitaires au Nicaragua et contre celui-ci car tout emploi de la force n'est pas automatiquement qualifié d'agression armée[47]. En revanche, une agression armée, elle, est forcément un recours à la force.

44. Bien que l'agression n'ait pas de définition obligatoire en droit international posée conventionnellement, il existe cependant une définition de l'A.G.N.U. En effet l'A.G.N.U., dont les résolutions sont non-obligatoires, l'a défini dans sa résolution 3314 comme « *l'emploi de la force armée par un État contre la souveraineté, l'intégrité territoriale ou l'indépendance politique d'un État de toute autre manière incompatible avec la Charte des Nations unies ainsi qu'il ressort de la présente définition*. »[48] Elle a de plus précisé les différents actes constitutifs d'une agression[49]. Si cette résolution n'a pas de force obligatoire (puisqu'elle provient de l'A.G.N.U.), ayant été adoptée par consensus, elle est considérée par les États et selon la C.I.J. comme l'acceptation d'une coutume internationale [50].

45. L'A.G.N.U. a précisé dans le préambule de sa résolution que la définition de l'agression avait été nécessaire étant donné que c'est l'un des objectifs des Nations unies de maintenir la paix et la sécurité internationales en réprimant tout acte d'agression ou de rupture de la paix, que l'agression est particulière car elle est *« la forme la plus dangereuse de l'emploi illicite de la force, qui renferme, étant donné l'existence de tous les types d'armes de destruction massive, la menace possible d'un conflit mondial avec*

[45] C.I.J. « *Affaire des Activités militaires et paramilitaires au Nicaragua et contre celui-ci* » du 27 juin 1986 (Nicaragua *c.* États-Unis d'Amérique), fond, arrêt, Recueil 1986, § 190, p. 100
[46] En ce sens *v*. KAMTO Maurice, « *L'agression en droit international* », éditions Pédone, 2010, p. 12
[47] *Ibid*.
[48] A.G.N.U résolution A/RES/3314 (XXIX), article 1er
[49] *Ibid*. article 3 g)
[50] C.I.J. « *Affaire des Activités militaires et paramilitaires au Nicaragua et contre celui-ci* » du 27 juin 1986 (Nicaragua *c.* États-Unis d'Amérique), fond, arrêt, Recueil 1986, § 190-191, p.102

toutes ses conséquences catastrophiques »[51], et enfin pour dissuader les éventuels auteurs de tels actes.[52]

46. Pour être qualifiée comme telle, une agression doit être un recours à la force armée. Son ampleur n'est pas précisée. Une agression doit remplir plusieurs critères. Ce doit être un recours à la force qui viole la C.N.U. (c'est-à-dire ni autorisé par le Conseil de sécurité, ni justifié par l'exercice de la légitime défense), réalisé en premier par l'État et d'une gravité suffisante, atteignant la souveraineté, l'intégrité territoriale, l'indépendance politique ou étant incompatible avec la C.N.U.[53].

47. Ces actes de recours à la force armée constitutifs d'une agression peuvent être des invasions, des attaques militaires, des occupations militaires, des annexions, des bombardements, l'emploi de toute arme par un État contre le territoire d'un autre État, le blocus des ports ou des côtes, l'attaque des forces armées par les forces armées d'un autre État, l'utilisation de forces armées sur le territoire d'un autre État en contradiction avec l'accord de stationnement, l'envoi par un État de bandes ou de groupes armés, de forces irrégulières ou de mercenaires se livrant à des actes de forces armée contre un autre État d'une telle gravité qu'ils équivalent aux actes énumérés ci-dessus, ou le fait de s'engager de manière substantielle dans un tel acte[54]. Cette liste des critères constitutifs de l'agression est toutefois non-exhaustive et peut ainsi être complétée.

48. Quelques critères constitutifs de l'agression sont particulièrement intéressants pour les cyberattaques. Dans la résolution 3314, il a été précisé que l'attaque par les forces armées d'un État contre un autre État peut constituer une agression. Cela renvoie à la situation où « *les forces armées en question exercent au moyen de matériels militaires notamment les armes de guerre une violence dans un but offensif contre des objectifs militaires, voire parfois sans distinction entre biens civils et biens militaires. […] On parle d'attaque armée de grande ampleur dans le cas de l'agression* »[55]. En 1986, la C.I.J. a estimé qu'une agression n'était pas une simple opération militaire transfrontalière mais une véritable attaque armée « *par l'action des forces armées régulières à travers une frontière internationale mais encore l'envoi par un État ou en*

[51] A.G.N.U résolution A/RES/3314 (XXIX), préambule
[52] En ce sens *v*. KAMTO Maurice, « *L'agression en droit international* », éditions Pédone, 2010, p. 18
[53] *Ibid*. p. 19
[54] *Ibid*. p. 22
[55] *Ibid*. p. 23

son nom de bandes ou de groupes armés, de forces irrégulières ou de mercenaires se livrant à des actes de force armée contre un autre État tels qu'ils équivalent à une véritable agression armée accomplie par des forces régulières, ou au fait de s'engager d'une manière substantielle dans une telle action »[56]. Ce n'est pas un simple recours à la force, c'est un recours à la force « *visant l'intégrité, l'indépendance d'un État* »[57]. Comme nous le verrons plus tard, cet élément sera déterminant pour admettre que les cyberattaques peuvent constituer des agressions dès lors qu'elles sont utilisées comme des armes par les États.

49. L'agression, au terme de la résolution 3314, est donc un crime d'État. Puisque l'agression est prohibée au sein du système des Nations unies, sa commission est donc un fait internationalement illicite qu'aucune circonstance ne saurait justifier et qui engage de ce fait la responsabilité internationale de l'État responsable. L'agression va ainsi entrainer plusieurs conséquences sur le plan juridique.

50. Tout d'abord, le fait de réaliser une agression va engager la responsabilité de l'État responsable. C'est une nouvelle relation juridique qui va naitre entre les deux États. L'État responsable sera tenu de cesser son agression, et au besoin selon les circonstances, de donner des garanties de non-répétition à l'État victime lui assurant qu'un tel fait internationalement illicite ne se reproduira plus, si ce dernier estime qu'un simple retour à la licéité, au *statu quo ante*, ne suffit pas. L'État responsable va ensuite être tenu de réparer le préjudice causé à l'État victime, ce qui comprend tous les dommages matériels et/ou moraux. L'État victime pourra ainsi faire valoir son droit à réparation directement auprès de l'État responsable ou devant un tribunal arbitral, voire devant une juridiction permanente. L'État responsable devra alors procéder à la réparation par restitution *in integrum*, par indemnisation ou par satisfaction selon les cas[58]. La restitution *in integrum* est la réparation la plus favorisée car elle permet véritablement le recours au *statu quo ante*. Toutefois elle peut parfois ne pas être possible, ou entraîner une charge hors de toute proportion pour l'État responsable[59] : par

C.I.J. « *Affaire des Activités militaires et paramilitaires au Nicaragua et contre celui-ci* » du 27 juin 1986 (Nicaragua *c.* États-Unis d'Amérique), fond, arrêt, Recueil 1986, § 195, p. 103

[57] En ce sens *v*. RIVIER Raphaële, « *Droit International Public* » (2ème édition), éditions Presses Universitaires de France, 2012, p. 627

[58] En ce sens *v*. DUPUY Pierre-Marie et KERBRAT Yann, « *Droit International Public* », éditions Dalloz (13ème édition), 2016, p. 551

[59] *Ibid*. p. 552

exemple, en cas de destruction d'un bien. Elle peut également être incomplète pour rétablir le *statu quo ante* dans certains cas. Il sera alors possible de la remplacer ou de la compléter par une indemnisation. Enfin, la satisfaction permettra de réparer tout dommage qui ne peut pas être l'objet d'une estimation financière, c'est-à-dire les dommages immatériels, moraux, telle une atteinte à l'honneur de l'État[60]. Des excuses, ou la reconnaissance de la violation suffiront à établir cette satisfaction. C'est une nouvelle relation qui naît du fait internationalement illicite, qui pose des droits pour l'État victime et des obligations pour l'État responsable.

51. Ensuite, l'agression va avoir pour conséquence qu'elle peut entrainer l'application du droit de légitime défense des États. La légitime défense est un droit conventionnel posé par l'article 51 de la Charte des Nations unies, mais aussi un droit coutumier, reconnu par l'article 51 (« *droit naturel de légitime défense* »[61] et rappelé par la C.I.J. dans l'affaire des Activités militaires et paramilitaires au Nicaragua et contre celui-ci de 1986, en reconnaissant le « *droit naturel des États à la légitime défense* ». La légitime défense est une réponse directe à l'agression. En effet, la légitime défense n'est autorisée qu'en réponse à l'agression d'un autre État[62]. C'est la première et principale condition pour son exercice. La légitime défense doit également être nécessaire[63], immédiate, proportionnée, réalisée en l'absence de réaction du Conseil de sécurité, et portée à sa connaissance. C'est deux dernières conditions ne sont que conventionnelles[64] et ne sont pas prévues par le droit coutumier. Le principe de légitime défense a déjà été retenu, au sein du système onusien, pour des opérations militaires telles que la réaction du Royaume-Uni lors de la guerre des Malouines, ou encore l'intervention des États-Unis en Afghanistan en 2001.

52. Enfin, l'agression peut avoir pour conséquence la réaction du Conseil de sécurité. En effet, selon l'article 39 de la C.N.U.[65], le Conseil de sécurité est à même d'intervenir en

[60] En ce sens *v*. DUPUY Pierre-Marie et KERBRAT Yann, « *Droit International Public* », éditions Dalloz (13ème édition), 2016, p. 555
[61] Charte des Nations unies, article 51
[62] En ce sens *v*. RIVIER Raphaële, « *Droit International Public* », éditions Presses Universitaires de France, (2ème édition), 2012, p. 751
[63] C.I.J. « *Affaire des Activités militaires et paramilitaires au Nicaragua et contre celui-ci* » du 27 juin 1986 (Nicaragua *c.* États-Unis d'Amérique), fond, arrêt, Recueil 1986, § 194, p. 103
[64] Chartes des nations unies, article 51
[65] En ce sens *v*. RIVIER Raphaële, « *Droit International Public* », éditions Presses Universitaires de France, (2ème édition), 2012, p. 616

cas de menace à la paix, rupture de la paix ou encore d'agression. Il peut dès lors qualifier une situation comme telle et réagir en prenant des mesures provisoires, des mesures coercitives non armées[66] ou encore des mesures coercitives armées[67]. Il peut, dans les cas les plus extrêmes, autoriser les États à recourir à la force contre l'État responsable de la menace/de la rupture de la paix, ou de l'agression. Initialement, le C.S. aurait dû posséder sa propre armée et son propre centre de commandement mais cela n'ayant pas été possible il fonctionne avec un système d'autorisation, et autorise les États à recourir à la force à sa place. Le Conseil de sécurité a notamment recouru au chapitre VII de la C.N.U. pour l'Irak en 1990.[68]

53. Les agressions entraînent donc de fortes conséquences en droit international, allant de l'obligation de réparation pour l'État responsable, au droit d'obtenir réparation et de mettre en exécution son droit de légitime défense, voire à l'intervention du Conseil de sécurité lui-même.

Paragraphe 2 : La pratique des États en matière d'agression.

Dans ce paragraphe, il sera question de la pratique étatique en matière d'agression.

54. Les agressions étant prohibées par le système onusien en vertu de l'article 2 paragraphe 4 de la C.N.U., la réalisation d'un tel acte a plusieurs conséquences. Elle peut engager la responsabilité de l'État responsable, entraîner la réaction de l'État victime qui pourra aller jusqu'à recourir à la force au nom de son droit à la légitime défense, et/ou déclencher l'intervention du Conseil de sécurité qui pourra se saisir de la situation, la qualifier de menace ou de rupture de la paix, voire d'agression, ce qui lui permettra d'appliquer les articles 40, 41, et 42 de la C.N.U. Toutefois, bien que les recours à la force soient interdits, cela n'a pas empêché certains États de réaliser des recours à la force sous leur forme la plus grave et de constituer, de ce fait, des agressions. Les Nations unies réagissent donc dès que possible à ces agressions. Le Conseil de sécurité en particulier a eu à faire face à plusieurs cas d'agressions.

---

[66] En ce sens *v*. RIVIER Raphaële, « *Droit International Public* », éditions Presses Universitaires de France, (2ème édition), 2012, p. 619
[67] *Ibid*. p. 621
[68] *Ibid*. p. 616

55. Tout d'abord, la Rhodésie du Sud a réalisé plusieurs actions d'agressions contre plusieurs États d'Afrique notamment contre la Zambie. En effet, en 1976, la Rhodésie, en guerre contre une guérilla depuis 1966, lance des attaques contre des bases d'entrainement situées au Mozambique et en Zambie. Ces raids, réalisés de 1976 à 1980, ont entrainé la mort de nombreux réfugiés. Dans sa résolution 424 du 17 mars 1978[69], le C.S. les a qualifiés « *d'actes d'agression et d'hostilités* », ainsi que « *d'actes d'agression contre des États voisins constituant une menace contre la paix, et violant la souveraineté et l'intégrité territoriale de ces pays* ».[70]

56. Le Conseil de sécurité s'est également intéressé aux actes de l'Afrique du Sud à partir de 1976 et ce jusqu'à 1987, qui a notamment commis des actes d'agression contre l'Angola. En effet, des affrontements avaient lieu depuis 1976 entre le Mouvement Populaire de Libération de l'Angola, idéologiquement marxiste, et l'Union pour l'Indépendance Totale de l'Angola soutenue par les États-Unis et l'Afrique du Sud. L'Afrique du Sud intervient alors militairement de manière récurrente pour aider l'UNITA à combattre le MPLA et sécuriser par la même occasion sa colonie du Sud-Ouest Africain (actuelle Namibie) dont les bases arrières sont installées en Angola.[71] Le C.S. a qualifié la situation « *d'actes d'agression commis par l'Afrique du Sud contre l'Angola en violation de la souveraineté et de l'intégrité* territoriale de ce pays » et a condamné « *l'agression de l'Afrique du Sud contre l'Angola* ».[72] Le Conseil de sécurité a, par la suite, rappelé le droit de l'Angola de prendre les mesures nécessaires, en citant tout particulièrement l'article 51. Le Conseil de sécurité a ici visé expressément le droit de légitime défense de l'Angola. Le C.S. a également réaffirmé le droit de l'Angola d'obtenir une réparation pour cette agression dont l'Afrique du Sud était responsable.

57. En 1985, le C.S a également condamné des attaques réalisées par Israël contre la Tunisie. A la suite de l'assassinat de trois touristes israéliens le 25 septembre 1985 par deux palestiniens et un ressortissant britannique, Israël décide de bombarder le siège de

[69] En ce sens *v*. Nations Unies, « *Analyse historique des faits relatifs à l'agression* », éditions Nations unies, 2003, p. 257
[70] *Ibid*. p. 258
[71] Le Monde Diplomatique, Archives de décembre 1986, p. 24-25, https://www.monde-diplomatique.fr/1986/12/CONCHIGLIA/39702
[72] Nations Unies, « *Analyse historique des faits relatifs à l'agression* », éditions Nations unies, 2003, p. 260

l'OLP situé en Tunisie, près de la ville de Tunis[73]. Ces actes ont été qualifiés « *d'actes d'agression illicites* » par la résolution 573 du 4 octobre 1985[74]. Le Conseil de sécurité a ici rappelé le devoir d'Israël de cesser son illicéité, de remplir son obligation de non-répétition et le droit à des réparations appropriées de la Tunisie.

58. Plusieurs affaires présentées à la CI.J. concernaient la commission d'agression par recours à la force par un État. Il est ainsi possible de citer l'affaire de la frontière terrestre et maritime entre le Cameroun et le Nigéria. Le Nigéria avait décidé de contester la délimitation de sa frontière avec le Cameroun dans la région du Lac Tchad. Le Nigéria avait établi sa domination sur des îles camerounaises au moyen d'une occupation militaire et administrative des forces nigérianes, malgré les protestations camerounaises. Le différend est alors introduit devant la C.I.J. par le Cameroun le 29 mars 1994, qui rendra son arrêt le 10 octobre 2002, rejetant les prétentions nigérianes sur ces îles. En 2006, à la suite d'un accord signé entre le Nigéria et le Cameroun, le Nigéria retirera finalement ses troupes de ces îles en août 2008.

59. Il est aussi possible de citer l'affaire des Activités armées au Congo où le Congo accusait l'Ouganda d'agression en violation de l'article 2 paragraphe 4 de la C.N.U.[75] L'Ouganda était intervenu militairement au Congo, en envoyant des forces régulières et en soutenant des groupes armés œuvrant au Congo. L'Ouganda souhaitait sécuriser ses frontières avec le Congo mais aussi piller les ressources congolaises (notamment minières), empêcher l'émergence d'une puissance congolaise forte ainsi que de concurrencer le Rwanda, également très actif dans la région. L'affaire sera introduite par le Congo en 1999. La C.I.J. rendra son arrêt le 19 décembre 2005.[76] Elle reconnaît l'agression de la République Démocratique du Congo (R.D.C.) contre lui et profitera d'ailleurs de cette affaire pour réaliser une liste non exhaustive des actes qui peuvent constituer une agression. Parmi ceux-ci figurent les blocus, les invasions, les bombardements, les attaques contre une force armée, le fait de ne pas se retirer conformément à un accord de stationnement, la mise à disposition du territoire à des

[73] En ce sens *v*. ROUSSEAU Charles, « *Chronique des faits internationaux* », RGDIP, 1986, p. 457
[74] En ce sens *v*. Nations Unies, « *Analyse historique des faits relatifs à l'agression* », éditions Nations unies, 2003, p. 267
[75] *Ibid*. p. 296
[76] Le Monde, « *L'Ouganda condamné par le Cour Internationale de justice pour son action en R.D.C.* », 19 décembre 2005, http://www.lemonde.fr/afrique/article/2005/12/19/l-ouganda-condamne-par-la-cour-internationale-de-justice-pour-son-action-en-rdc_722771_3212.html

fins d'agressions et l'envoi de bandes de mercenaires et de groupes armés. La C.I.J. rappelle enfin qu'une agression armée peut donner lieu à l'application du droit de légitime défense.

60. Enfin, une affaire notable doit être citée, bien que l'agression n'ait pas été reconnue par la C.I.J., : l'affaire des Activités militaires et paramilitaires au Nicaragua et contre celui-ci le Nicaragua de 1986[77]. Dans cette affaire, le Nicaragua avait allégué devant la Cour avoir été victime d'une violation de l'article 2 paragraphe 4 de la C.N.U. de la part des États-Unis. En 1979, la révolution sandiniste prend la tête du gouvernement. Proches de l'URSS, les Sandinistes mettent en place un régime communiste. La CIA aide alors les Contras, une force contre-révolutionnaire, dans leur lutte contre les Sandinistes. Les États-Unis fourniront notamment un soutien financier, logistique et un encadrement pour former les Contras au travers de la CIA. A la suite d'exactions commises par les Contras durant la guerre opposant le gouvernement sandiniste aux Contras, et à des opérations de sabotage des États-Unis qui ont notamment miné des ports nicaraguayens et réalisé un embargo à l'encontre du Nicaragua, l'affaire sera portée devant la C.I.J.

61. Le 9 avril 1984, le Nicaragua dépose une requête à l'encontre des États-Unis assortie d'une demande de mesures conservatoires. Le 10 mai 1984, la Cour rend une ordonnance de mesures conservatoires, puis reconnaît sa compétence par un arrêt le 26 novembre 1984 et rend son arrêt sur le fond le 27 juin 1986. Si elle ne retient pas l'agression des États-Unis contre le Nicaragua, elle pose cependant le principe selon lequel une agression peut être réalisée « *par l'action des forces armées régulières à travers une frontière internationale mais encore l'envoi par un État ou en son nom de bandes ou de groupes armés, de forces irrégulières ou de mercenaires […] dans une telle action* »[78]. Elle pose également le principe du « *contrôle effectif* » [79] car, pour de tels agissements, elle estime qu'un degré particulièrement élevé de contrôle est requis afin de ne pas distordre la responsabilité des États, qui ne peuvent être responsables que de leur fait (leurs organes) ou du fait des organes sous leur contrôle. Cet arrêt est essentiel en matière d'agression étatique car elle pose le critère retenu par la C.I.J. pour attribuer ou non les agissements d'individus à un État, et donc retenir ou non une

[77] C.I.J. « *Affaire des Activités militaires et paramilitaires au Nicaragua et contre celui-ci* » du 27 juin 1986 (Nicaragua *c.* États-Unis d'Amérique), fond, arrêt, Recueil 1986
[78] *Ibid.*
[79] *Ibid.*

agression de l'État en question. L'application de ce critère devant la C.I.J. sera rappelée lors de l'affaire opposant la Serbie à la Bosnie en 2007.[80]

62. Si des agressions font l'objet de l'attention du Conseil de sécurité, ou sont introduites devant la C.I.J., d'autres donnent lieu à des conséquences beaucoup plus graves et spectaculaires, pouvant aller jusqu'à des réponses incluant des recours à la force armée licites. Ces recours à la force armée sont alors autorisés par le Conseil de sécurité, ou entrent dans le cadre de la légitime défense.

63. En août 1990, l'Irak envahi le Koweït. Il prend possession du pays en quatre heures et décide d'occuper militairement le pays. Le C.S qualifie alors la situation de menace à la paix et demande à l'Irak de se retirer. L'Irak refuse d'obtempérer ce qui pousse le Conseil de sécurité à qualifier d'agression, dans sa résolution 667[81], les agissements de l'Irak. En qualifiant la situation de menace à la paix, le Conseil de sécurité entre ainsi dans le champ du chapitre VII de la C.N.U. Il remplit ainsi son obligation de qualification de la situation qui lui ouvre la voie des articles 40, 41 et 42 de la C.N.U. Le Conseil de sécurité prend alors plusieurs mesures. Il utilise notamment l'article 41 de la C.N.U. pour mettre en place un embargo général contre l'Irak afin d'exercer des pressions, celles-ci devant amener l'Irak à se conformer aux résolutions du Conseil de sécurité. Mais l'Irak refuse toujours de mettre fin à son invasion du Koweït et à son annexion militaire. Dans sa résolution 678, le Conseil de sécurité utilise alors l'article 42 de la C.N.U. pour autoriser le recours à la force des États contre l'Irak. Cette autorisation est « *l'avènement de la nouvelle ère de la sécurité collective* »[82]. Etant donné que le Conseil de sécurité ne dispose pas de forces armées propres, il fonctionne alors par un système d'habilitation et autorise les États à recourir à la force contre l'Irak à sa place. Ce recours à la force des États contre l'Irak dans le cadre d'une habilitation du Conseil de sécurité, l'opération *« Tempête du désert* »[83] est un succès. L'Irak est vaincu par la Coalition et le Conseil de sécurité met en place le désarmement de l'Irak et la fin de la crise dans sa résolution 687. C'est la première fois que le Conseil de

[80] C.I.J. « *Application de la convention pour la prévention et la répression du crime de génocide* » du 26 février 2007 (Bosnie-Herzégovine *c.* Serbie-et-Monténégro), fond, arrêt, Recueil 2007
[81] En ce sens *v*. Nations Unies, « *Analyse historique des faits relatifs à l'agression* », éditions Nations unies, 2003, p. 269
[82] KREIPE Nils, « *Les autorisations données par le Conseil de sécurité des nations unies à des mesures militaires* », éditions Lextenso, 2009, p. 1
[83] *Ibid*. p. 68

sécurité autorise un recours à la force contre un État à des fins coercitives en vertu du chapitre VII de la C.N.U., en particulier de manière explicite[84].

64. Si les agressions peuvent amener les États à agir après avoir été habilités par le Conseil de sécurité, elles peuvent aussi fonder une application du droit à la légitime défense des États. Cela a notamment été le cas pour les États-Unis. Le 11 septembre 2001, les États-Unis sont victimes d'une attaque terroriste de grande envergure. Ces attentats sont revendiqués par l'organisation terroriste Al-Qaïda, dont les principales bases sont en Afghanistan. Les États-Unis attribuent alors la responsabilité des attaques au régime Taliban qui dirige l'Afghanistan et qui a permis à l'organisation terroriste d'Al-Qaïda d'établir ses bases en Afghanistan. Rattacher ces actes au régime Taliban permet de fonder leur caractère étatique et donc de considérer que ces attaques sont une agression. Les États-Unis invoquent alors leur droit de légitime défense individuelle[85] coutumier consacré par l'article 51 de la C.N.U. Leurs alliés, quant à eux, invoquent la légitime défense collective, ce qui leur permet d'intervenir militairement en Afghanistan contre les Talibans et Al-Qaïda. Cette intervention sera plus tard avalisée par le Conseil de sécurité.[86]

65. Les agressions peuvent donc donner lieu à un examen du Conseil de sécurité, à un règlement pacifique notamment par la CIIJ, mais elles peuvent aussi avoir pour conséquences des recours à la force licites, soit par autorisation du Conseil de sécurité, soit par l'application du doit de légitime défense des États.

Section 2 : États des lieux juridique et pratique des cyberattaques.

Au sein de cette section, sera abordé le manque de règles juridiques spécifiques aux cyberattaques, en contradiction avec l'utilisation de plus en plus récurrente des cyberattaques par les États.

[84] En ce sens *v*. KREIPE Nils, « *Les autorisations données par le Conseil de sécurité des nations unies à des mesures militaires* », éditions Lextenso, 2009, p. 67
[85] En ce sens *v*. LAGOT Daniel, « *Le droit international et les guerres de notre temps* », éditions L'Harmattan, 2016, p. 48
[86] *Ibid*. p. 120

Paragraphe 1 : L'absence de règles juridiques spécifiques aux cyberattaques, un vide juridique difficilement comblé.

Dans ce paragraphe, il sera question du manque de règlementation internationale spécifique en matière de cyberattaque étatique, manque qui permet aux États de les utiliser à mauvais escient.

66. Si les agressions classiques sont anciennes, les cyberattaques, quant à elles, sont une nouveauté. Elles sont apparues avec le développement des nouvelles technologies, d'Internet et ainsi du cyberespace. Internet est un « *ensemble de réseaux informatiques privés et publics interconnectés grâce à un protocole de communication en commun […] conçus par les milieux américains de la défense et de la recherche dans les années 1960* ».[87]

67. C'est avec le développement d'Internet que les cyberattaques sont apparues. Le terme de cyberattaque est un « *néologisme formé à partir du préfixe cyber et du substantif attaque* ».[88] Le terme de cyberespace, qui peut être analysé à la lumière de plusieurs prismes, sera envisagé dans ce mémoire dans le sens de réseau, c'est-à-dire « *comme cet espace virtuel des ordinateurs reliés entre eux grâce à des réseaux, constitue un environnement global qui est le siège d'évènements ayant des conséquences juridiques* »[89].

68. Par conséquent, il représente « *un espace universel « constitué d'un réseau interdépendant d'infrastructures informatiques comprenant l'Internet, les réseaux de télécommunications, les systèmes informatiques ainsi que les processeurs et les contrôleurs intégrés* ».[90] Les cyberattaques étatiques peuvent donc être « *une agression contre les systèmes qui organisent, qui dirigent* »,[91] soit ceux des autres États, ce qui se confirme au vu de la pratique des États.

---

[87] BAUDIN Laura, « *Les cyberattaques dans les conflits armées* », éditions L'Harmattan, 2014, p. 16
[88] AKOTO Evelyne. « *Les cyberattaques étatiques constituent-elles des actes d'agression en vertu du droit international public* » : Première partie. Revue de droit d'Ottawa - Ottawa Law Review, Faculty of Law, Common Law Section, University of Ottawa, 2015, 46 (1), pp.1. p. 6
[89] TRUDEL Pierre, « *Droit du cyberespace* », éditions Thémis, 1997, p. 1-15
[90] AKOTO Evelyne. « *Les cyberattaques étatiques constituent-elles des actes d'agression en vertu du droit international public » ?* : Première partie. Revue de droit d'Ottawa - Ottawa Law Review, Faculty of Law, Common Law Section, University of Ottawa, 2015, 46 (1), pp.1. p. 6
[91] BAUDIN Laura, « *Les cyberattaques dans les conflits armées* », éditions L'Harmattan, 2014, p. 23

69. Ce nouvel espace qu'est le cyberespace est rapidement devenu un terrain de choix pour les affrontements entre États, où les rapports de force peuvent s'exprimer voire s'inverser. En effet, théoriquement, un petit pays est tout à fait à même de tenir tête à une grande puissance dans le cyberespace. C'est la raison pour laquelle le cyberespace est vite devenu un espace potentiel d'affrontement entre les États. A maintes reprises, les autorités militaires de plusieurs pays, dont les États-Unis, ont qualifié le cyberespace « *d'espace de bataille* », « *d'espace de lutte* », ou encore de « *nouveau champ de bataille* ».[92] Les États ont de plus développé des stratégies militaires intégrant à part entière le cyberespace.

70. Pourtant, à ce jour, les cyberattaques étatiques ne sont pas spécialement prises en compte par le droit international[93]. Il n'existe pas de convention internationale spécifique aux cyberattaques étatiques. C'est une véritable lacune du droit international en la matière qui explique, en partie, le futur danger que peuvent représenter ces dernières.

71. Les cyberattaques étatiques ne se voient donc réglementées que par le régime général du droit international ce qui rend leur contrôle limité. Ce contrôle est, toutefois, un peu plus complet en temps de guerre qu'en temps de paix. En effet, en temps de guerre, il est possible de parvenir à encadrer l'utilisation des cyberattaques, même en l'absence de convention spéciale, grâce au droit des conflits armés, le droit international humanitaire.

72. Tel était d'ailleurs le constat de Laura Baudin [94], « *les textes encadrant le droit international humanitaire permettent pour l'instant de réglementer les cyberattaques lorsque celles-ci sont utilisées par les forces dans le cadre d'un conflit armé. Le problème est qu'il n'existe aucune disposition encadrant spécifiquement l'emploi de ces armes cybernétiques. On ne peut qu'interpréter les textes en vigueur face à cette situation.* » Si cette absence de textes spéciaux demeure un problème, le D.I.H. permet toutefois d'y parer et d'encadrer les cyberattaques mais uniquement quand celles-ci ont

[92] En ce sens *v*. VENTRE Daniel, « *Cyberespace et acteurs du cyberconflit* », éditions Lavoisier, 2011, p. 72
[93] En ce sens *v*. BAUDIN Laura, « *Les cyberattaques dans les conflits armées* », éditions L'Harmattan, 2014, p. 27
[94] *Ibid*. p. 9-10 (préface)

lieux lors de conflits armés[95]. Cet encadrement reste limité et doit obéir à plusieurs conditions. Il comporte en outre deux problèmes de taille.

73. Tout d'abord, cet encadrement est le fruit d'une interprétation extensive des règles du D.I.H. afin qu'elles soient reconnues aux cyberattaques. En effet, le D.I.H. encadre la tenue des hostilités depuis la fin de la Seconde Guerre mondiale. Il a été développé dans le but de ne pas laisser se reproduire les horreurs et les crimes de cette dernière. Il s'attache par conséquent à « *soulager en période de conflit le sort des militaires blessés, des prisonniers, des populations civiles et des biens* » au moyen des quatre Conventions de Genève de 1949 et des trois Protocoles Additionnels. A cette fin, le D.I.H. règlemente notamment les moyens et méthodes de guerre afin que les parties respectent toujours plusieurs principes, à savoir le principe de précaution (éviter des dommages collatéraux disproportionnés), le principe de distinction (entre militaires et civils), et le principe d'éviter les maux superflus.

74. Or, lorsque le D.I.H. a été créé, il répondait à un besoin de règlementation, correspondant aux moyens de l'époque, dont les cyberattaques ne faisaient pas partie.[96] Fort heureusement, le D.I.H. a été rédigé dans un esprit évolutif de telle sorte qu'il permet d'appliquer ses critères aux nouvelles armes et aux nouveaux moyens de guerre. En effet, cela est rendu possible grâce au Protocole Additionnel I (P.A.I.) aux Conventions de Genève qui précise que « *dans l'étude, la mise au point, l'acquisition ou l'adoption d'une nouvelle arme, de nouveaux moyens ou d'une nouvelle méthode de guerre, […] obligation de déterminer si l'emploi en serait interdit, dans certaines circonstances ou dans toutes circonstances, par les dispositions du présent protocole ou pour toute règle du droit international applicable à cette Haute Partie contractante* ».[97]

75. Si l'article 26 du P.A.I. permet d'appliquer le D.I.H. aux nouvelles armes, il n'en demeure pas moins que cet encadrement est soumis à une condition *sine qua non* : si le D.I.H. s'applique à toutes les armes utilisées lors d'un conflit armé y compris les

[95] En ce sens *v*. BORIES Clémentine, « *Appréhender la cyberguerre en droit international, Quelques réflexions et mises au point* », La Revue des Droits de l'Homme, éditions Revue du centre de recherche et d'études sur les droits fondamentaux, 6.2014, § 15
[96] BAUDIN Laura, « *Les cyberattaques dans les conflits armées* », éditions L'Harmattan, 2014, p. 142
[97] *Ibid*. p. 143

nouvelles armes, encore faut-il que les cyberattaques soient reconnues comme telles, c'est-à-dire comme des armes nouvelles (ou des nouveaux moyens de guerre) afin de pouvoir leur appliquer les principes et les règles du D.I.H. Le droit international doit donc *a minima* reconnaître, comme le considère déjà le C.I.C.R.,[98] que les cyberattaques peuvent être des armes utilisées par au moins une des parties au conflit, et qu'elles sont donc soumises au D.I.H. quand elles sont utilisées lors de conflits armés.

76. Ensuite, se pose un second problème majeur à l'encadrement des cyberattaques par le D.I.H. Même si les cyberattaques sont reconnues comme étant des armes, et que le D.I.H. est ainsi à même de règlementer leur utilisation, le D.I.H. demeure le droit des conflits armés. C'est du *jus in bello* qui ne peut donc s'appliquer qu'en temps de guerre.[99] S'il permet donc de réglementer l'utilisation des cyberattaques en temps de guerre, il ne peut aller jusqu'à encadrer l'utilisation des cyberattaques en temps de paix.

77. En effet, le D.I.H., étant utilisé exclusivement lors des conflits armés, ne peut s'appliquer que lorsque le conflit armé a commencé, et ne prend donc pas en compte les cyberattaques lancées contre un État en temps de paix. Or, ceci constitue une limite majeure à l'utilisation du D.I.H. pour encadrer les cyberattaques car, si les États utilisent parfois les cyberattaques en parallèle de leurs opérations militaires classiques, ils ont également recours aux cyberattaques en amont de la déclaration des hostilités, pour préparer le terrain avant que la guerre ne soit officiellement déclarée. Les États peuvent également décider de totalement remplacer leurs attaques cinétiques par des cyberattaques.[100] Et c'est justement dans ce cas de figure qu'ils peuvent réaliser une agression contre d'autres États de manière dématérialisée. Or c'est exactement ce qui n'est pas pris en compte par le droit international existant, et qui ne peut pas être pris en compte non plus par le D.I.H. Par conséquent, outre le fait de devoir reconnaître que les cyberattaques peuvent bien être utilisées comme des armes (ce qui permettra leur encadrement par le D.I.H. lors des conflits armés), le droit international devra se décider

[98] En ce sens *v.* LAGOT Daniel, « *Le droit international et les guerres de notre temps* », éditions L'Harmattan, 2016, p. 87
[99] BORIES Clémentine, « *Appréhender la cyberguerre en droit international, Quelques réflexions et mises au point* », La Revue des Droits de l'Homme, éditions Revue du centre de recherche et d'études sur les droits fondamentaux, 6.2014, § 13
[100] VENTRE Daniel, « *Cyberattaque et cyberdéfense* », éditions Lavoisier, 2011, p. 57, in. BAUDIN Laura, « *Les cyberattaques dans les conflits armées* », éditions L'Harmattan, 2014, p. 33

à règlementer les cyberattaques[101] en temps de paix afin d'éviter leurs recours abusifs par les États, sans quoi il laisserait une faille dans le système onusien alors même que ce dernier a pour objectif de prohiber les agressions entre États.

78. Cela est d'ailleurs le constat actuel du droit international. Une absence totale de règles en la matière semble ouvrir la porte à tous les abus. Avant de voir les raisons d'opérer un tel encadrement des cyberattaques, il convient de s'interroger sur la raison d'être d'un tel vide juridique du droit international en la matière. Ce vide juridique est l'expression d'un désaccord au sein de la communauté internationale. En effet, les États ne parviennent pas à s'accorder sur une définition commune des cyberattaques, qui serait à la base de tout régime juridique. Il n'existe pas, de ce fait, « *d'acceptation juridique assurée du terme de cyberguerre et de cyberattaque* »,[102] ce qui entretient une « *totale imprécision de la définition du terme de cyberattaque* »[103].

79. Ainsi, en l'absence de textes spécifiques sur les cyberattaques étatiques, en particulier celles utilisées comme des armes en temps de paix et des conséquences qui en découleraient, le droit international peine à les appréhender alors même que, comme nous le verrons, elles sont à même de violer certains de ses principes fondamentaux. Cela se matérialise par la manière dont sont actuellement considérées les cyberattaques. Quand celles-ci se produisent, et surtout quand elles ont lieu en dehors des conflits armés, elles sont plutôt considérées comme des ingérences et non comme des agressions, ce qui encourage les États à recourir aux cyberattaques et ce jusqu'à créer une distorsion entre la manière dont le droit international appréhende les cyberattaques, et celles dont les États les pratiquent.

[101] BAUDIN Laura, « *Les cyberattaques dans les conflits armées* », éditions L'Harmattan, 2014, p. 9-10 (préface)
[102] BORIES Clémentine, « *Appréhender la cyberguerre en droit international, Quelques réflexions et mises au point* », La Revue des Droits de l'Homme, éditions Revue du centre de recherche et d'études sur les droits fondamentaux, 6.2014, § 4
[103] *Ibid*.

Paragraphe 2 : La situation actuelle des cyberattaques : le vide juridique en contradiction avec la pratique des États.

Au sein de ce paragraphe, il sera mis en lumière le décalage qu'il existe entre l'absence de développement de règles juridiques spécifiques aux cyberattaques étatiques, et l'évolution des pratiques étatiques. A cette fin, nous aborderons donc l'épisode estonien de 2007, véritable tournant dans l'instrumentalisation des cyberattaques.

80. Le droit international ne s'est donc pas encore adapté aux cyberattaques et ne peut les prendre en compte qu'à travers une lecture extensive du D.I.H. Il existe *de facto* un écart certain entre d'une part, le vide juridique en matière de cyberattaques se matérialisant par l'absence de convention en la matière, et d'autre part leurs utilisations par les États.

81. En effet, les cyberattaques sont un fait dont il faut tenir compte dès aujourd'hui. Les Nations unies elles-mêmes reconnaissent de plus en plus leur impact notamment à travers les déclarations de l'Union Internationale des Télécommunications (U.I.T.)[104]. Certes, la C.I.J. ne s'est pas encore prononcé en la matière, mais ce silence tient plus au fait de sa compétence que de sa volonté. Outre le consentement des États, la C.I.J. n'est compétente que pour des litiges concernant des violations du droit international, ou des points du droit international (en cas d'avis consultatifs). Or, les cyberattaques n'étant pas règlementées en droit international, les États ne peuvent donc pas encore saisir la C.I.J. lorsqu'ils en sont victimes. La C.I.J. n'étant pas saisie, elle ne peut pas se prononcer. C'est pourquoi il serait vain d'attendre une solution de la C.I.J. en matière de règlementation des cyberattaques.

82. Mais cette absence de réactions de la part de la C.I.J. n'a pas empêché les Nations unies de reconnaître le danger des cyberattaques. Si le Conseil de sécurité n'a pas encore pris les devants, ni même l'A.G.N.U. d'ailleurs, les Nations unies portent toute de même une attention particulière aux cyberattaques, ce qui démontre leur importance grandissante. L'O.N.U. a effectivement reconnu le danger des cyberattaques. En effet, en 2010 déjà, lors du Forum Economique Mondial, dit le Forum de Davos, Hamadoun

[104] Déclaration du Secrétaire Général de l'U.I.T. Houlin Zhao au Conseil de l'U.I.T. de Genève « *State Of the Union Adress* », 15.05.17

Touré, secrétaire général de l'U.I.T., une des institutions spécialisées de l'O.N.U., proposait la création d'un traité de « *cyberpaix* »[105] afin d'éviter une escalade incontrôlée des tensions entre États et ainsi une rupture de la paix qui prendrait la forme d'une cyberguerre, pour commencer… [106]

83. La préoccupation des Nations unies à travers l'U.I.T. démontre bien que la cyberguerre est devenue une réalité pour l'O.N.U. Lors du Forum mondial de Davos, Hamadoun Touré avait affirmé que désormais les cyberattaques ayant pour objectif d'utiliser Internet pour mener des attaques dans le cyberespace était une réalité et que le monde devait s'y préparer, « *la cyberguerre étant bien déclarée* »[107].

84. De plus, en 2013, les Nations unies ont estimé qu'il était nécessaire *« d'assouplir le discours sur la cyberguerre* »[108] considérant que, même en l'absence de règle en matière de cyberattaque, les États avaient tendance à estimer « *que les cyberattaques constituent un acte de cyberguerre* »[109]. Les Nations unies encouragent donc à « *démilitariser* » le terme de cyberattaque et surtout à « *continuer de plaider en faveur de traités relatifs au cyberespace* »[110] car il faut « *établir des règles d'engagement dans le cyberespace* ».[111]

85. Bien que l'O.N.U. se préoccupe de la question et appelle les États à reconnaître l'importance et le danger des cyberattaques ainsi que la nécessité de leur encadrement par un traité, le droit international demeure muet sur le régime applicable aux cyberattaques. Or, en l'absence de fondement juridique, les États peinent à qualifier les cyberattaques d'agression. La question s'est d'ailleurs posée pour l'Estonie en 2007. Confrontée à *« une véritable attaque armée dans le cyberespace selon les mots du général Keith B. Alexander, responsable du U.S. Cyber Command, l'Estonie, estimant faire face à une véritable agression avait un temps envisagé d'invoquer l'article V du Traité de l'Atlantique Nord* ».[112]

---

[105] TOURE Hamadoun in Le Monde Technologies, « *La seule façon de gagner la cyberguerre, c'est de l'éviter* », 03.02.2010
[106] Le Monde Technologies, « *La seule façon de gagner la cyberguerre, c'est de l'évit*er », 03.02.2010
[107] Déclaration d'Hamadoun Touré, secrétaire général de l'Union Internationale des Télécommunications, au Forum Mondial de Davos, 2010
[108] Nations Unies, « *Les cyberconflits et la sécurité nationale* », éditions Chronique O.N.U., Vol. L No. 2 09/2013
[109] *Ibid*.
[110] *Ibid*.
[111] *Ibid*.
[112] SIMONET Loïc, « *L'usage de la force dans le cyberespace et le droit international* », Annuaire de droit français international, 2012, 58, pp. 117-143, p. 120

86. Si l'Estonie avait considéré être victime d'une cyberattaque, cela tranche avec le sentiment habituel des États. En effet, jusqu'à la cyberattaque dont a été victime l'Estonie en 2007, les États avaient plutôt tendance à qualifier les cyberattaques d'ingérence dans les affaires intérieures, ou de violations du principe de non-intervention. Cela s'explique en partie par le degré d'intensité des attaques qui a évolué.

87. Les cyberattaques étaient surtout utilisées de manière discrète jusqu'en 2007. C'était des « *actions d'espionnage classiques, de type écoutes et interceptions électroniques (vols de renseignement sensibles) ou guerre de l'information (prise de contrôle d'un site Internet pour en modifier les informations)* ».[113] L'une des premières opérations connues en matière de guerre informatique serait attribuée à la CIA au début des années 1980 avec l'implantation d'un virus dans un système de contrôle « *dérobé* » par les Russes.[114] Pendant longtemps, les cyberattaques sont ainsi restées des attaques de faible intensité, contre des cibles très précises.

88. Les États continuent à avoir recours à des cyberattaques pour de telles actions afin d'acquérir des informations sensibles notamment par les Russes et les Chinois qui tentent d'atteindre ces objectifs d'espionnage au moyen de chevaux de Troie[115]. Des opérations de désinformation sont également menées, ainsi que des tentatives de détourner le contenu des sites Internet[116] dans le but de relayer de fausses informations, ou de permettre l'infiltration du réseau de l'utilisateur consultant le site.

89. Il est également possible de prendre un exemple concret, toujours dans le même genre de cyberattaques. Treize ressortissants russes, et trois entités russes ont été inculpés par la justice américaine en février 2018 pour ingérence et complot en vue de tromper les États-Unis.[117] Cette arrestation s'inscrit dans un contexte de suspicion initié par les services de renseignements américains qui ont dénoncé une « *ingérence russe sur les réseaux sociaux et le piratage d'informations* », bien que « *la Russie ait démenti toute*

---

[113] MONGIN Dominique, « *Les cyberattaques, armes de guerres en temps de paix* », éditions Esprit, 01/2013, p. 32-49, § 11
[114] *Ibid*. § 4
[115] *Ibid*. § 11
[116] *Ibid*. § 12
[117] Le Monde, « *États-Unis : la justice poursuite treize Russes pour ingérence dans l'élection présidentielle de 2016* », 16.02.2018 http://www.lemonde.fr/ameriques/article/2018/02/16/États-unis-la-justice-poursuit-treize-Russes-pour-ingerence-dans-l-election-presidentielle-de-2016_5258249_3222.html

ingérence ».[118] . En effet, en juillet 2016, lors de la campagne électorale, « *19 952 e-mails et 8 034 pièces jointes issus des serveurs du Comité national du parti démocrate (DNC) sont piratés par des hackers et publiés sur le site Wikileaks.* »[119]. La CIA accusera par la suite la Russie d'être à l'origine de cette cyberattaque. Cette affaire démontre bien que les États font encore face, ou se considèrent encore face à des cyberattaques qualifiées de « *classiques* », consistant à mener des actions d'espionnage classiques ou de guerre de l'information, et leur pratique de toujours qualifier ce genre d'attaque « *d'ingérence* » comme cela est le cas pour la pseudo-cyberattaque subie par les États-Unis qu'ils ont eux-mêmes qualifiée « *d'ingérence* » ou « *d'intervention* » de Moscou[120].

90. Mais, si cette utilisation classique des cyberattaques, généralement qualifiée d'ingérence, est encore au goût du jour des États, ce n'est désormais plus la seule. En effet, de nouvelles utilisations des cyberattaques sont apparues récemment, au sein d'opérations étatiques moins discrètes. Ces cyberattaques étatiques très intenses, comme en Estonie ou en Géorgie, ont remis en cause la qualification habituelle d'ingérence des cyberattaques et ont posé la question de leur assimilation à un acte d'agression.

91. Un tournant a effectivement eu lieu avec l'Estonie, qui a été réitéré ensuite en Géorgie puis en Ukraine, ce qui a démontré que les cyberattaques appartiennent « *désormais au répertoire d'action des États* »[121]. Des cyberattaques de grande intensité ont eu lieux, poursuivant également un objectif différent. Ces cyberattaques ont été réalisées sur l'ensemble d'un pays, dans le but non d'atteindre un objectif ciblé (comme prendre le contrôle d'un système, ou de recueillir des informations en particulier), mais dans le but de paralyser l'ensemble du pays. A cette différence d'objectif s'est également ajouté le fait que ces cyberattaques ont précédé, à deux reprises, l'intervention officielle ou officieuse des forces étatiques soupçonnées de la cyberattaque.

---

[118] Le Monde, *« États-Unis : Poutine promet une riposte après l'attaque contre la chaîne de télévision RT »*, 11.11.2017 www.lemonde.fr/international/article/2017/11/11/États-unis-poutine-promet-une-riposte-apres-l-attaque-contre-la-chaine-de-television-rt_5213568_3210.html

[119] LIMONIER Kévin et GERARD Colin, « *La guerre hybride russe dans le cyberespace* », éditions Hérodote, 2017, n°166-167, pp 145-163, § 1

[120] Le Monde Diplomatique, « *Ingérences russe, de l'obsession à la paranoïa* », 12.2017, p. 12-13 https://www.monde-diplomatique.fr/2017/12/MATE/58207

[121] En ce sens *v.* TAILLAT Stéphane, « *un mode de guerre hybride dissymétrique ? Le cyberespace* », éditions Institut de Stratégie Comparée, 2016/1 (n°111), p. 89-106, § 27

92. Les cyberattaques ont ainsi franchi un cap : elles ont prouvé leur efficacité et leur dangerosité, ce qui explique que se pose désormais la question de leur assimilation à une agression en droit international, et non plus à une simple ingérence dans les affaires intérieures de l'État. Certes, *« l'Internet fait surgir des interrogations nouvelles pour le droit, il appelle des règles particulières. Aussi les cyberattaques dans leur diversité se caractérisent-elles par un besoin de normativité spécifique, propre* »[122] et nécessite la création d'un régime juridique spécifique pour les cyberattaques. Toutefois, en attendant, il n'en demeure pas moins qu'il est nécessaire de permettre leur qualification en agression en étendant la notion actuelle de l'agression afin de les y inclure.

Chapitre 2 : La nécessité d'étendre la notion d'agression aux cyberattaques.

Dans ce chapitre, nous verrons que l'extension de la notion d'agression afin d'y inclure les cyberattaques apparaît essentielle étant donné l'évolution des cyberattaques, et leurs similarités de plus en plus flagrantes avec les recours à la force classique.

Section 1 : Une extension justifiée au vu de l'intensité croissante des cyberattaques et de leurs nouvelles instrumentalisations.

Au sein de cette section, nous aborderons l'évolution des cyberattaques, utilisées depuis l'Estonie de plus en plus agressivement et de manière de plus en plus récurrente par les États.

Paragraphe 1 : L'Estonie, la Géorgie et l'Iran, des tournants majeurs dans l'instrumentalisation des cyberattaques.

Dans ce paragraphe, il sera question des nouvelles instrumentalisations des cyberattaques par les États qui marquent un tournant majeur initié depuis l'épisode Estonien, nouvelles instrumentalisations qui, d'ailleurs, ne cessent de

[122] BORIES Clémentine, « *Appréhender la cyberguerre en droit international, Quelques réflexions et mises au point* », La Revue des Droits de l'Homme, éditions Revue du centre de recherche et d'études sur les droits fondamentaux, 6.2014, § 13

gagner en intensité, ce constat étant en faveur de l'extension de la notion d'agression afin d'y inclure les cyberattaques.

93. Devant le vide juridique dont font l'objet les cyberattaques, il est donc urgent d'étendre la notion d'agression afin de les encadrer. Si ce régime doit intégrer la possibilité de qualifier les cyberattaques non plus seulement d'ingérence, mais aussi d'agression quand elles dépassent une certaine intensité, cela est dû aux récentes évolutions qu'ont connu les cyberattaques dans leurs utilisations par les États. Ces évolutions justifient une extension de la notion d'agression au sein d'un nouveau régime spécifique aux cyberattaques, permettant de qualifier d'agression les cyberattaques dépassant une certaine intensité, en plus des recours à la force physique dépassant une certaine intensité.

94. Certes, le constat que les États ont de plus en plus recours aux cyberattaques s'impose. Mais celles-ci ont également connu un tournant dans leur instrumentalisation par les États. C'est d'ailleurs ce tournant dans l'utilisation des cyberattaques qui renforce le besoin de les règlementer. L'utilisation par la Russie des cyberattaques a notamment marqué un tournant dans l'approche des cyberattaques par la communauté internationale.

95. En effet, si aucune preuve n'a été officiellement apportée quant à son rôle dans les cyberattaques subies par l'Estonie et par la Géorgie, de fortes présomptions pèsent sur elle. L'instrumentalisation des cyberattaques, initiée par la Russie, a démontré que leur utilisation a commencé à évoluer. Si jusqu'alors les cyberattaques relevaient des opérations de « *cyberespionnage* »[123], dans une logique de discrétion inhérente à l'espionnage[124] et à la guerre secrète, elles peuvent désormais être utilisées au grand jour, à l'appui d'une diplomatie de Realpolitik ou d'une opération militaire.

96. Tout d'abord, le cas de l'Estonie a révolutionné la perception des cyberattaques. En 2007, l'Estonie, « *pays pionner de l'UE en matière d'utilisation de l'Internet* [125]» et

[123] D'ELIA Danilo, « *La guerre économique à l'ère du cyber*espace », Revue Hérodote, éditions La Découverte, 2014/I (N°152-153), p. 240-260, § 10
[124] *Ibid*.
[125] Le Monde Europe, « *L'Estonie tire les leçons des cyberattaques massives lancées contre elle pendant la crise avec la Russie* », 27.06.2007

dont la plupart des transactions bancaires se font en ligne, décide de déplacer la Statue du Soldat de Bronze de Tallin, un monument à la gloire de l'Armée rouge, symbole de fierté pour la Russie. La minorité russophone proteste alors fortement contre ce projet. Cela attise également de vives tensions avec la Russie.[126] Dès l'annonce du transfert de la Statue du Soldat de Bronze, des responsables Russes « *ont appelé au renversement du gouvernement estonien "fasciste". A Moscou, les Nachi (nom d'une organisation de jeunesse pro-Poutine, signifiant « Les nôtres » en russe) ont agressé l'ambassadeur de la petite république balte au beau milieu d'une conférence de presse, et attaqué à coups de pierres l'ambassadeur de Suède, venu un peu plus tard lui apporter son soutien.* »[127] et *« le 10 mai 2007 le consulat estonien à Pskov (nord de la Russie) a été la cible de tirs.* »[128]

97. C'est dans ce contexte qu'en avril 2007 l'Estonie subit une cyberattaque contre ses sites gouvernementaux et privés. Cette cyberattaque a été lancée « *à partir de soixante pays différents, depuis des millions d'ordinateurs, mais à l'insu de leurs propriétaires. Pour parvenir à leurs fins, les pirates ont réussi à constituer des réseaux clandestins et éphémères de plus d'un million d'utilisateurs, prompts à noyer les sites au moyen de multiples demandes d'accès.* »[129]

98. Cette cyberattaque a eu des effets désastreux. En effet, la « *Hansapank, première banque du pays, était contrainte de fermer, pour plusieurs heures, son service en ligne. Les 15 et 16 mai 2007, c'était le tour de SEB Eesti Uhispank, deuxième établissement d'Estonie. Une véritable nuisance, lorsqu'on sait que 99 % des transactions bancaires de la petite république balte se font via Internet.* »[130]

99. Si jusque-là les cyberattaques étaient surtout utilisées discrètement, la cyberattaque subie par l'Estonie en 2007 a démontré que les cyberattaques peuvent être utilisées pour des « *actions de perturbations* »[131] de grande ampleur. Cette cyberattaque a ainsi complètement perturbé des sites gouvernementaux et des sites privés considérés vitaux

[126] Le Monde Europe, « *L'Estonie tire les leçons des cyberattaques massives lancées contre elle pendant la crise avec la Russie* », 27.06.2007
[127] *Ibid.*
[128] *Ibid.*
[129] *Ibid.*
[130] *Ibid.*
[131] MONGIN Dominique, « *Les cyberattaques, armes de guerres en temps de paix* », éditions Esprit, 01/2013, p. 32-49, § 7

pour le fonctionnement du pays[132] en les saturant de connexion. Or ces actions offensives qui avaient pour objectif de perturber le fonctionnement d'un État ont eu lieu dans un contexte de « *tension diplomatique entre ce pays balte et la Russie […] et donc l'origine russe de cette action -non signée mais d'une portée diplomatique évidente- ne semble guère faire de doute* »[133]. Par conséquent, bien que non signée, la Russie a tout de même clairement fait passer son message à l'Estonie.

100. Cette cyberattaque dont a été victime l'Estonie a ainsi démontré deux éléments importants dans le changement de perception des cyberattaques : celles-ci sont à même de paralyser entièrement un pays et ses infrastructures[134] aussi efficacement (voire mieux) que l'utilisation de la force armée, et elles peuvent être prises dans le cadre d'une Realpolitik appuyée, ce qui a fait réagir les États car, comme M. Raiend le faisait remarquer, « *de nouvelles offensives informatiques sont à craindre, et pas seulement vers l'Estonie car si les attaques marchent ici sur nos systèmes, qui sont très performants, alors elles marcheront ailleurs »*[135].

101. Une autre manière d'utiliser les cyberattaques a été dévoilée lors des actions des États-Unis contre l'Iran avec le virus Stuxnet, et de la Russie contre la Géorgie. Cette fois, c'est la capacité des cyberattaques à réaliser des « *actions de destructions* »[136] qui a été démontrée. Contrairement aux actions de perturbations, la finalité de ces attaques est la destruction d'un objectif.

102. La cyberattaque Stuxnet lancée par les États-Unis contre le programme nucléaire de la République islamique est un vers informatique introduit dans le complexe iranien de Natanz en 2010 « *au moyen d'un périphérique USB* »[137]. Cette cyberattaque avait pour objectif de prendre le contrôle du système informatique du complexe nucléaire iranien et plus particulièrement du programme contrôlant les centrifugeuses afin de causer des dommages physiques aux infrastructures iraniennes en perturbant le

[132] BAUDIN Laura, « *Les cyberattaques dans les conflits armées* », éditions L'Harmattan, 2014, p. 51
[133] MONGIN Dominique, « *Les cyberattaques, armes de guerres en temps de paix* », éditions Esprit, 01/2013, p. 32-49, § 7
[134] HUYGHE François Bernard, « *Stratégie dans le cyberespace* », éditions Médium, 2012, N°31, pp 129-146, § 4
[135] Le Monde Europe, « *L'Estonie tire les leçons des cyberattaques massives lancées contre elle pendant la crise avec la Russie* », 27.06.2007
[136] MONGIN Dominique, « *Les cyberattaques, armes de guerres en temps de paix* », éditions Esprit, 01/2013, p. 32-49, § 8
[137] Le Monde, « *Les risques de cyberattaques contre les centrales nucléaires se multiplient* », 06.10.2015.

fonctionnement des centrifugeuses et en les détruisant[138]. Cette cyberattaque a d'ailleurs entrainé la « *destruction de 1000 d'entre-elles* »[139] ce qui a démontré que désormais les cyberattaques sont à même de permettre la « *destruction physique des infrastructures* »[140]. Cette cyberattaque des États-Unis dévoile ainsi une nouvelle instrumentalisation des cyberattaques dont la logique n'est plus l'ingérence dans les affaires du pays au moyen d'espionnage ou de désinformation, mais bien d'attaque du pays en causant des destructions physiques d'infrastructures, comme les États-Unis l'avaient expérimenté dans les années 80 pendant la guerre froide (officieusement).[141]

103. Ce sont donc des cas de cyberattaques très intenses, pouvant mener à la destruction des biens d'un État (qui pourraient avoir pour conséquence la mort de personnels civils ou militaires) alors même que les États ne sont pas en situation de guerre. En effet les cyberattaques sont de plus en plus utilisées pour de telles actions, et « *fréquemment en dehors de tout conflit armé* »[142] ce qui fait qu'un « *tel acte de cyberattaque ne correspond ni à la guerre, ni à la paix mais « somewhere between* » ».[143] De tels actes sont de plus utilisés par les États-Unis, la Chine, Taïwan, la Russie[144] ce qui fait des cyberattaques un potentiel « *outil de destruction comme cela a été le cas avec le vers informatique Stuxnet en 2010* »[145].

104. Une autre facette des cyberattaques a été également récemment révélée lors de la guerre d'Ossétie du Sud. En 2008, cette région géorgienne réclame son indépendance et des miliciens en prennent le contrôle. La Géorgie déclenche alors une offensive début août pour reprendre la région.[146] La Russie riposte alors en déployant ses troupes dans cette région séparatiste, au nom d'une opération de maintien de la paix.[147] Les Russes se servent alors de cyberattaques pour paralyser le système « *d'information, de*

---

[138] En ce sens *v*. MONGIN Dominique, « *Les cyberattaques, armes de guerres en temps de paix* », éditions Esprit, 01/2013, p. 32-49, § 8-9
[139] Le Monde, « *Les risques de cyberattaques contre les centrales nucléaires se multiplient* », 06.10.2015.
[140] En ce sens MONGIN Dominique, « *Les cyberattaques, armes de guerres en temps de paix* », éditions Esprit, 01/2013, p. 32-49, § 9
[141] *Ibid*. § 4
[142] BORIES Clémentine, « *Appréhender la cyberguerre en droit international, Quelques réflexions et mises au point* », La Revue des Droits de l'Homme, éditions Revue du centre de recherche et d'études sur les droits fondamentaux, 6.2014, § 5
[143] *Ibid*.
[144] *Ibid*.
[145] GHERNAOUTI-HELIE Solange, « *Menaces, conflits dans le cyberespace et cyberpouvoir* », Revue Sécurité et Stratégie, éditions Club des directeurs de Sécurité des Entreprises, 2011/3 (7), p. 61-67 § 4
[146] Le Monde Europe, « *La Russie préparait de longue date la guerre en Géorgie* », 13.08.2012
[147] Le Monde Europe, « *Russie et Géorgie en guerre pour l'Ossétie du Sud* », 05.08.2008

renseignement et de commandement »[148] géorgien pendant que des forces militaires russes détruisaient physiquement des infrastructures géorgiennes.[149] Les Russes, en se servant d'une cyberattaque afin de préparer et faciliter leur invasion, ont montré que les cyberattaques peuvent ainsi être utilisées à l'appui ou en prévision d'opérations militaires et que, de ce fait, les cyberattaques peuvent avoir un but de destruction d'objectifs en étant combinées à des opérations militaires classiques lors d'un conflit armé avéré tel que la guerre d'Ossétie du Sud.[150]

105. Cette seconde nouvelle instrumentalisation réalisée par les Russes démontre qu'aujourd'hui les cyberattaques peuvent avoir des objectifs de destruction non seulement en elles-mêmes (affaire Stuxnet) mais également en les combinant avec des opérations militaires.[151] Cela inscrit donc encore plus les cyberattaques dans cette nouvelle vision consistant à les utiliser pour réaliser des dommages matériels chez l'ennemi, directement (Stuxnet en Iran) ou indirectement (la cyberattaque contre la Géorgie).

106. Ces deux évolutions, à la fois dans l'intensité des cyberattaques mais aussi dans leur instrumentalisation, appellent à étendre la notion d'agression afin de la rendre accessible aux cyberattaques. En effet, la nouvelle gravité des attaques milite en faveur de cette extension, celles-ci étant déjà « *élevées au rang d'acte de guerre par les États* »[152]. Au vu de leur utilisation de plus en plus fréquentes par les États, ce besoin d'extension va d'ailleurs se faire de plus en plus pressant. En effet, si les cyberattaques ont gagné en complexité, elles ont aussi vu leur nombre croître[153].

---

[148] MONGIN Dominique, « *Les cyberattaques, armes de guerres en temps de paix* », éditions Esprit, 01/2013, p. 32-49, § 10
[149] LIMONIER Kévin et GERARD Colin, « *La guerre hybride russe dans le cyberespace* », éditions Hérodote, 2017, n°166-167, pp 145-163, § 9
[150] *Ibid*. § 5
[151] En ce sens *v*. DOUZET Frédéric, « *La géopolitique pour comprendre le cyberespace* », éditions Hérodote, 2014, n°152-153, pp. 3-21, § 19
[152] HUYGHE François Bernard, « *Stratégie dans le cyberespace* », éditions Médium, 2012, N°31, pp 129-146, § 5
[153] En ce sens *v*. D'ELIA Danilo, « *La guerre économique à l'ère du cyberespace* », Revue Hérodote, éditions La Découverte, 2014/I (N°152-153), p. 240-260, § 2

Paragraphe 2 : Une adéquation entre une utilisation de plus en plus récurrente des cyberattaques étatiques et la prise de conscience par les États de leur utilité.

Dans ce paragraphe, nous verrons que les États ont recours de plus en plus souvent aux cyberattaques, utilisation de plus en plus récurrente qui va de pair avec la prise de conscience des États de leur incroyable potentiel.

107. Ces nouvelles instrumentalisations des cyberattaques par les États ne sont pas des faits isolés. Ces nouvelles méthodes d'attaques sont de plus en plus utilisées. En effet, leur recours est de plus en plus récurrent par les États qui ont pris conscience du danger, et en même temps, du formidable potentiel des cyberattaques.[154]

108. La Russie, à la suite de ses succès en Estonie et en Géorgie, a réitérée sa stratégie d'attaque cybernétique en Ukraine. En 2013, le gouvernement ukrainien décide de ne pas rejoindre l'accord d'association avec l'UE. Des émeutes éclatent et mènent à la destitution du gouvernement en place. Un nouveau gouvernement est mis en place.

109. En réaction, plusieurs provinces à forte population russophone se soulèvent afin d'organiser des référendums d'autodétermination. La Crimée est la première, et exprime son désir de rattachement à la Russie. Suivent ensuite plusieurs autres provinces, dont celle du Donbass en 2014. C'est en particulier dans cette région que les Russes vont mener une « *guerre hybride* » c'est-à-dire combinant « *des modes d'actions numériques aux modes d'actions réguliers et irréguliers* »[155].

110. Les Russes vont recourir à des actions offensives cybernétiques tel que le virus Snake[156] (aussi appelé *Uroboros*) contre des ministères de la Défense des pays de l'Est, dont l'Ukraine. La même année « *une centrale ukrainienne est mise hors d'État de fonctionner par un trojan baptisé Black Energy, privant de fait des centaines de milliers de personnes d'électricité pendant vingt-quatre heures et provoquant un certain émoi*

[154] En ce sens *v*. DOUZET Frédéric, « *La géopolitique pour comprendre le cyberespace* », éditions Hérodote, 2014, n°152-153, pp. 3-21, § 19
[155] TAILLAT Stéphane, « *un mode de guerre hybride dissymétrique ? Le cyberespace* », éditions Institut de Stratégie Comparée, 2016/1 (n°111), p. 89-106, § 3
[156] En ce sens *v*. LIMONIER Kévin et GERARD Colin, « *La guerre hybride russe dans le cyberespace* », éditions Hérodote, 2017, n°166-167, pp 145-163, § 10

dans les médias dans la mesure où il s'agissait d'une première. »[157] Effectivement, une fois encore, les Russes ont démontré que les États peuvent développer des cyberattaques de plus en plus dangereuses pour les autre États car, avant cette attaque cybernétique, *« aucune infrastructure électrique n'avait auparavant été empêchée de fonctionner par une attaque informatique* ».[158]

111. Cette cyberattaque n'est pas la seule de la Russie : depuis 2007, près de trente-deux attaques ont été attribuées à la Russie[159] (bien que cela n'a pas pu être officiellement prouvé). Pourtant, ce pays n'est pas le plus efficace en la matière. Il apparaît que la Russie *« a une capacité offensive bien moindre que les États-Unis, la Chine ou Israël qui sont des pays également reconnus pour l'excellence de leurs experts en cybersécurité* ».[160]

112. La Chine fait également partie des États connus pour avoir recours à des cyberattaques. La Chine est en effet considérée comme « *la menace principale* » en matière de cyberattaques ».[161] La Chine est soupçonnée d'utiliser des cyberattaques contre des journaux américains, mais aussi des entreprises privées notamment en matière d'exfiltration d'informations confidentielles pour lesquelles le gouvernement chinois « *est directement accusé d'être le commanditaire et la menace est qualifiée d'une telle ampleur qu'elle pourrait porter atteinte à la compétitivités du système économique du pays entier* »[162]. Ces cyberattaques sont des « *attaques sophistiquées persistantes (A.P.T.)* » dont l'analyse aurait permis de remonter *« à l'unité 61 398 de l'armée chinoise en charge des opérations sur les réseaux informatiques* ».[163]

113. Citons également l'opération *Orchard*, lancée par Israël en 2007[164] qui a neutralisé les « *moyens de détection et de lutte contre les intrusions aériennes de la*

---

[157] LIMONIER Kévin et GERARD Colin, « *La guerre hybride russe dans le cyberespace* », éditions Hérodote, 2017, n°166-167, pp 145-163, § 10
[158] *Ibid.*
[159] *Ibid.*
[160] *Ibid.* § 5
[161] DOUZET Frédéric, « *Chine, États-Unis : la course aux cyberarmes a commencé* », éditions sécurité globale, 2013, n°23, pp 43-51, § 2
[162] D'ELIA Danilo, « *La guerre économique à l'ère du cyberespace* », Revue Hérodote, éditions La Découverte, 2014/I (N°152-153), p. 240-260, § 1
[163] DOUZET Frédéric, « *Chine, États-Unis : la course aux cyberarmes a commencé* », éditions sécurité globale, 2013, n°23, pp 43-51, § 3
[164] En ce sens *v.* TAILLAT Stéphane, « *un mode de guerre hybride dissymétrique ? Le cyberespace* », éditions Institut de Stratégie Comparée, 2016/1 (n°111), p. 89-106, § 30

Syrie » ce qui a permis à l'aviation israélienne de bombarder des sites de production nucléaire.[165]

114. Dans la même lignée, le Brésil a été victime d'une cyberattaque en 2009 qui a paralysé le fonctionnement d'une centrale hydroélectrique et ainsi privé « *durant trois jours une dizaine de villes et soixante millions d'habitants de transports en commun, deux de circulation télécommunication etc.* »[166] ce qui a démontré la possibilité de lancer « *une cyberattaque sophistiquée contre une infrastructure vitale d'un État avec son lot de dégâts et de nuisances, certes temporaires mais équivalent à un bombardement aérien* ».[167] Cela a d'ailleurs en partie confirmé le risque de voir les infrastructures vitales d'un État attaquées cybernétiquement (services d'urgence, contrôle de la circulation et de la communication, hôpitaux, banques, centrales électriques…) afin de plonger un pays dans le chaos[168]. Le C.I.C.R. lui-même a soulevé la « *vulnérabilité de l'infrastructure civile* » et « *l'ampleur des conséquences humanitaires que peuvent avoir ces agressions* »[169].

115. Ce type de cyberattaques fait partie de la catégorie très fournie des cyberattaques qui ont eu lieu mais qui n'ont pu être attribuées à des États compte tenu des difficultés d'identification de l'auteur mais qui, pour autant, au vu des moyens qu'elles requièrent, nécessitent de telles installations informatiques que seuls les États peuvent en être à l'origine, « *sans pour autant formellement pouvoir mettre en accusation des autorités gouvernementales* »[170]. Il apparaît donc une croissance exponentielle des cyberattaques étatiques car « *aux attaques majeures ayant pour cible les secrets d'État (Pentagone 2007, Bercy 2011, Elysée 2012) se sont ajoutées les opérations visant les infrastructures vitales (Areva 2011, Aramco et RasGas 2012) et les attaques contre les systèmes industriels (Stuxnet, 2010)* »[171].

---

[165] En ce sens *v.* BAUDIN Laura, « *Les cyberattaques dans les conflits armées* », éditions L'Harmattan, 2014, p. 54
[166] *Ibid.*
[167] *Ibid.*
[168] En ce sens *v.* HUYGHE François-Bernard, « *Stratégie dans le cyberespace* », éditions Médium, 2012/2 (n°31), pp 129-146, § 6
[169] C.I.C.R., « *Déclaration du C.I.C.R. aux Nations unies sur les armes, 2017* », 10.10.2017
[170] MONGIN Dominique, « *Les cyberattaques, armes de guerres en temps de paix* », éditions Esprit, 01/2013, p. 32-49, § 15
[171] D'ELIA Danilo, « *La guerre économique à l'ère du cyberespace* », Revue Hérodote, éditions La Découverte, 2014/I (N°152-153), p. 240-260, § 2

116. Il est donc important de réguler l'utilisation des cyberattaques car celles-ci sont utilisées de manière récurrente par les États. Elles sont aussi de plus en plus agressives, entrainant la perturbation ou la destruction d'infrastructures matérielles à grande échelle en temps de guerre (Géorgie, Ukraine), comme en temps de paix (Iran). Comme le président Barack Obama l'a déclaré en 2013 « *Désormais nos ennemis cherchent à obtenir les capacités de saboter notre réseau électrique, nos institutions financières et nos systèmes de contrôle aérien* ».[172] Utilisés comme tels, ces actes peuvent donc constituer des actes de guerres des États qui, en temps de paix, peuvent être une agression. La reconnaissance de ce constat est donc inéluctable et finira par s'imposer devant la prise de conscience des États des risques mais aussi des possibilités des cyberattaques, « *la prise de conscience des questions cyber s'étant accélérée* »[173].

117. Les cyberattaques russes ne sont que la partie émergée de l'iceberg. En effet, les Russes ne sont pas les seuls à avoir recours aux cyberattaques. Toutefois, la nature de leurs attaques et leur répercussion médiatique a précipité l'appropriation de l'espace cybernétique par les États. En effet, alors que le terme de cyberattaque était « *quelque peu tombé en désuétude* »[174], il réapparait dans les années 2000 à la suite des cyberattaques précitées d'Estonie, d'Iran et de Géorgie. Les États prennent alors conscience de la nécessité de considérer le cyberespace comme un territoire « *à conquérir, à contrôler, à surveiller, à se réapproprier. Un territoire sur lequel il faut faire respecter ses frontières, sa souveraineté, ses lois ; et surtout, une menace pour la sécurité nationale et les intérêts de la nation* ».[175]

118. Les États ont dès lors axé leurs efforts sur le développement de leur capacité cybernétique, et plus précisément leur potentiel dans *« le contrôle et la puissance dans le cyberespace* ».[176] La France notamment fait partie des États qui ont pris conscience de ce fait. En ce sens, le livre blanc de la Défense de 2013 est « *explicite, le cyberespace est une priorité stratégique et les armes cybernétiques font désormais partie de*

[172] DOUZET Frédéric, « *Chine, États-Unis : la course aux cyberarmes a commencé* », éditions sécurité globale, 2013, n°23, pp 43-51, § 4
[173] COUSTILLIERE Arnaud, « *La cyberdéfense : un enjeu global et une priorité stratégique pour le ministère de la défense* », Revue Sécurité Globale, éditions ESKA, 2013/I (n°23), p. 27-32, § 2
[174] DOUZET Frédéric, « *La géopolitique pour comprendre le cyberespace* », éditions Hérodote, 2014, n°152-153, pp. 3-21, § 18
[175] *Ibid*.
[176] *Ibid*. § 19

l'arsenal ».[177] La France n'est pas la seule à avoir développer des stratégies militaires intégrant les cyberattaques.

119. D'autres États ont également développé des programmes cybernétiques, tels que la Chine et les États-Unis, « *dont la conscience de l'importance de l'information est historiquement aiguisée, et qui sont à la pointe des avancées technologiques, avaient amorcé très tôt une réflexion stratégique en la matière* »[178].

120. Il est également possible de citer la Grande-Bretagne qui compte sept cents agents au sein du CESG (*Communication and Electronic Security Group*) et qui a placé les cyberattaques *« juste après le terrorisme comme la menace la plus élevée pour le pays en 2010* » dans sa *National Security Strategy* (stratégie de sécurité nationale).[179]

121. L'Allemagne pour sa part a adopté en 2005 un « *plan national pour la protection des infrastructures d'information et a mis au point une stratégie en matière de cybersécurité, dont la coordination est assurée par le ministère fédéral de l'intérieur »,* auquel « *le BSI (undesamt für Sicherheit in der Informationstechnik) est attaché, comptant plus de cinq cents agents* »[180].

122. La prise de conscience des États se matérialisent donc au premier plan dans la création et le développement de stratégies militaires incorporant en leur sein les cyberattaques. Les États ont ainsi pris conscience de la nécessité de protéger leurs infrastructures dites vitales dont « *la perturbation ou le sabotage pourrait mettre en danger les populations civiles* »[181] mais aussi du potentiel des cyberattaques et du fait que la maîtrise de l'information est désormais cruciale lors des conflits.

123. D'une part, cela constitue « *la capacité à collecter, analyser, manipuler l'information peut offrir un avantage à l'ennemi et le faire douter de la fiabilité de sa propre information* »[182] ce qui peut s'avérer stratégiquement très intéressant pour les

[177] DOUZET Frédéric, « *La géopolitique pour comprendre le cyberespace* », éditions Hérodote, 2014, n°152-153, pp. 3-21, § 20
[178] *Ibid*. § *21*
[179] MONGIN Dominique, « *Les cyberattaques, armes de guerres en temps de paix* », éditions Esprit, 01/2013, p. 32-49, § 17
[180] *Ibid*.
[181] DOUZET Frédéric, « *La géopolitique pour comprendre le cyberespace* », éditions Hérodote, 2014, n°152-153, pp. 3-21, § 22
[182] *Ibid*. § *23*

États notamment dans des opérations de désinformation comme cela a été le cas pour les Russes en Ukraine.

124. D'autre part, les cyberattaques peuvent « *plus directement perturber les communications, désorienter l'ennemi et même affecter ses capacités opérationnelles qui dépendent de plus en plus des réseaux pour leur coordination et leur fonctionnement* ».[183]

125. Ces stratégies sont ainsi au centre des développements militaires. Les États ne sont d'ailleurs pas les seuls, les organisations de défense commune et les organisations régionales elles aussi prennent en compte les cyberattaques. En effet, des études de « *Jean-Loup Samaan et Vincent Joubert montrent que l'Union européenne et l'Otan ont intégré ces questions dans leurs priorités stratégiques et pris des initiatives parallèles* ».[184] Ce fait renforce le constat que désormais le développement des cyberattaques et le recours aux cyberattaques s'imposent comme un fait incontournable.

126. Cette prise de conscience des États s'illustre également par la création de centres cybernétiques, notamment militaires, qui témoignent de la volonté des États d'utiliser les cyberattaques à des fins militaires, défensives ou offensives.

127. En effet, les États-Unis avaient déjà créé le *U.S. Cyber-command* en 2010. Le *U.S. Cyber Command*, unité militaire de cyberopérations de la *National Security Agency* (N.S.A.) témoignait de l'intérêt des États-Unis pour l'utilisation des cyberattaques, intérêt grandissant puisque ses effectifs devraient passer de « *400 à 900 dans les années à venir* ».[185]

128. En 2008, la France a pour sa part rendu publique pour la première fois dans son livre blanc sa conception selon laquelle il est nécessaire « *pour un pays comme la France de disposer d'une capacité en matière de lutte informatique [...] car il faudra pour se défendre, savoir attaquer* »[186]. La France a annoncé en 2013 qu'elle entendait développer ses capacités offensives. La même année la Grande-Bretagne a également

[183] DOUZET Frédéric, « *La géopolitique pour comprendre le cyberespace* », éditions Hérodote, 2014, n°152-153, pp. 3-21, § *23*
[184] *Ibid*. § 43
[185] *Ibid*. § 36
[186] MONGIN Dominique, « *Les cyberattaques, armes de guerres en temps de paix* », éditions Esprit, 01/2013, p. 32-49, § 16

fait part de sa volonté d'améliorer ses capacités cybernétiques. Le fait que les pays mettent « *l'accent sur le développement de leur cyberdéfense et de leur cybercapacités* »[187] serait une preuve que désormais « *la course aux cyberarmes a commencé* ».[188] Dès 2009, « *la loi (française) de programmation 2009/14 indiquait que la menace informatique est désormais une préoccupation majeure [...] est qu'une doctrine d'emploi – élaborée sous la responsabilité du chef d'état-major des armées et validée par le chef de l'État* ».[189] La même année la Direction Générale de la Sécurité des Systèmes d'Information (D.G.S.S.I.) est devenu l'Agence Nationale de la Sécurité des Systèmes d'Information (A.N.S.S.I.) et en 2011 la « *stratégie française en matière de cyberdéfense* »[190] a été publiée, affichant l'ambition de la France d'être une « *puissance mondiale de cyberdéfense* ».[191]

129. L'Organisation du Traité de l'Atlantique Nord (l'OTAN) a elle-même décidé de développer une « *capacité pour contrer les cyberattaques, sur demande d'un pays membre* » à la suite de la cyberattaque subie par l'Estonie, ce qui a été confirmé aux sommets de Lisbonne en 2010 et de Chicago en 2012[192]. Ainsi, a été créé un « *Centre d'excellence pour la Cyberdéfense de l'OTAN (NATO CCD COE)* »[193] ayant pour mission « *d'améliorer les capacités, la coopération, le partage d'informations au sein de l'OTAN* »[194]. Cela doit permettre à l'OTAN de se préparer à « *défendre ses réseaux et opérations contre les cybermenaces et les cyberattaques toujours plus complexes auxquelles elle est confrontée* »[195].

130. Dès lors, l'instrumentalisation militaire des cyberattaques initiée par la Russie en Estonie, en Géorgie, en Ukraine et par les États-Unis en Iran n'est plus un cas d'école, mais le commencement et le signe de l'imbrication des cyberattaques dans les attaques de demain.

---

[187] DOUZET Frédéric, « *La géopolitique pour comprendre le cyberespace* », éditions Hérodote, 2014, n°152-153, pp. 3-21, § 38
[188] *Ibid.*
[189] MONGIN Dominique, « *Les cyberattaques, armes de guerres en temps de paix* », éditions Esprit, 01/2013, p. 32-49, § 16
[190] *Ibid.*
[191] *Ibid.*
[192] *Ibid.* § 21
[193] COUSTILLIERE Arnaud, « *La cyberdéfense : un enjeu global et une priorité stratégique pour le ministère de la défense* », Revue Sécurité Globale, éditions ESKA, 2013/I (n°23), p. 27-32, § 23
[194] *Ibid.*
[195] Site officiel de l'OTAN, dossier « *cyberdéfense* », https://www.nato.int/cps/fr/natohq/topics_78170.htm

131. Un tel constat nous donne à penser que dans l'avenir l'utilisation des cyberattaques ira *crescendo*, d'où la nécessité, me semble-t-il impérieuse, d'étendre la notion d'agression aux cyberattaques afin que le droit international les encadre. Les États eux-mêmes prennent conscience de ce besoin au fil de leurs avancées. La Russie et la Chine elles-mêmes « *ont montré la volonté de coopérer dans l'élaboration de règles internationales* », bien qu'à l'heure actuelle « *de fortes divergences de vue persistent* », bloquant un tel projet.[196] Il sera pourtant nécessaire pour les États de parvenir à créer un tel régime juridique au vu de l'évolution des cyberattaques et du cyberespace, ce dernier étant devenu « *un enjeu de rivalités de pouvoir entre acteurs, un théâtre d'affrontement et une arme redoutable dans les conflits géopolitiques qui sont intimement mêlés à des considérations politiques, économiques, sociales et culturelles* »[197], géopolitique dont il faut d'ailleurs tenir compte puisqu'elle permet « *d'aborder ces questions dans toute leur complexité* »[198].

Section 2 : Une extension de la notion d'agression justifiée au vu de la similarité des effets et des conséquences entre une cyberattaque et une attaque conventionnelle.

Dans cette section, nous allons aborder la similarité qui existe entre les attaques cinétiques et les cyberattaques, démontrant que les cyberattaques peuvent être des recours à la force, et, *de facto*, potentiellement des agressions.

Paragraphe 1 : Cyberattaques et attaques conventionnelles, des perceptions, des objectifs et des utilisations étatiques similaires.

Dans ce paragraphe, il sera question de la similarité entre les attaques cinétiques et les cyberattaques quant à leur perception par les États en tant qu'arme, mais aussi quant aux objectifs qu'elles permettent d'atteindre et à la manière dont elles sont utilisées par les États.

[196] DOUZET Frédéric, « *La géopolitique pour comprendre le cyberespace* », éditions Hérodote, 2014, n°152-153, pp. 3-21, § *42*
[197] *Ibid*. § *58*
[198] *Ibid*. § *58*

132. Pour les États, il est impératif de s'entendre sur l'extension de la notion d'agression et de reconnaître que les cyberattaques peuvent constituer des agressions (au même titre que les attaques cinétiques) quand elles dépassent un certain seuil, au vu des similarités entre les cyberattaques et les attaques conventionnelles. En effet celles-ci sont perçues de la même manière par les États, et permettent de poursuivre les mêmes objectifs. Leurs utilisations, leurs effets et leurs conséquences sont également similaires.

133. Tout d'abord, il faut relever la similarité de perception des cyberattaques par les acteurs du droit international. Les cyberattaques sont aujourd'hui considérées comme des armes, au même titre que les moyens d'attaques conventionnels.

134. Les armes sont le corollaire de tout conflit armé ainsi que de toute agression depuis la naissance de la guerre.[199] Les forces armées d'un État sont considérées comme étant à même de mener des opérations militaires et ainsi peuvent réaliser des agressions en ayant recours à la force armée contre un autre État. Les armes tels que les chars, les avions, les navires de guerre, ainsi que l'armement individuel du personnel militaire tels que les fusils, mitrailleuses, mitraillettes, pistolets mitrailleurs, pistolets, canons, missiles sont considérés comme des armes, définis par Jean Salmon comme tout *« engin ou objet destiné à l'attaque ou à la défense, soit par nature (par exemple le poignard, le révolver), soit par l'usage qui en est fait (par exemple le couteau, la canne, les ciseaux* ».[200] Ce sont donc des moyens de combat auquel un État à recours pour attaquer un autre État.

135. Cette définition peut tout à fait s'appliquer aux cyberattaques. Elles peuvent en effet être considérées comme des armes et plus précisément des armes par destination, c'est-à-dire qu'elles deviennent des armes « *par l'usage qu'il en est fait* » puisqu'elles sont des moyens d'attaquer ou de défendre les réseaux et les infrastructures d'un État à partir d'un appareil informatique. En effet, les cyberattaques sont une « *arme qui permet de procéder à la destruction physique d'infrastructures dépendantes des technologies de l'information […] et provoque des dommages collatéraux qui peuvent être massifs et non maîtrisables* »[201] Les cyberattaques sont d'ailleurs considérées comme des armes

[199] En ce sens *v*. BETTATI Mario, « *Droit Humanitaire* », éditions Dalloz, 2012, p. 128
[200] SALMON Jean, « *Dictionnaire de Droit International Public* », éditions Bruylant, 2001, p. 81
[201] MONGIN Dominique, « *Les cyberattaques, armes de guerres en temps de paix* », éditions Esprit, 01/2013, p. 32-49, § 26

par les experts en la matière[202] ainsi que par les États (par exemple les États-Unis comme en témoigne la création de l'*U.S. Cyber-Command*[203] ou encore la France[204]). La Russie et la Chine font d'ailleurs référence, dans les instruments juridiques qu'elles proposent, à « *l'arme informatique* »[205]. Elles sont même parfois perçues comme des « *armes parfaites* »[206] en raison de leurs caractéristiques (*anonymat, rapidité, discrétion*)[207]. Les cyberattaques sont des armes si efficaces que le mouvement international de la Croix-Rouge et du Croissant-Rouge (C.I.C.R.) considère d'ailleurs que « *les cyberopérations peuvent constituer en elles-mêmes de véritables conflits armés* »[208] étant donné que le manuel de Tallinn, considéré par le C.I.C.R. comme une avancée majeure, a défini la cyberattaque comme une « *cyberopération offensive ou défensive raisonnablement susceptible de blesser ou de tuer des personnes, ou d'endommager de détruire des biens* ».[209]

136. Il a souvent été argué que les cyberattaques ne peuvent être des armes devant l'absence d'effet cinétique. Mais cela peut être écarté avec le constat suivant. Tout d'abord, le fait que les cyberattaques n'aient pas d'effet cinétique ne semblent pas influer sur leur perception par les États, qui perçoivent les cyberattaques ainsi qu'« *Internet, les ordinateurs, le code informatique ainsi que les données* »[210] comme de « *nouvelles armes de guerre* »[211]. De plus, le C.I.C.R. les considère également comme telles, et les cite d'ailleurs dans sa déclaration sur les armes aux Nations unies de 2017[212]. Enfin, le droit international lui-même a déjà reconnu que des armes peuvent être dépourvues d'effet cinétique. Dès lors, cela semble ouvrir la voie aux cyberattaques

---

[202] Manuel de Tallin 2.0, 2013
[203] DOUZET Frédéric, « *La géopolitique pour comprendre le cyberespace* », éditions Hérodote, 2014, n°152-153, pp. 3-21, § 36
[204] *Ibid*. § 20
[205] SIMONET Loïc, « *L'usage de la force dans le cyberespace et le droit international* », Annuaire de droit français international, 2012, 58, pp. 117-143, p. 123
[206] BAUDIN Laura, « *Les cyberattaques dans les conflits armées* », éditions L'Harmattan, 2014, p. 46
[207] *Ibid*. Chapitre I, Section I, pp. 34-46
[208] C.I.C.R., « *Quelles limites le droit de la guerre impose-t-il aux cyberattaques ?* », 28.06.2013 https://www.icrc.org/fre/resources/documents/faq/130628-cyber-warfare-q-and-a-eng.htm
[209] *Ibid*.
[210] GHERNAOUTI-HELIE Solange, « *Menaces, conflits dans le cyberespace et cyberpouvoir* », Revue Sécurité et Stratégie, éditions Club des directeurs de Sécurité des Entreprises, 2011/3 (7), p. 61-67 § 5
[211] *Ibid*.
[212] C.I.C.R., « *Déclaration du C.I.C.R. aux Nations unies sur les armes, 2017* », 10.10.2017

en posant le principe selon lequel des attaques peuvent être réalisées par des armes non-cinétiques[213].

137. En effet, des traités ont précisé que les attaques conventionnelles ne sont pas exclusives d'attaques non-cinétiques. Les attaques chimiques ont en effet déjà été reconnues comme des moyens de combat et même prohibées[214] alors mêmes qu'elles ne correspondent pas à des attaques conventionnelles. Cela laisse donc entendre que des cyberattaques menées au moyen d'ordinateurs, même sans effet cinétique, peuvent aussi être considérées comme des armes susceptibles de constituer des recours à la force au même titre que n'importe quelle arme.[215] La C.I.J. a elle-même confirmé cette hypothèse en précisant qu'un recours à la force armée peut être *« tout emploi de la force par n'importe quelle arme* » (même non-cinétique)[216]. Ce constat de la C.I.J. permet donc de conclure qu'une cyberattaque lancée depuis un ou plusieurs appareils informatiques peut être considérée comme une arme et, dès lors, peut également constituer un recours à la force.

138. Il semble donc bien clair que les cyberattaques sont perçues comme des armes, qui peuvent servir à réaliser des actions de perturbation de haute intensité ainsi que des actions de destruction au vu de l'émergence de leur « *caractère potentiellement destructeur* »[217] (autonomes ou complémentaires, à l'appui d'opérations conventionnelles). Or, si les cyberattaques sont des armes, et que leur utilisation constitue bien un recours à la force, alors quand celles-ci dépassent une certaine intensité elles doivent pouvoir être qualifiées d'agressions lorsqu'elles sont utilisées en temps de paix, d'autant que bien que cybernétiques, elles peuvent engendrer les mêmes conséquences dévastatrices que des attaques cinétiques.

139. En effet, les cyberattaques et les attaques cinétiques peuvent entraîner les mêmes conséquences pour les États. Elles ont effectivement de nombreux points communs :

---

[213] En ce sens *v*. AKOTO Evelyne. « *Les cyberattaques étatiques constituent-elles des actes d'agression en vertu du droit international public* » : Première partie. Revue de droit d'Ottawa - Ottawa Law Review, Faculty of Law, Common Law Section, University of Ottawa, 2015, 46 (1), pp.1. p. 4

[214] C.I.J. « *Licéité de la menace ou de l'emploi d'armes nucléaires* », avis consultatif, Recueil 1996 §57

[215] *Ibid*. § 86

[216] *Ibid*. § 86

[217] MONGIN Dominique, « *Les cyberattaques, armes de guerres en temps de paix* », éditions Esprit, 01/2013, p. 32-49, § 5

d'une part, elles peuvent permettre aux États de poursuivre les mêmes objectifs, et d'autre part, les États en font indifféremment la même utilisation.

140. Les cyberattaques peuvent poursuivre le même objectif que des attaques classiques lorsqu'elles sont utilisées en tant qu'armes. Toutes deux peuvent servir à attaquer un État. « *En effet si la subversion et les conflits de basse intensité étaient les méthodes privilégiées des grandes puissances pendant la Guerre froide, l'acquisition progressive de l'arme nucléaire par de plus en plus de pays a fait des cyberattaques étatiques l'outil parfait pour atteindre les mêmes objectifs d'hégémonie* ».[218] La seule différence est que là où les attaques cinétiques, prévues par la résolution 3314 de l'A.G.N.U. se matérialisent par des bombardements, des invasions etc. afin de porter atteinte à la souveraineté d'un État[219], les cyberattaques quant à elles se matérialisent par des prises de contrôle de réseaux, des perturbations ou des interruptions.

141. Cependant, si les deux diffèrent dans leurs matérialisations, ce sont bien deux moyens utilisés par les États pour perturber le fonctionnement d'un autre État, le paralyser, voire l'empêcher d'agir ou détruire ses infrastructures, de manière autonome comme de manière complémentaire.

142. De manière autonome, sans tomber dans la prospective, il est possible de prendre l'exemple de l'affaire Stuxnet. Les États-Unis et Israël ont pu, par le biais de cette cyberattaque, mettre à mal le programme nucléaire iranien en entrainant la destruction de plus de mille centrifugeuses dans le complexe de Natanz[220] aussi efficacement qu'un raid aérien aurait pu les détruire, comme Israël avait déjà fait contre l'Irak et son réacteur *Osirak* en 1981[221].

143. En ce qui concerne les cyberattaques complémentaires, il est avéré que la réussite russe en Géorgie a été la conséquence directe de perturbations dans les communications et les réseaux géorgiens, orchestrés par les services russes. Par conséquent, le fruit de la

[218] AKOTO Evelyne. « *Les cyberattaques étatiques constituent-elles des actes d'agression en vertu du droit international public* » : Première partie. Revue de droit d'Ottawa - Ottawa Law Review, Faculty of Law, Common Law Section, University of Ottawa, 2015, 46 (1), pp.1. p. 1
[219] A.G.N.U résolution A/RES/3314 (XXIX), article 3, a) et b)
[220] En ce sens *v*. MONGIN Dominique, « *Les cyberattaques, armes de guerres en temps de paix* », éditions Esprit, 01/2013, p. 32-49, § 8-9
[221] En ce sens *v*. Le monde, « *Israël revendique la destruction d'un réacteur nucléaire en Syrie en 2007* », 21.03.2018

destruction d'infrastructures a été directement permis grâce, ou à cause, des cyberattaques qui ont été menées en amont et qui ont paralysé le pays, préparant ainsi le terrain pour les moyens conventionnels[222], et ce aussi efficacement que le sabotage d'antennes relais ou de câbles relais par des espions ou des forces conventionnelles.

144. Les attaques cinétiques et les attaques cybernétiques peuvent donc tout à fait être utilisées afin d'atteindre les mêmes objectifs, qui peuvent se résumer à attaquer un État afin de lui causer des dommages. Là où les premières agissent dans l'espace terrestre, maritime ou aérien d'un État, les autres interviennent dans son cyberespace. Cependant, les deux correspondent à un recours à la force contre un autre État, c'est-à-dire au « *comportement d'un sujet du droit international ou de toute autre entité qui emploi la force, […] l'action d'un État qui prend des mesures militaires, blocus, bombardement, occupation de territoire* ».[223] Les cyberattaques sont par conséquent bien des mesures permettant à un État d'employer la force au sens de l'article 3 de la résolution 3314.[224]

145. Cela est d'ailleurs confirmé par le fait qu'elles correspondent à la définition d'un recours à la force donnée par la C.I.J., c'est-à-dire que « *toute intervention illicite dans les affaires d'un autre État et accompagnée d'un moyen de contrainte qui est la force constitue une violation de l'interdiction du recours à la force dans les relations internationales* ».[225]

146. Or, un recours à la force peut être qualifié d'agression dès lors qu'il dépasse une certaine intensité, qu'il revêt une certaine gravité, comme la C.I.J. l'a rappelé dans son affaire des Activités militaires au Nicaragua et contre celui-ci en 1986 en précisant qu'il existe « *les formes les plus graves de recours à la force (celles constituant une agression armée) et d'autres moins brutales* »[226].

---

[222] En ce sens *v.* LIMONIER Kévin et GERARD Colin, « *La guerre hybride russe dans le cyberespace* », éditions Hérodote, 2017, n°166-167, pp 145-163, §s 5 et 9

[223] SALMON Jean, « *Dictionnaire de Droit International Public* », éditions Bruylant, 2001, p. 951

[224] A.G.N.U résolution A/RES/3314 (XXIX)

[225] C.I.J. « *Affaire des Activités militaires et paramilitaires au Nicaragua et contre celui-ci* » du 27 juin 1986 (Nicaragua *c.* États-Unis d'Amérique), fond, arrêt, Recueil 1986, supra note 24 aux para 205, 209. In. AKOTO Evelyne. « *Les cyberattaques étatiques constituent-elles des actes d'agression en vertu du droit international public* » : Deuxième partie partie. Revue de droit d'Ottawa - Ottawa Law Review, Faculty of Law, Common Law Section, University of Ottawa, 2015, 46 (2), pp. 199-221, p. 205

[226] C.I.J. « *Affaire des Activités militaires et paramilitaires au Nicaragua et contre celui-ci* » du 27 juin 1986 (Nicaragua *c.* États-Unis d'Amérique), fond, arrêt, Recueil 1986, § 191, p. 101

147. Dès lors, une cyberattaque peut constituer un recours à la force d'un État contre un autre État selon deux critères. *Primo,* parce qu'elle correspond à l'utilisation d'une arme par un État contre un autre État. *Segundo,* parce que cela correspond à une activité subversive en contradiction avec l'article 2 paragraphe 4 de la C.N.U., tel que la C.I.J. l'interprète[227] c'est-à-dire que « *la subversion, étant en règle générale la déstabilisation d'un gouvernement établi, peut être interprétée comme un acte contre l'intégrité territoriale ou l'indépendance politique de l'État visé comme cela a été le cas en Estonie ou encore en Géorgie »*[228]. Par conséquent, les cyberattaques doivent être soumises au même régime que les armes conventionnelles. Cela induit donc que l'utilisation des cyberattaques par les États doit être considérée comme des recours à la force constituant une agression au même titre que des recours à la force constitués par des attaques classiques, dès lors qu'elles dépassent une certaine intensité.

148. Au surplus, la liste des actes constitutifs d'une agression selon la résolution 3314 n'est pas limitative[229] et les cyberattaques peuvent, au sens de cette résolution, constituer de tels actes dès lors qu'elles sont utilisées comme des armes par un État contre un autre État dans la même optique que des attaques cinétiques. Cela correspond en effet à la définition de la résolution 3314 de l'A.G.N.U. qui a précisé qu'une agression était constituée de *« l'emploi de toutes armes par un État contre le territoire d'un autre État* ».[230]

149. Les cyberattaques étant donc l'emploi d'une arme par un État contre un autre État, elles sont à même de constituer un recours à la force au même titre qu'une attaque cinétique (par exemple un bombardement), prohibée par l'article 2 § 4 de la C.N.U.[231]. Elles constituent donc bien un recours à la force illicite en temps de paix et, par conséquent, une agression.

150. Ce constat est d'autant plus important que les cyberattaques sont utilisées par les États en remplacement d'actions qui pourraient être considérées comme des agressions

[227] En ce sens *v*. AKOTO Evelyne. « *Les cyberattaques étatiques constituent-elles des actes d'agression en vertu du droit international public »* : Deuxième partie partie. Revue de droit d'Ottawa - Ottawa Law Review, Faculty of Law, Common Law Section, University of Ottawa, 2015, 46 (2), pp. 199-221, p. 217
[228] *Ibid*.
[229] A.G.N.U résolution A/RES/3314 (XXIX), article 4
[230] *Ibid*. article 3, b)
[231] En ce sens *v*. Charte des nations Unis, l'article 2 § 4

si elles n'étaient pas cybernétiques. En effet, « *puisqu'ils ne peuvent plus recourir directement à la force sans justifications, les États sont obligés de se tourner vers des méthodes indirectes et subtiles d'affrontement, comme ce fut le cas pendant la guerre froide, et de nos jours avec les cyberattaques* ».[232]

151. Cela explique que, comme vu précédemment, les États ont recours aux cyberattaques pour déstabiliser des pays et perturber leur fonctionnement, comme cela fut le cas au Brésil lors de la cyberattaque contre la centrale hydroélectrique. Ils se servent aussi des cyberattaques pour perturber le développement de projets des autres États (par exemple le projet nucléaire iranien) ou encore pour soutenir leurs actions militaires conventionnelles en lançant des cyberattaques au préalable contre l'autre État.[233]

152. Or, l'ensemble de ces objectifs aurait pu être atteint (et l'a déjà été par le passé) par des moyens conventionnels. Des raids aériens ont permis de perturber le fonctionnement d'un pays. En 1981, Israël a lancé un raid aérien contre l'Irak et a détruit un complexe nucléaire irakien et son réacteur « *Osirak* »[234]. Enfin, les États ont déjà envisagé d'avoir recours à des moyens conventionnels pour détruire des câbles de communication sous-marins et ainsi perturber ou paralyser les communications d'un autre État.[235] Les États n'ont fait que remplacer les moyens pour arriver aux mêmes résultats. Ce sont, en quelque sorte, des palliatifs à l'interdiction de recourir à la force principalement développée pour les attaques classiques ou pour les armes non-cinétiques nucléaires, radiologiques, biologiques et chimiques (N.R.B.C.)[236].

153. Les cyberattaques sont donc un nouveau moyen pour les États de remplir des objectifs qui seraient considérés comme des actes d'agression s'ils étaient réalisés par des moyens conventionnels. En effet, bien que réalisé par cyberattaque, le résultat obtenu par le virus Stuxnet a été le même qu'une attaque conventionnelle : Il a

---

[232] AKOTO Evelyne. « *Les cyberattaques étatiques constituent-elles des actes d'agression en vertu du droit international public* » : Deuxième partie partie. Revue de droit d'Ottawa - Ottawa Law Review, Faculty of Law, Common Law Section, University of Ottawa, 2015, 46 (2), pp. 199-221, p. 203

[233] Partie I, Chapitre 2, Section 1, Paragraphe 1 § 104

[234] En ce sens *v.* Le monde, « *Israël revendique la destruction d'un réacteur nucléaire en Syrie en 2007* », 21.03.2018

[235] En ce sens *v.* Le Monde, « *Les sous-marins Russes près des câbles transatlantiques inquiètent les américains* », 26.10.2015

[236] AKOTO Evelyne. « *Les cyberattaques étatiques constituent-elles des actes d'agression en vertu du droit international public* » : Deuxième partie partie. Revue de droit d'Ottawa - Ottawa Law Review, Faculty of Law, Common Law Section, University of Ottawa, 2015, 46 (2), pp. 199-221, p. 218

seulement été « *plus discret, plus propre que l'attaque sur le réacteur Osirak* »[237]. Les cyberattaques peuvent donc servir à réaliser des agressions, et il est d'ailleurs estimé que « *le brouillage des communications, les attaques informatiques sur les systèmes de contrôle aérien ou de contrôle des pipelines […] pourrait être considérée comme étant des actes de guerre […] la population civile n'étant pas plus épargnée qu'elle ne l'a été à Hiroshima* »[238]. Devant ce constat, il est nécessaire d'ouvrir cette notion d'agression aux cyberattaques, afin que lorsque celles-ci sont utilisées comme des armes, en poursuivant un objectif de paralysie, de perturbation ou de destruction d'une infrastructure d'un autre État, elles puissent être qualifiées d'agression, en particulier lorsqu'elles ont les mêmes effets et les mêmes conséquences, que des attaques conventionnelles (classiques).

Paragraphe 2 : Cyberattaques et attaques conventionnelles, des perceptions, des effets et des conséquences similaires.

Dans ce paragraphe, nous allons voir que les attaques cinétiques et les cyberattaques peuvent avoir les mêmes effets et les mêmes conséquences, ce qui permet d'établir que les cyberattaques peuvent aussi être des recours à la force constituant des agressions.

154. La similarité des cyberattaques et des attaques cinétiques dans leur intensité et dans leurs conséquences est essentielle pour reconnaître qu'une cyberattaque constitue un recours à la force assez grave pour être qualifié d'agression. Partant du constat que tous les recours à la force ne sont pas qualifiés d'agression, mais seulement ceux ayant une certaine intensité, il nous faut donc démontrer que les cyberattaques peuvent atteindre le même degré de gravité que des attaques conventionnelles. Ce degré de gravité peut s'estimer à travers l'intensité et les conséquences des cyberattaques, qui avoisinent ceux des attaques cinétiques.

[237] MULLET-FEUGA Philippe, « *Cyberespace, nouvelles menaces et nouvelles vulnérabilités* », éditions sécurité globale, 2017/I n°9, pp. 83-95 § 42
[238] GHERNAOUTI-HELIE Solange, « *Menaces, conflits dans le cyberespace et cyberpouvoir* », Revue Sécurité et Stratégie, éditions Club des directeurs de Sécurité des Entreprises, 2011/3 (7), p. 61-67 § 7

155. L'intensité entre une cyberattaque et une attaque cinétique constituant un recours à la force qualifié d'agression peut être la même. En effet, une attaque cinétique est à même de paralyser un pays entier aussi sûrement qu'une attaque cinétique. Selon la C.I.J., des accrochages de frontières entre deux États ne sont pas considérés comme pouvant caractériser une agression[239]. En revanche, une attaque sur l'ensemble du territoire est tout à fait à même de la caractériser, et cela est précisément sur cet élément que l'intensité entre une cyberattaque et une attaque cinétique est similaire.

156. Une cyberattaque massive dans l'ensemble d'un pays, dirigée contre tous ses secteurs et ses infrastructures vitaux ou stratégiques est à même de paralyser entièrement le pays ainsi que de lui causer d'importants dommages matériels. Comme l'a déclaré Evelyne Akoto, « *Si les réseaux vitaux d'information cessaient de fonctionner, une société de l'information serait paralysée et sombrerait vite dans le chaos* ».[240] Il est à noter d'ailleurs qu'une telle paralysie d'un État tout entier, dans son ensemble, ne pourrait être atteint que par une attaque conventionnelle de très grande envergure sur l'ensemble de son territoire (Irak) car cela induit que la zone de conflit soit étendue à l'ensemble du territoire de l'État victime. Par conséquent, une attaque conventionnelle aurait du mal à atteindre une telle intensité avec un effet aussi général dans l'État, et seul un recours à la force particulièrement important et intense, pourrait atteindre de tels effets. Cela confirme qu'une cyberattaque peut donc avoir un niveau extrêmement élevé de gravité et être d'une intensité extrême, avoisinant les recours à la force les plus graves. C'est d'ailleurs la conception du Manuel de Tallinn qui, selon Evelyne Akoto, confirme « *qu'une cyberattaque constitue un emploi de la force si ses dimensions et ses effets sont pareils à ceux que l'on aurait obtenus après l'emploi d'armes cinétiques* »[241].

157. Les conséquences d'une telle cyberattaque aussi intense peuvent être particulièrement graves pour les États étant donné l'interconnexion des différents services étatiques et l'omniprésence de l'informatique dans nos sociétés actuelles (y compris dans nos systèmes de défense et le secteur énergétique, particulièrement dans le domaine nucléaire) étant donné que « *les infrastructures informatiques sont devenues*

---

[239] C.I.J. « *Affaire des Activités militaires et paramilitaires au Nicaragua et contre celui-ci* » du 27 juin 1986 (Nicaragua *c.* États-Unis d'Amérique), fond, arrêt, Recueil 1986, §195.
[240] AKOTO Evelyne. « *Les cyberattaques étatiques constituent-elles des actes d'agression en vertu du droit international public* » : Première partie. Revue de droit d'Ottawa - Ottawa Law Review, Faculty of Law, Common Law Section, University of Ottawa, 2015, 46 (1), pp.1. p. 1
[241] *Ibid*. p. 219

les points névralgiques de nos sociétés modernes ».[242] Les réseaux informatiques sont désormais vitaux pour les États. Les réseaux de communication sont d'une extrême importance car ils permettent aux États de coordonner leurs actions, leurs services. Toute absence de communication paralyserait donc un État, en bloquant toute action ou réaction de l'État-victime, comme cela a été le cas en Géorgie[243].

158. De plus, une cyberattaque contre les secteurs vitaux peut également paralyser le pays voire lui causer des dommages matériels. En effet, une perturbation du secteur énergétique peut déstabiliser les États comme cela a été le cas au Brésil (paralysie de son territoire à la suite d'une cyberattaque contre une de ses centrales hydroélectriques).[244] Mais cela peut également causer des dégâts aux infrastructures comme lors de la destruction des centrifugeuses iraniennes par le virus Stuxnet[245]. En développant quelque peu ce point, une cyberattaque contre une centrale nucléaire pourrait ainsi aller jusqu'à perturber le fonctionnement d'une centrale nucléaire, pouvant déclencher son dysfonctionnement voire sa destruction et de fait, une explosion nucléaire. Dès lors, l'explosion d'une centrale nucléaire par un État tiers sur le territoire d'un autre État, initiée par une cyberattaque, n'aurait-elle pas les mêmes conséquences humaines et matérielles, pour ne citer que celles-là, qu'une attaque nucléaire conventionnelle par missile contre cet État ?

159. Il faut donc également voir les risques d'utilisations illicites des cyberattaques et s'empresser de règlementer leurs utilisations en sanctionnant les cyberattaques graves au même titre que les attaques conventionnelles graves, avant que les cyberattaques ne soient poussées à leur paroxysme et qu'elles aient exactement pour conséquences ce que le système des Nations unies a voulu interdire ; d'autant que, par exemple dans le domaine nucléaire, les risques de cyberattaques contre les centrales ne cessent de s'intensifier[246].

---

[242] AKOTO Evelyne. « *Les cyberattaques étatiques constituent-elles des actes d'agression en vertu du droit international public* » : Première partie. Revue de droit d'Ottawa - Ottawa Law Review, Faculty of Law, Common Law Section, University of Ottawa, 2015, 46 (1), pp.1. p. 1

[243] MONGIN Dominique, « *Les cyberattaques, armes de guerres en temps de paix* », éditions Esprit, 01/2013, p. 32-49, § 10

[244] En ce sens *v*. BAUDIN Laura, « *Les cyberattaques dans les conflits armées* », éditions L'Harmattan, 2014, p. 54

[245] En ce sens *v*. MONGIN Dominique, « *Les cyberattaques, armes de guerres en temps de paix* », éditions Esprit, 01/2013, p. 32-49, § 8-9

[246] Le Monde, « *les risques de cyberattaques contre les centrales nucléaires se multiplient* », 06.10.2015

160. Cette similarité des effets et des conséquences est d'ailleurs confirmée par les experts en la matière. Le Manuel de Tallinn, rédigé par un groupe d'experts après la cyberattaque subie par l'Estonie en 2007 a justement pour objectif de faire l'ébauche d'un régime juridique applicable aux cyberattaques, et exprime à cette fin à quelles conditions une cyberattaque pourrait constituer un recours à la force. Bien qu'il n'est pas un caractère obligatoire puisqu'il n'est que le fruit d'un collège d'experts, il apporte cependant des précisions et des indications importantes en la matière comme le reconnaît d'ailleurs le C.I.C.R.[247] puisque les experts se sont basés sur des indicateurs utilisés internationalement pour déterminer dans quelles conditions une cyberattaque constitue un recours à la force. Il démontre également, à l'instar d'autres développements en la matière, d'une « *volonté de normalisation* »[248] en matière de cyberattaque.

161. Le Manuel de Tallin a en effet soutenu qu'une « *cyberattaque constitue une menace ou un recours à la force* » et « *constitue un usage de la force quand l'ampleur et les effets sont comparables à une attaque dite classique* »[249]. Pour déterminer à partir de quel moment les effets entre une cyberattaque et une attaque cinétique sont comparables, les experts ont dégagé huit critères, évalués de façon holistique[250].

162. Les experts ont commencé par le critère de la gravité de l'attaque c'est-à-dire qu'une cyberattaque serait similaire dans sa gravité à une attaque cinétique dès lors qu'elle porterait atteinte aux personnes, aux propriétés et aux intérêts critiques nationaux[251]. Ces conséquences doivent ensuite être immédiates, et doivent donc suivre immédiatement la cyberattaque ou avoir lieu au cours de celle-ci. Cela induit que plus les conséquences se produisent rapidement, plus la cyberattaque sera considérée comme un recours à la force équivalent à une attaque cinétique.[252] Les experts ont également insisté sur l'effet direct qu'il doit y avoir entre la cyberattaque et ses conséquences. Les conséquences et les effets de la cyberattaque doivent avoir été directement causés par la

---

[247] C.I.C.R., « *Quelles limites le droit de la guerre impose-t-il aux cyberattaques ?* », 28.06.2013 https://www.icrc.org/fre/resources/documents/faq/130628-cyber-warfare-q-and-a-eng.htm

[248] En ce sens *v.* TAILLAT Stéphane, « *un mode de guerre hybride dissymétrique ? Le cyberespace* », éditions Institut de Stratégie Comparée, 2016/1 (n°111), p. 89-106, § 27

[249] Manuel de Tallin paru en 2013 2.0, Règle 69 Definition of use of force.

[250] En ce sens AKOTO Evelyne. « *Les cyberattaques étatiques constituent-elles des actes d'agression en vertu du droit international public* » : Deuxième partie partie. Revue de droit d'Ottawa - Ottawa Law Review, Faculty of Law, Common Law Section, University of Ottawa, 2015, 46 (2), pp. 199-221, p. 219

[251] Manuel de Tallin paru en 2013 2.0, Règle 69 Definition of use of force 9) a).

[252] *Ibid*. 9) b)

cyberattaque dont l'État a été victime. De plus, la cyberattaque doit également avoir un certain degré d'intrusion dans les réseaux de l'État victime. Enfin, la cyberattaque doit avoir des effets et des conséquences mesurables. Le fait que ceux-ci doivent pouvoir être estimés renvoie à la notion de dommages matériels. Cela induit donc que la cyberattaque ne sera un recours à la force, selon le Manuel de Tallinn, que « *si ses dimensions et ses effets sont pareils à ceux que l'on aurait obtenus après l'emploi d'armes cinétiques* »[253]. Il faut également que la cyberattaque ait un caractère militaire et, bien entendu, qu'elle soit le fruit d'un État.

163. Ce dernier critère est un des plus difficiles à fournir, l'attribution d'une cyberattaque à un État étant extrêmement compliquée. En effet « *L'imputation juridique d'une cyberattaque à un État est un exercice assez difficile, en raison : soit du caractère clandestin des attaques lorsqu'elles sont commises par des agents d'un État, soit de l'opacité enveloppant la nature exacte des liens existant entre un État et les personnes privées, auteures d'une attaque informatique contre un autre État* ».[254] Devant cette difficulté, il peut donc être « *extrêmement ardu, voire impossible, d'imputer une cyberattaque à un État* » étant donné que les auteurs de cyberattaques masquent leurs traces, et qu'il est donc très difficile de remonter jusqu'à eux. Et quand bien même cela s'avère possible, il est souvent compliqué d'attribuer une cyberattaque à un État lorsque ce dernier passe par des organismes privés, d'autant que l'article 8 du projet d'article de la Commission du Droit International (C.D.I.) exige la preuve du contrôle de l'État[255], contrôle qui, selon les exigences de la C.I.J., doit être effectif[256]. Pour illustrer ce constat, « *l'exemple géorgien est la parfaite illustration de ce qui s'apparente à un nœud gordien* ».[257]

164. Si le Manuel de Tallinn a développé huit critères pour encadrer la qualification de recours à la force d'une cyberattaque, compte tenu que les cyberattaques sont très

[253] AKOTO Evelyne. « *Les cyberattaques étatiques constituent-elles des actes d'agression en vertu du droit international public* » : Deuxième partie partie. Revue de droit d'Ottawa - Ottawa Law Review, Faculty of Law, Common Law Section, University of Ottawa, 2015, 46 (2), pp. 199-221, p. 219
[254] *Ibid*. p. 221
[255] *Ibid*. p. 222
[256] C.I.J « *Application de la convention pour la prévention et la répression du crime de génocide* » (Bosnie-Herzégovine *c.* Serbie-et-Monténégro), arrêt, C.I.J. Recueil 2007, p. 43
[257] AKOTO Evelyne. « *Les cyberattaques étatiques constituent-elles des actes d'agression en vertu du droit international public* » : Deuxième partie partie. Revue de droit d'Ottawa - Ottawa Law Review, Faculty of Law, Common Law Section, University of Ottawa, 2015, 46 (2), pp. 199-221, p. 222

complexes et peuvent être amenées à évoluer dans le temps, il faut noter que « *les critères proposés par Schmitt ne sont pas exhaustifs et que les États pourront considérer en fonction des circonstances, d'autres facteurs tels que le climat politique, d'imminentes manœuvres militaires, l'identité de l'attaquant, les antécédents de celui-ci en matière de cyberopérations ainsi que la nature de la cible telles que les infrastructures critiques.*[258] Par conséquent, *« La qualification d'une cyberattaque devra se faire au cas par cas* »[259] ce qui laisse entendre que le régime prévu pour les cyberattaques devra lui aussi être non-exhaustif afin de permettre son évolution. Il faudrait donc « *repenser la notion d'agression armée afin de l'ajuster* »[260]. Toutefois, à ce jour, l'analyse d'une cyberattaque constituant un emploi de la force voire une agression, selon ses dimensions et ses effets s'ils sont pareils à ceux obtenus après l'emploi d'armes cinétiques, développée par Schmitt et retenue dans le Manuel de Tallin[261], semble *« la démarche [...] la mieux appropriée à l'examen d'une cyberattaque étatique survenue en temps de paix, au regard des dispositions de l'article 2(4) de la Charte* ».[262]

165. Au terme de cette première partie, il apparaît que les cyberattaques étatiques peuvent être des recours à la force étant donné qu'elles sont perçues et utilisées comme telles. Elles peuvent également avoir les mêmes effets et les mêmes conséquences dévastateurs que des attaques cinétiques. Devant ce constat, il apparaît nécessaire de reconnaître que les cyberattaques peuvent être des recours à la force tout comme les attaques cinétiques, et qu'à ce titre, elles sont susceptibles, elles-aussi, de constituer une agression. Or, il sera nécessaire qu'une agression constituée par un recours à la force issue d'une cyberattaque, puisse entraîner les mêmes conséquences qu'une agression constituée par un recours à la force réalisé par une attaque conventionnelle.

---

[258] AKOTO Evelyne. « *Les cyberattaques étatiques constituent-elles des actes d'agression en vertu du droit international public* » : Deuxième partie partie. Revue de droit d'Ottawa - Ottawa Law Review, Faculty of Law, Common Law Section, University of Ottawa, 2015, 46 (2), pp. 199. P. 219, note de bas de page 177
[259] *Ibid*.
[260] LOUIS-SIDNEY Barbara, « *La dimension juridique du cyberespace* », éditions revue internationale et stratégique, 2012/3 (n°87), p. 73-82, § 16
[261] En ce sens voir AKOTO Evelyne. « *Les cyberattaques étatiques constituent-elles des actes d'agression en vertu du droit international public* » : Deuxième partie partie. Revue de droit d'Ottawa - Ottawa Law Review, Faculty of Law, Common Law Section, University of Ottawa, 2015, 46 (2), pp. 199. p. 219
[262] *Ibid*. p. 221

Partie II : L'extension de la notion d'agression afin d'y inclure les cyberattaques : les conséquences de cette évolution.

Les cyberattaques appellent l'extension de la notion d'agression afin de les y inclure. Les agressions pourraient dès lors être constituées par des attaques cinétiques ainsi que des cyberattaques, réalisées en temps de paix et dépassant une certaine intensité. Ce constat dressé, il semble nécessaire de s'interroger sur les conséquences juridiques qu'entraînerait cette extension de la notion d'agression aux cyberattaques. Cette extension pourrait avoir pour conséquence la responsabilité de l'État responsable de la cyberattaque, mais aussi déclencher des réactions légitimes de la part des autres États.

Chapitre 1 : Première conséquence, l'imputation de la cyberattaque à l'État responsable.

Dans ce chapitre, nous allons voir qu'une cyberattaque constituant une agression doit entraîner les mêmes conséquences qu'une agression par attaque conventionnelle. Une cyberattaque constituant une agression entraînerait donc la responsabilité de l'État agresseur pour fait internationalement illicite (F.I.I.), et permettrait des ripostes de la part de l'État victime.

Section 1 : La naissance de la responsabilité internationale étatique pour agression.

Dans cette section, nous aborderons les conséquences d'une agression constituée par une cyberattaque en matière de responsabilité internationale.

Paragraphe 1 : Un fait internationalement illicite constitué par la violation des principes fondamentaux du droit international.

Dans ce paragraphe, il sera question de la possibilité d'engager la responsabilité internationale de l'État responsable, l'agression par cyberattaque étant un fait internationalement illicite selon les principes fondamentaux du droit international.

166. Un fait internationalement illicite est réalisé par un État « *lorsqu'un comportement consistant en une action ou une omission est attribuable à l'État en vertu du droit international et constitue une violation d'une obligation internationale par un État* »[263]. Peu importe sa qualification en droit interne dès lors qu'il est qualifié de F.I.I. en droit international[264], et dès sa commission la responsabilité de l'État agresseur est engagée.[265]

167. Les cyberattaques étant reconnues comme des agressions peuvent constituer un tel fait illicite. En effet, d'une part une cyberattaque étatique remplit les deux critères d'un F.I.I. à savoir : l'attribution à un État et la violation d'une obligation internationale[266] ; et d'autre part, en 2013, « *un groupe d'experts gouvernementaux de la première commission de l'O.N.U. sur le désarmement et la sécurité internationale déclara que le droit international, et en particulier la Charte des Nations unies, s'applique dans le cyberespace* »[267]. Les cyberattaques sont donc à même de constituer un F.I.I. si elles violent le droit international (en particulier la C.N.U.) et ses principes fondamentaux.

168. Or, une cyberattaque constituant une agression est une violation de plusieurs obligations internationales. Tout d'abord, elle est une violation de l'interdiction de recours à la force[268], « *pierre angulaire* »[269] du mécanisme des Nations unies. Comme vu précédemment[270], le système des Nations unies a fait de l'interdiction du recours à la force entre États l'élément central des relations internationales modernes, et a prohibé tout recours à la force entre États, et particulièrement les agressions, recours à la force d'un État contre un autre État en temps de paix. Or, les cyberattaques peuvent constituer des actes semblables à des recours à la force étatique, atteignant une telle intensité qu'elles peuvent être similaires à des recours à la force constituant une agression. Les cyberattaques étatiques, dès lors qu'elles constituent des agressions, violent le principe d'interdiction de recours à la force entre États, et constituent un crime d'agression.

---

[263] C.D.I., « *Projet d'articles sur la responsabilité de l'État pour fait internationalement illicite* », Documents officiels de l'Assemblée générale, cinquante-sixième session, Supplément n° 10 (A/56/10), article 2
[264] *Ibid*. article 3
[265] *Ibid*. article 1er
[266] POMES Eric, « *Droit International Public* », éditions Panorama du droit, 2012, p. 247
[267] Le Monde, « *Penser la cyberpaix* », 04.2016, p. 18
[268] Charte des Nations unies, article 2 § 4
[269] C.I.J., « *Activités armées sur le territoire du Congo* », REC. 2005, § 148
[270] Partie I, Chapitre 1, Section 1, Paragraphe 1, § 37

169. Les cyberattaques étatiques sont également une violation du principe de règlement pacifique des différends. Tous les États sont tenus de régler leurs différends de manière pacifique[271]. Ce principe a été posé par la Charte des Nations unies en son article 2 paragraphe 3. Ce principe consacré par la C.N.U. a également été repris à de nombreuses reprises par l'A.G.N.U. dans ses résolutions, par exemple dans la résolution 37/10 de l'A.G.N.U. de 1982.[272] Le principe de règlement pacifique des différends est donc un principe extrêmement bien posé dans le système des Nations unies.

170. Un différend a été défini par la Cour Permanente de Justice Internationale (C.P.J.I.) comme « *un désaccord sur un point de droit ou de fait, une contradiction, une opposition de thèse juridique ou d'intérêt entre deux personnes* »[273]. Dans l'affaire du Sud-Ouest Africain, la C.I.J. a précisé qu'un différend existe lorsqu'une « *prétention se heurte à l'opposition manifeste de l'autre* »[274].

171. Les États disposent d'un panel de possibilités pour résoudre leurs différends de manière pacifique. Mais quel qu'il soit, ce doit être un moyen permettant que la « *paix et la sécurité internationales ainsi que la justice ne soient pas mises en danger* »[275]. La Charte des Nations unies consacre à cette fin son chapitre VI en ses articles 33 à 38. L'article 33 notamment énumère les différents moyens à la disposition des États pour résoudre leurs litiges, et l'article 34 précise le rôle du Conseil de sécurité en la matière. En effet, le Conseil de sécurité lui-même peut intervenir pour garantir un règlement pacifique des différends[276].

172. Afin d'éviter de recourir à la force entre eux, les États peuvent avoir recours à des moyens non-juridictionnels et des moyens juridictionnels de règlements des différends[277]. Les moyens non-juridictionnels, aussi appelés moyens diplomatiques,

---

[271] POMES Eric, « *Droit International Publi*c », éditions Panorama du droit, 2012, p. 225
[272] En ce sens *v.* A.G.N.U résolution A/37/590 (IX)
[273] C.P.J.I. « *Affaire des concessions Mavrommatis en Palestine du 30 août 1924* » (Grèce contre Grande-Bretagne), Recueil 1924, Série A - n°2, p. 11, *I.*
[274] C.I.J. « *Affaires du Sud-Ouest africain* » (Éthiopie *c.* Afrique du Sud ; Libéria *c.* Afrique du Sud), Exceptions préliminaires, Arrêt du 21 décembre 1962 : Recueil 1962, p. 319
[275] Charte des Nations unies, article 2 § 3.
[276] En ce sens *v. COMBACAU* Jean, SUR Serge, « *Droit International Public* », LGDJ Lextenso éditions (8ème édition), 2014 p. 563
[277] *Ibid*. p. 564

permettent de trouver une solution aux différends qui ne sera pas obligatoirement basée sur le droit, et qui ne s'imposera pas aux États. Parmi ceux-ci figure la négociation. C'est une discussion organisée entre les parties qui jouissent généralement d'une grande liberté et qui peut répondre à un désir de discrétion des États. La négociation permet souvent de résoudre un différend ce qui explique qu'elle soit parfois une condition préalable à tout autre moyen de règlement des différends, comme cela a été rappelé par la C.I.J. dans l'affaire de l'application de la Convention internationale pour l'élimination des discriminations raciales de 2008 (Géorgie-Russie)[278]. Dans ce cas de figure, la négociation est une obligation de moyen, non de résultat, qui doit toutefois être menée de bonne foi.[279]

173. Viennent ensuite les bons offices, où un tiers s'interpose pour amener les parties à entamer ou reprendre des négociations, comme cela fut le cas pour l'Allemagne dans l'affaire du personnel diplomatique de Téhéran[280]. Une médiation peut également avoir lieu où, là encore, un tiers va intervenir pour aider les États à tenir des négociations, mais va également s'investir dans la recherche d'une solution. Dans la même affaire, l'Algérie a procédé à une médiation à la suite de l'échec des bons offices de l'Allemagne[281].

174. Les États peuvent également avoir recours à une conciliation en chargeant une commission d'examiner le litige sous tous ses angles et proposer un arrangement fondé sur des éléments juridiques et non juridiques, ou demander à une organisation internationale d'intervenir dans la recherche d'une solution pacifique.

175. Les États peuvent enfin avoir recours aux moyens juridictionnels. Ils ont la possibilité de soumettre leur différend à une juridiction qui rendra une solution obligatoire pour eux, fondée sur le droit. Cette solution peut être rendue par un tribunal arbitral, choisi par les parties et investi par ces derniers du pouvoir de rendre une décision obligatoire. Elle peut également être apportée par un règlement judiciaire c'est-à-dire devant une juridiction permanente internationale telle que la C.I.J., dès lors que

[278] En ce sens *v.* C.I.J. « *Application de la convention internationale sur l'élimination de toutes les formes de discrimination raciale* » (Géorgie c. Fédération de Russie), exceptions préliminaires, arrêt, Recueil 2011, p. 70 § 158-159
[279] *Ibid*. § 123
[280] C.I.J « *Personnel diplomatique et consulaire des États-Unis à Téhéran* », arrêt, Recueil 1980, p. 3.
[281] *Ibid*.

les États ont accepté le principe de sa compétence pour régler leur différend et signé ses statuts.[282]

176. Les États disposent donc d'un panel de possibilités pour résoudre leurs différends de manière pacifique et ne pas avoir à recourir à la force, leur permettant ainsi de respecter leur obligation internationale, posée par deux des principes essentiels du système des Nations unies : le règlement pacifique des différends et l'interdiction de recours à la force.

177. Les cyberattaques ne correspondent à aucun des moyens mis à la disposition des États pour résoudre leurs différends pacifiquement sans user de la force. Pire, elles sont exactement à l'opposé.

178. Une cyberattaque, prise dans le cadre d'un différend entre États, destinée à le faire plier ou à le contraindre d'adopter tel ou tel comportement, correspond à une mesure violant le principe de règlement pacifique des différends. En effet, elle permet d'exercer des actes similaires à des recours à la force conventionnels, constituant des recours à la force cybernétiques soit une nouvelle forme de recours à la force. Dès lors, même sans atteindre la qualification d'agression, le simple fait qu'une cyberattaque soit un recours à la force viole les obligations des États posées par l'article 2 de la C.N.U. De surcroit, une cyberattaque étant un recours à la force constituant une agression est une grave violation de ces deux principes majeurs des Nations unies.

179. Certes, il est cependant possible que des cyberattaques ne soient pas le résultat d'un différend au sens juridique du terme, c'est-à-dire, d'une « *prétention [qui] se heurte à l'opposition manifeste de l'autre* »[283]. Par exemple dans l'affaire Stuxnet, les États-Unis, Israël et l'Iran n'étaient pas dans ce qu'il est possible juridiquement d'appeler un différend puisqu'il n'y avait pas de prétention de l'un de ces pays se heurtant à l'opposition d'un autre. Dans ce cas, la cyberattaque peut ne pas être considérée comme étant une violation du principe de règlement pacifique des différends en l'absence de différend au sens juridique. Toutefois, elle demeure une violation du principe d'interdiction de recours à la force entre États posé par l'article 2 paragraphe 4 de la C.N.U.

[282] En ce sens *v.* Statuts de la C.I.J., article 36
[283] Charte des Nations unies, article 2 § 3.

180. Le fait de reconnaître les cyberattaques comme pouvant être des recours à la force constituant des agressions permet donc de qualifier ces dernières de F.I.I. puisqu'elles constituent dès lors des violations d'obligations internationales, en particulier de deux des principes essentiels du mécanisme des Nations unies.

181. Par ailleurs, il a été développé, notamment par Laura Baudin, la nécessité de réaliser un régime spécial afin d'encadrer les cyberattaques de manière spécifique[284], soit conventionnellement, soit par le biais du Conseil de sécurité. Si ces régimes prévoyaient des règles destinées à éviter de telles violations du mécanisme des Nations unies, les cyberattaques étatiques étant des recours à la force constituant des agressions seraient également des violations d'obligations internationales conventionnelles ou posées par le Conseil de sécurité. Le Conseil de sécurité est à même d'intervenir directement pour poser des obligations internationales afin de réglementer l'utilisation des cyberattaques par les États. Ses résolutions sont en effet obligatoires et s'imposent aux États.[285] Le Conseil de sécurité a déjà, par le passé, utilisé ses résolutions pour se poser en législateur et définir des obligations précises pour les États. Le Conseil de sécurité a notamment adopté ce comportement dans sa résolution 1373 sur le terrorisme dans laquelle il intègre un certain nombre d'obligations pour les États concernant la prévention et la répression du terrorisme[286]. Le C.S a ainsi imposé aux États des obligations auxquelles ceux-ci n'avaient pas consenti et s'était posé, en adoptant des énoncés obligatoires généraux abstraits et permanents[287], comme un créateur de normes. Le Conseil de sécurité pourrait donc agir de même et poser des obligations pour les États en matière de cyberattaques. Dès lors, un État violant une résolution du Conseil de sécurité posant un régime destiné à encadrer les cyberattaques violerait ses obligations internationales et commettrait un F.I.I.

182. Enfin, de telles cyberattaques peuvent aussi constituer des violations du D.I.H., mais uniquement lors de conflits armés, comme le rappelait Cordula Droege puisque « *le D.I.H. n'entre en ligne de compte que si des attaques informatiques se produisent*

[284] En ce sens *v.* BAUDIN Laura, « *Les cyberattaques dans les conflits armées* », éditions L'Harmattan, 2014, p. 27
[285] Charte des Nations unies, article 25
[286] En en ce sens *v.* C.S. S/RES/1373 (2001)
[287] *Ibid*.

dans le cadre d'un conflit armé »[288]. Tel qu'exprimé par Laura Baudin, les cyberattaques utilisées dans des conflits armés sont des armes que le D.I.H. est à même d'encadrer.[289] De fait, les obligations internationales du D.I.H. s'imposent aux États lorsqu'ils ont recours à des cyberattaques lors de conflits armés, et leur violation est à même de constituer un F.I.I.

183. Par conséquent, les cyberattaques remplissent tout à fait le premier critère du F.I.I. car elles constituent (et constitueront) la violation d'obligations internationales des États. Les cyberattaques commises par les États sont donc bien des F.I.I., à la condition toutefois de pouvoir les imputer aux États, second critère essentiel pour constituer un F.I.I.

Paragraphe 2 : La condition d'attribution de la cyberattaque à l'État, essentielle mais problématique au vu de la technologie actuelle.

Dans ce paragraphe, nous verrons les difficultés d'attribution d'une cyberattaque à un État, condition pourtant essentielle pour engager la responsabilité internationale de l'État responsable, mais qui pourrait à terme être permise par le développement des technologies, avancée technologique qu'il faut par conséquent anticiper.

184. Un F.I.I. ne peut engager la responsabilité d'un État que s'il est commis par ce dernier. Il est donc nécessaire d'attribuer la violation des obligations internationales de l'État à l'État en question afin de « *désigner l'auteur de l'acte illicite* »[290].

185. L'imputation d'un acte à un État peut être opérée dès lors qu'il résulte de l'État lui-même ou de ses organes et agents. Ces organes *de jure* de l'État engagent la responsabilité de l'État[291] pour tout acte commis dans leurs fonctions, même s'ils ont outrepassé leurs compétences (excès de pouvoir) ou agi de manière contraire aux

[288] DROEGE Cordula, « *Pas de vide juridique dans le cyberespace* », C.I.C.R., 16.08.2011, *in* BAUDIN Laura, « *Les cyberattaques dans les conflits armées* », éditions L'Harmattan, 2014, p. 85
[289] En ce sens *v.* BAUDIN Laura, « *Les cyberattaques dans les conflits armées* », éditions L'Harmattan, 2014, p. 86
[290] POMES Eric, « *Droit International Public* », éditions Panorama du droit, 2012, p. 252
[291] C.D.I., « *Projet d'articles sur la responsabilité de l'État pour fait internationalement illicite* », Documents officiels de l'Assemblée générale, cinquante-sixième session, Supplément n° 10 (A/56/10), article 4

instructions qui leur ont été données[292]. L'État n'est pas responsable de leurs actes dans l'unique hypothèse où ce sont des actes privés, c'est-à-dire détachés de tout lien avec leurs fonctions. Si un acte est commis grâce aux fonctions de l'organe ou de l'agent de l'État, il ne sera pas considéré comme privé.

186. Ensuite, l'État est responsable des personnes étant sous son contrôle « *si cette personne ou ce groupe de personnes, en adoptant ce comportement, agit en fait sur les instructions ou les directives ou sous le contrôle de cet État* »[293]. Sont visées ici les personnes qui ne sont pas des organes ou des agents de l'État mais qui agissent tout de même sous son contrôle. S'est ainsi posé la question du moment à partir duquel l'État contrôle ces personnes.

187. Deux thèses ont été confrontées : celle du contrôle effectif et celle du contrôle global. Le contrôle effectif a été dégagé par la C.I.J. dans l'affaire des Activités militaires et paramilitaires au Nicaragua et contre celui-ci. Dans cette affaire, la C.I.J. a établi que ce contrôle doit être « *tellement étroit que les individus doivent être considérés comme un organe de fait de l'État* »[294], et qu'il doit « *s'exercer pour chacune des opérations au cours desquelles les violations se sont produites* »[295]. Le contrôle effectif nécessite donc soit que l'État ait eu le contrôle de l'opération dans laquelle s'est produite la violation, soit qu'il ait donné des instructions ou des directives précises quant à la conduite de l'opération, soit que celle-ci soit dans le cadre d'une de ses activités[296]. La C.I.J. a opté pour cette solution afin de ne pas trop distendre la responsabilité de l'État et le principe selon lequel un État n'est responsable que de son propre fait.

188. Une seconde thèse a été avancée par le Tribunal pénal international pour l'Ex-Yougoslavie (T.P.I.Y.). Dans l'affaire Procureur *c*. Tadic[297], ce dernier a estimé qu'un État pouvait être responsable des actes d'une personne qui n'était pas un de ses organes ou un de ses agents, mais qui agissait sous son contrôle, dès lors que l'État exerçait un contrôle global des opérations à laquelle cette personne a participé.

---

[292] C.D.I., « *Projet d'articles sur la responsabilité de l'État pour fait internationalement illicite* », Documents officiels de l'Assemblée générale, cinquante-sixième session, Supplément n° 10 (A/56/10), article 7
[293] *Ibid*. article 8
[294] POMES Eric, « *Droit International Publi*c », éditions Panorama du droit, 2012, p. 252
[295] *Ibid*.
[296] En ce sens *v*. SIMONET Loïc, « *L'usage de la force dans le cyberespace et le droit international* », Annuaire de droit français international, 2012, 58, pp. 117-143, p. 134
[297] En ce sens *v*. T.P.I.Y. « *Le Procureur c/ Dusko Tadic* », arrêt du 15 juillet 1999

189. La C.I.J. a refusé d'appliquer le critère du contrôle global dans l'affaire de l'application de la Convention pour la répression du génocide (Bosnie *c*. Serbie) et a confirmé l'application du critère du contrôle effectif pour déterminer si la Serbie était responsable des actes de personnes ayant commis un génocide, ce qui l'a conduit a déclaré que le contrôle n'étant pas effectif, « *la Serbie-Monténégro n'a pas commis de génocide en Bosnie sauf à Srebrenica* »[298].

190. Un État pouvant donc être responsable pour les actes de ses organes et de ses agents ou des personnes qu'il a sous son contrôle, des cyberattaques commises par ces personnes doivent entraîner la responsabilité de l'État pour lequel elles agissent, si elles violent les obligations internationales dudit État. Toutefois, si cette attribution a pu être dans le passé source de vifs débats, l'attribution des cyberattaques, élément pourtant essentiel à la reconnaissance d'un F.I.I., est le défi majeur qui se pose au droit international.

191. En effet, l'attribution des cyberattaques est la difficulté qui se pose pour les imputer aux États[299] car une cyberattaque a pour principale caractéristique d'être anonyme. D'ailleurs, « *l'anonymat, la discrétion, la rapidité sont autant de caractéristiques permettant d'envisager les cyberattaques comme des armes parfaites* »[300].

192. Les cyberattaques sont donc par leurs caractéristiques même extrêmement difficiles à tracer. Si l'Estonie « *se doutait bien d'où provenaient les cyberattaques, le problème est celui de la traçabilité* »[301]. Quand les États réalisent des cyberattaques, ils s'appliquent effectivement à masquer leurs traces pour deux raisons, inhérentes à la nature même des cyberattaques. Tout d'abord, les États « *ne souhaitent pas être identifiés comme étant le premier à avoir lancé une cyberattaque* »[302]. Si cela est déjà le comportement adopté par les États, l'élaboration d'un régime permettant la reconnaissance de l'illicéité des cyberattaques et, *de facto*, la possibilité d'engager leur responsabilité les confortera dans leur choix de rester les plus anonymes possible.

---

[298] POMES Eric, « *Droit International Public* », éditions Panorama du droit, 2012, p. 252
[299] En ce sens *v*. SIMONET Loïc, « *L'usage de la force dans le cyberespace et le droit international* », Annuaire de droit français international, 2012, 58, pp. 117-143, p. 135
[300] BAUDIN Laura, « *Les cyberattaques dans les conflits armées* », éditions L'Harmattan, 2014, p. 9-10 (préface)
[301] *Ibid*. p. 38
[302] *Ibid*. p. 38

193. Ensuite, les États cherchent à ne pas être identifiés car, comme l'a fait remarquer Daniel Ventre, « *signer des cyberattaques, c'est révéler aux autres acteurs du droit international le niveau de technicité qu'on a soi-même atteint, niveau qu'on ne veut bien évidemment pas divulguer* »[303].

194. Toutefois, cette difficulté de traçabilité pourrait bien finir par être surmontée. En effet, les États commencent à chercher des moyens d'identifier les auteurs des cyberattaques qu'ils subissent. Comme Michel Baud le faisait remarquer, ce constat sur la traçabilité est susceptible d'évoluer devant les efforts des États déployés en la matière. Citons l'exemple du ministère de la Défense japonais « *a mandaté l'entreprise Fujitsu pour réaliser une cyberarme susceptible d'identifier la source des cyberattaques par DDoS (Distribued Denial of Service, c'est-à-dire par déni de services), ainsi que les auteurs de vols de données* »[304]. Selon Pierre Fontaine, « *là où ce virus-antivirus se distingue d'un simple antivirus, c'est qu'il va collecter des informations en remontant la piste de l'attaque. Ainsi, d'ordinateurs en serveurs infectés, il va réparer les dégâts ou au moins effacer les traces du virus et tenter d'atteindre l'ordinateur source, celui d'où sont partis les premiers assauts. Ce bon virus serait opérationnel aussi bien contre les attaques en déni de service que contre les tentatives d'intrusion visant à voler des données* »[305]. Il apparaît donc que cette difficulté de traçabilité pourrait être surmontée par les États au moyen du développement de technologies à même de tracer les cyberattaques. Cela serait donc une avancée dans la recherche de l'attribution des cyberattaques aux États afin d'engager leur responsabilité pour F.I.I.

195. Cependant, des problèmes subsisteraient pour réussir à attribuer une cyberattaque à un État : des problèmes liés à la preuve du contrôle de l'État dans l'opération. En effet, la finalité de ce travail de traçabilité n'est pas de parvenir à identifier de quel État la cyberattaque a été lancée, mais quel État l'a lancée. Cela implique bien évidemment de remonter à la source de la cyberattaque, puis ensuite de prouver l'implication de l'État. Car, comme Nicolas Arpagian le fait justement

---

[303] BAUDIN Laura, « *Les cyberattaques dans les conflits armées* », éditions L'Harmattan, 2014, p. 38
[304] BAUD Michel, « *La cyberguerre n'aura pas lieu, mais il faut s'y préparer* », Revue de l'institut français des relations internationales, Politique étrangère, volume 77, été 2012, p. 305 à 314 *in* BAUDIN Laura, « *Les cyberattaques dans les conflits armées* », éditions L'Harmattan, 2014, p. 41
[305] FONTAINE Pierre, « *Virus et cyberattaques, le Japon soigne le mal par le mal* », 04.01.2012 *in* BAUDIN Laura, « *Les cyberattaques dans les conflits armées* », éditions L'Harmattan, 2014, p. 41

remarquer, « *il est très difficile, voire impossible, d'établir avec certitude l'origine géographique de la cyberattaque, et même l'origine géographique de l'attaque ne suffirait pas à imputer à l'État du pays en question la responsabilité* »[306]. Pourquoi ? Parce que se poserait dans ce cas la question de l'attribution de cette cyberattaque à l'État, c'est-à-dire si cette cyberattaque sur son sol a été réalisée par des organes, des agents ou des personnes sous le contrôle de l'État. Or, c'est ici que se pose la seconde difficulté, et non la moindre.

196. En effet, il serait possible qu'une cyberattaque soit lancée par des organes et des agents de l'État à partir d'infrastructures étatiques. Il est notamment possible de citer le cas de la Chine qui a lancé des cyberattaques depuis des infrastructures étatiques. Des « *attaques sophistiquées persistantes (A.P.T.)* » réalisées contre des entreprises américaines ont été analysées et ont permis de remonter *« à l'unité 61 398 de l'armée chinoise en charge des opérations sur les réseaux informatiques* »[307]. Dans de tels cas, l'attribution d'une cyberattaque semblerait à première vue concevable étant donné que le lien entre l'État et les organes ou les agents responsables (ainsi qu'avec l'utilisation de leurs fonctions) serait assez facile à établir. Dès lors que les cyberattaques seront bel et bien reconnues comme étant des F.I.I. permettant d'engager la responsabilité d'un État, il serait donc légitime que les États responsables voient leur responsabilité engagée.

197. Cependant, toutes les cyberattaques ne sont pas lancées depuis des infrastructures étatiques, et ce lien avec l'État pourrait être beaucoup plus problématique si les cyberattaques étaient lancées par des particuliers sous le contrôle dudit État. Or, pour réaliser des cyberattaques, les États ont souvent recours à des hackers qui ne font partie ni de ses organes ni de ses agents car, comme l'a expliqué Charles Bweles, *« il est difficile de prouver de manière incontestable l'implication d'un autre État dans le cas d'une cyberattaque, car dans le cyberespionnage comme dans la cyberguerre, les organisations évitent autant que possible d'appuyer elles-mêmes sur le déclic ou la*

[306] ARPAGIAN Nicolas, « *La cyberattaque, nouvelle arme de guerre des États ?* », site Internet France Info, 22.03.2013, *in* BAUDIN Laura, « *Les cyberattaques dans les conflits armées* », éditions L'Harmattan, 2014, p. 40

[307] DOUZET Frédéric, « *Chine, États-Unis : la course aux cyberarmes a commencé* », éditions sécurité globale, 2013, n°23, pp 43-51, § 3

détente électronique »[308]. C'est pourquoi sont plutôt utilisés « *des moyens indirects comme recourir à des hackers doués dans les arts numériques du camouflage et de la diversion* »[309]. Cela est également une pratique commune des États, et dans ce cas de figure le lien ne serait pas automatique[310]. Il faudrait donc l'établir en prouvant que l'État exerçait un contrôle effectif sur l'opération de cyberattaque réalisée par cette personne, soit en ayant le contrôle de l'opération, soit en ayant donné des instructions ou des directives précises, soit que cette opération ait été réalisée dans le cadre d'une activité de l'État[311]. Or, la preuve d'un tel contrôle de l'État sur un groupe d'hackers est extrêmement délicate à apporter, de surcroît si celui-ci se trouve sur le territoire dudit d'État en raison même de la nature de la cyberattaque. L'attaque ayant été réalisée à distance, il sera dès lors très difficile de pouvoir prouver le contrôle de l'État par témoignages comme cela a été le cas lors de l'affaire C.I.J. Bosnie *c*. Serbie de 2007[312]. De plus, les auteurs de la cyberattaque résidant dans l'État, il ne sera pas possible de les arrêter et de les interroger sans l'accord de l'État lui-même, chose qu'il refusera systématiquement. Cet ensemble de facteurs combinant une réalisation à distance, un manque de témoins et une protection de l'État responsable grâce à son droit de souveraineté sur son territoire rend l'attribution de la cyberattaque à l'État presque impossible.

198. Par exemple, de nombreuses cyberattaques ont été officieusement attribuées à la Russie. Lors des cyberattaques contre le parti démocrate au cours de la campagne d'Hilary Clinton[313] ou encore contre le gouvernement fédéral allemand[314], la Russie a été clairement pointée du doigt. Il a été possible de tracer et d'attribuer ces cyberattaques à des hackers venant de Russie, et à des groupes russes. Ces cyberattaques ont ainsi été tracées comme provenant du groupe russe « *Fancy Bear* »[315]. Ce groupe est en effet

---

[308] BWELES Charles, « *Peut-on dissuader dans le cyberespace ?* » *in* BAUDIN Laura, « *Les cyberattaques dans les conflits armées* », éditions L'Harmattan, 2014, p. 40
[309] *Ibid*.
[310] En ce sens *v*. SIMONET Loïc, « *L'usage de la force dans le cyberespace et le droit international* », Annuaire de droit français international, 2012, 58, pp. 117-143, p. 135
[311] *Ibid*. p. 136
[312] C.I.J. *Application de la convention pour la prévention et la répression du crime de génocide* du 26 février 2007 (Bosnie-Herzégovine *c.* Serbie-et-Monténégro), fond, arrêt, Recueil 2007
[313] En ce sens *v*. The Huffington post, « *Ce que nous dit le tableau de chasse de Fancy Bear, les hackers Russes qui ont attaqués Macron* », 25.04.2017
[314] En ce sens *v*. Le Monde, « *L'Allemagne attaquée par des hackeurs Russes* », 01.03.2018
[315] En ce sens *v*. The Huffington post, « *Ce que nous dit le tableau de chasse de Fancy Bear, les hackers Russes qui ont attaqués Macron* », 25.04.2017

spécialisé dans le piratage de *« ministères, armées, partis politiques, industriels dans le secteur de la défense, organisation internationales, ONG russes ou encore médias »*[316].Toutefois, même si ce groupe est considéré comme proche du gouvernement russe[317], d'autant que ces cibles « *se recoupent souvent avec les intérêts russes* »[318], et que le traçage des cyberattaques a permis d'établir que « *les adresses IP atterrissent en Russie* »[319], il a été impossible pour les victimes des cyberattaques « *de faire le lien formel avec le gouvernement russe* »[320], ainsi que d'être en mesure de prouver le contrôle de l'État russe sur le groupe *Fancy Bear*[321]. De cette manière, malgré le fait d'avoir pu tracer les cyberattaques, l'absence de preuve du lien entre les auteurs des cyberattaques et le gouvernement d'un État empêche l'attribution. Or, sans attribution, il n'est pas possible de poursuivre un État pour F.I.I. et *de facto*, *« la quasi-impossibilité d'attribuer l'attaque informatique à un État neutralise la qualification d'agression »*[322]. C'est donc le véritable défi qui se pose en matière de cyberattaque et qui devra faire l'objet d'une attention particulière sur la manière de prouver l'implication d'un État.

199. Il faudra donc trouver des moyens d'assurer la preuve pour qu'un État victime d'une cyberattaque puisse engager la responsabilité de l'État responsable. Cela permettra également de garantir l'effectivité d'un régime prohibant les agressions par attaque conventionnelle ou par cyberattaque. Enfin, cela permettra d'éviter que les États aient recours à des groupes comme celui des *Fancy Bear* pour réaliser des cyberattaques[323]. S'il n'est pas possible de lutter contre la réalisation à distance des cyberattaques ainsi que contre l'absence de témoins extérieurs (cela étant inhérent à la nature même des cyberattaques), il faut donc orienter nos efforts vers la poursuite des auteurs. Le moyen de permettre l'attribution d'une cyberattaque à un État pourrait être dans la certitude d'arrêter les auteurs, et donc d'avoir une chance de prouver le contrôle

[316] The Huffington post, « *Ce que nous dit le tableau de chasse de Fancy Bear, les hackers Russes qui ont attaqués Macron* », 25.04.2017
[317] En ce sens *v.* Le Monde, « *L'Allemagne attaquée par des hackeurs Russes* », 01.03.2018
[318] En ce sens *v.* The Huffington post, « *Ce que nous dit le tableau de chasse de Fancy Bear, les hackers Russes qui ont attaqués Macron* », 25.04.2017
[319] *Ibid*.
[320] *Ibid*.
[321] *Ibid*.
[322] LOUIS-SIDNEY Barbara, « *La dimension juridique du cyberespace* », éditions revue internationale et stratégique, 2012/3 (n°87), p. 73-82, § 14
[323] En ce sens *v.* The Huffington post, « *Ce que nous dit le tableau de chasse de Fancy Bear, les hackers Russes qui ont attaqués Macron* », 25.04.2017

de l'État, qu'il soit direct, par instructions, par directives ou dans le cadre d'une de ses activités[324]. Par exemple, il est possible d'envisager de confier à la CPI la poursuite des hackers responsables de cyberattaques, qui ensuite pourra les déférer aux États-victimes.

Section 2 : La mise en œuvre de la responsabilité internationale de l'État agresseur.

Dans cette section, nous aborderons la mise en œuvre de la responsabilité de l'État responsable et les conséquences que cela impliquerait.

200. Une fois la cyberattaque reconnue comme un F.I.I., il sera donc possible d'engager la responsabilité de l'État responsable de la cyberattaque. L'État victime sera donc en mesure de l'invoquer, mais également les autres États si l'on considère que les cyberattaques, étant un recours à la force et constituant une agression, violent des normes *erga omnes*, où tous les États ont un intérêt à agir en cas de violation.

Paragraphe 1 : L'engagement de la responsabilité de l'État agresseur.

Dans ce paragraphe, il sera question de la possibilité pour l'État victime, mais également pour l'ensemble de la communauté internationale, d'engager la responsabilité de l'État responsable.

201. Dès lors que les cyberattaques sont reconnues comme étant des F.I.I., alors la responsabilité de l'État responsable peut être engagée. L'État victime et l'État responsable se verront ainsi octroyer de nouveaux droits et obligations, le F.I.I. donnant naissance à une nouvelle relation juridique entre eux puisque « *la responsabilité internationale de l'État qui […] résulte d'un fait internationalement illicite comporte les conséquences juridiques* »[325] suivantes, parmi lesquelles le maintien de l'obligation primaire, les obligations de cessation et de non-répétition ainsi que la réparation.[326] La responsabilité internationale recouvre ainsi « *toute les sortes de relations nouvelles qui*

[324] En ce sens *v.* SIMONET Loïc, « *L'usage de la force dans le cyberespace et le droit international* », Annuaire de droit français international, 2012, 58, pp. 117-143, p. 135
[325] C.D.I., « *Projet d'articles sur la responsabilité de l'État pour fait internationalement illicite* », Documents officiels de l'Assemblée générale, cinquante-sixième session, Supplément n° 10 (A/56/10), article 34
[326] *Ibid*. Chapitre II

peuvent naître, en droit international, du fait internationalement illicite d'un État »[327]. Il sera donc possible pour l'État victime d'exiger le maintien de l'obligation primaire ainsi qu'une cessation de l'illicite et une garantie de non-répétition, mais aussi de demander réparation à l'État responsable.

202. Les cyberattaques similaires à des recours à la force et constituant une agression sont donc des violations d'obligations internationales conventionnelles, à savoir pour le moment l'article 2 paragraphe 3 et l'article 2 paragraphe 4 de la C.N.U. Elles peuvent également être (et doivent être) de potentielles violations pour les régimes juridiques à venir encadrant les cyberattaques. Les États violant ces obligations et commettant un F.I.I. sont cependant toujours tenus d'exécuter leurs obligations primaires car « *les conséquences juridiques d'un fait internationalement illicite [...] n'affectent pas le maintien du devoir de l'État responsable d'exécuter l'obligation violée* »[328]. Les obligations primaires correspondent aux obligations qui liaient les États antérieurement au F.I.I. En matière de cyberattaque, il s'agit de l'interdiction pour les États de réaliser une cyberattaque étant un recours à la force et constituant une agression contre un autre État. Cette interdiction de recourir à la force et d'agresser un État par ce biais est donc toujours en vigueur au moment de la commission du F.I.I. et, par conséquent, l'État responsable est normalement toujours tenu de s'y conformer.

203. Cependant, si l'État responsable n'a pas encore cessé sa cyberattaque, l'État victime est en droit de lui demander de cesser son illicéité. En effet, les obligations secondaires de l'État responsable, celles qui naissent avec la commission du F.I.I., permettent à l'État victime d'exiger la cessation de l'illicéité.[329] L'État responsable doit en effet « *mettre fin si ce fait continue* » à la violation de ses obligations internationales afin de pouvoir reprendre son obligation primaire, mais aussi de pouvoir remplir une autre de ses obligations secondaires, l'obligation de réparation. En effet, « *la cessation n'est pas un élément de la réparation, elle en est à condition lorsque, du moins, le fait*

[327] Annuaire de la C.D.I., 1973, vol II, p. 178 *in* POMES Eric, « *Droit International Public* », éditions Panorama du droit, 2012, p. 246
[328] C.D.I., « *Projet d'articles sur la responsabilité de l'État pour fait internationalement illicite* », Documents officiels de l'Assemblée générale, cinquante-sixième session, Supplément n° 10 (A/56/10), article 29 *in* DUPUY Pierre-Marie et KERBRAT Yann, « *Droit International Public* », éditions Dalloz (13ème édition), 2016, p. 548
[329] En ce sens *v.* DUPUY Pierre-Marie et KERBRAT Yann, « *Droit International Public* », éditions Dalloz (13ème édition), 2016, p. 548

générateur de la responsabilité est un fait illicite continu »[330]. Les États victimes doivent donc pouvoir exiger la cessation de la cyberattaque de la part de l'État responsable.

204. Au besoin ils peuvent également demander des garanties de non-répétition. Ces garanties de non-répétition ne sont pas automatiques. En effet, l'État responsable doit « *offrir des assurances et des garanties de non-répétition appropriées si les circonstances l'exigent* »[331] Ces assurances et garanties de non-répétition ont pour but de restaurer la confiance entre les États en assurant à l'État victime qu'il ne verra plus ses droits violés. C'est donc une obligation de l'État responsable qui, cette fois, est tournée « *vers l'avenir* »[332] car elle n'a pas pour but de réparer mais de prévenir de potentielles violations futures. Toutefois, ces assurances et garanties de non-répétition doivent avoir lieux lorsque les circonstances l'exigent. Cependant, n'étant pas automatiques, elles ne sont pas données pour chaque violation dans le but d'éviter les demandes abusives des États. Il est donc légitime de se demander si, et pourquoi, elles devraient être données pour les cyberattaques.

205. Les cyberattaques, étant des recours à la force constituant à ce titre une agression contre un autre État, doivent entraîner la mise en place de ces assurances et garanties de non-répétition pour deux raisons. D'une part, la nature même des cyberattaques tend à compromettre la confiance entre les États. En effet, les cyberattaques ont un caractère insidieux et discret. Elles sont réalisées à l'insu de l'État victime.[333] Ce dernier a donc des raisons de craindre de nouvelles attaques de la part du même État, qu'il ne pourrait cette fois pas tracer, voire ne même pas remarquer. D'autre part, ce type de cyberattaques sont des violations extrêmement graves du droit international puisqu'elles portent atteinte aux principes fondamentaux des Nations unies : l'interdiction du recours à la force entre États et le règlement pacifique des États. Par conséquent, ce type de cyberattaques portant atteinte aux deux principes majeurs des Nations unies, leurs

[330] DUPUY Pierre-Marie et KERBRAT Yann, « *Droit International Public* », éditions Dalloz (13e éditions), 2016, p. 549
[331] C.D.I., « *Projet d'articles sur la responsabilité de l'État pour fait internationalement illicite* », Documents officiels de l'Assemblée générale, cinquante-sixième session, Supplément n° 10 (A/56/10), article 90
[332] DUPUY Pierre-Marie et KERBRAT Yann, « *Droit International Public* », éditions Dalloz (13e éditions), 2016, p. 549
[333] En ce sens *v. BAUDIN* Laura « *Les cyberattaques dans les conflits armées* », éditions L'Harmattan, 2014, p. 43

réalisations par un État constituent des circonstances suffisamment graves, exigeant donc des assurances et des garanties de non-répétition.

206. Si les États-victimes peuvent invoquer la responsabilité des États responsables de cyberattaques étant des recours à la force et constituant des agressions, devant la gravité de ces faits, les autres États doivent également avoir la possibilité d'invoquer la responsabilité de l'État responsable. En effet, il est possible pour des États autres que l'État directement lésé d'invoquer la responsabilité de l'État responsable dans le cadre de violation d'obligations collectives internationales, c'est-à-dire d' « *obligations erga omnes* »[334]. Ces obligations sont dues à l'ensemble des États, et ces derniers doivent tous les respecter même en l'absence de conventions. Lors de violation de *normes erga omnes*, l'invocation est possible puisqu'il s'agit d'un intérêt commun qui est en péril et que, de ce fait, la défense de cet intérêt général concerne tous les États. Le projet d'article a précisé à cette fin que les « *États autres que l'État lésé* »[335] peuvent dès lors engager la responsabilité de l'État responsable. Mais cette expression est controversée, certains auteurs estimant qu'en cas de violation *erga omnes* tous les États subiraient en fait un préjudice et donc seraient lésés. Toutefois demeure le principe selon lequel des États n'ayant pas été directement lésés peuvent, lors de violations d'obligation *erga omnes*, invoquer la responsabilité de l'État responsable.[336] La Cour a d'ailleurs précisé dans l'affaire *Barcelona Traction* que les obligations *erga omnes* sont bien dues à la communauté dans son ensemble car « *vu l'importance des droits en cause, tous les États peuvent être considérés comme ayant un intérêt à ce que ces droits soient protégés : les obligations dont il s'agit* » étant « *erga omnes* »[337].

207. De surcroît, certaines règles du droit international ne sont pas seulement e*rga omnes*, mais sont considérées comme des normes impératives. Les normes impératives du droit international ont notamment été reconnues par la C.I.J. dans l'affaire *Barcelona Traction*[338]. Ce sont des normes non seulement *erga omnes*, mais également revêtues

[334] DUPUY Pierre-Marie et KERBRAT Yann, « *Droit International Public* », éditions Dalloz (13ème édition), 2016, p. 546
[335] C.D.I., « *Projet d'articles sur la responsabilité de l'État pour fait internationalement illicite* », Documents officiels de l'Assemblée générale, cinquante-sixième session, Supplément n° 10 (A/56/10), article 48
[336] En ce sens *v.* DUPUY Pierre-Marie et KERBRAT Yann, « *Droit International Public* », éditions Dalloz (13ème édition), 2016, p. 546
[337] *Ibid*.
[338] En ce sens *v. C.*I. J. « *Barcelona Traction, Light and Power Company* », Limited, arrêt, C.I.J. Recueil 1970, p. 3.

du *jus cogens* : elles sont tellement essentielles en droit international que tous les États doivent les respecter (caractère *erga omnes*) et qu'aucun État ne peut y déroger même par traité. Tout traité contraire à cette règle étant automatiquement considéré nul (caractère *de jus cogens*). La prohibition de la guerre d'agression fait notamment partie de ces règles. La prohibition de l'agression en droit international est donc une règle *erga omnes* ce qui, par conséquent, fonde l'intérêt à agir de tout État pour protéger cet intérêt collectif.

208. De plus, la possibilité pour tout État d'engager la responsabilité de l'État responsable d'une violation du droit international est également ouverte lorsqu'une même obligation lie plusieurs États en raison d'une convention. Il est en effet possible que des règles de la convention soient considérées comme *erga omnes* à l'égard des États-parties à la convention et que, dès lors, ceux-ci ont tous un intérêt à agir en cas de violation de ces règles par un autre État-partie. Tel est le cas de la Convention sur la torture où la Cour « *a souligné dans l'affaire Belgique c/ Sénégal que les États n'ont pas d'intérêts propres ; ils ont seulement tous, et chacun, un intérêt commun, celui de préserver les fins supérieures qui sont la raison d'être de la Convention* »[339]. Les autres États-parties ont donc la possibilité d'invoquer la responsabilité de l'État responsable « *dans le but, au moins, de faire constater le manquement à de telles obligations* »[340]. Tous les États ont donc un intérêt à agir en cas de violation de cette convention afin de protéger l'intérêt commun. Il s'agit dans ce cas d'obligation *erga omnes partes*.

209. Or, les cyberattaques étant des recours à la force constituant des agressions portent atteinte à des normes *erga omnes* reconnues comme telles par le droit coutumier et la C.I.J., mais aussi à des normes *erga omnes partes* puisque, si l'interdiction du recours à la force et de l'agression sont des principes coutumiers, cette interdiction est aussi posée à l'article 2 paragraphe 4 de la C.N.U.

210. En effet, l'interdiction du recours à la force a tout d'abord un fondement coutumier. La C.I.J. a rappelé le caractère coutumier et conventionnel du principe d'interdiction du recours à la force entre États dans l'affaire des Activités militaires et paramilitaires au Nicaragua et contre celui-ci de 1986. Une cyberattaque, constituant un

[339] En ce sens *v.* DUPUY Pierre-Marie et KERBRAT Yann, « *Droit International Public* », éditions Dalloz (13ème édition), 2016, p. 547
[340] *Ibid*.

recours à la force viole donc le droit coutumier qui s'impose à tous les États en l'absence de convention (à moins qu'il n'ait objecté de manière persistante à cette coutume).

211. Les cyberattaques étant des recours à la force constituant des agressions sont de surcroît illicites, et fondent l'intérêt à agir de tous les États même ceux qui n'ont pas été directement lésés par celles-ci puisque l'agression a été reconnue comme une norme *erga omnes* dans l'affaire Barcelona Traction du 4 février 1970. Dans cette affaire, la Cour a défini les obligations *erga omnes* comme des « *obligations des États envers la communauté internationale dans son ensemble, ayant pour objets des droits que tous les États ont un intérêt juridique à voir protégés* »[341]. Elle a ensuite dressé une liste d'exemples parmi lesquels figure « *la mise hors la loi des actes d'agression* »[342].

212. Par la suite, au cours de l'affaire des Activités militaires et paramilitaires au Nicaragua et contre celui-ci , la Cour, « *sans prendre elle-même position, constata que les deux parties au litige étaient d'accord pour qualifier la prohibition du recours à la force de règle de jus cogens* », c'est-à-dire de normes impératives définies par l'article 53 de la Convention de Vienne comme « *une norme acceptée et reconnue par la communauté internationale dans son ensemble en tant que norme à laquelle aucune dérogation n'est permise* ».

213. De plus, « *les États et organisations internationales affectés par la violation de la norme de jus cogens […] sont par définition tous les États et organisations internationales : l'obligation violée, étant impérative, présente un caractère erga omnes, c'est-à-dire que son respect est dû par chaque État membre de la communauté internationale à tous les autres* ». Or la prohibition de la guerre d'agression fait partie de ces normes impératives, reconnues comme étant *erga omnes*.[343]

214. Par conséquent, les cyberattaques étant des recours à la force constituant des agressions doivent ouvrir les mêmes possibilités pour toute la communauté internationale et doivent permettre à tous les États de pourvoir engager la responsabilité de l'État responsable.

---

[341] PERRIN DE BRICHAMBAUT Marc, DOBELLE Jean-François, COULEE Frédérique, « *Leçons de droit international public* », éditions Dalloz (2ème édition), 2011, p. 279
[342] *Ibid*.
[343] DUPUY Pierre-Marie et KERBRAT Yann, « *Droit International Public* », éditions Dalloz (13ème édition), 2016, p. 515

Paragraphe 2 : Une demande de réparation possible de l'État victime.

Dans ce paragraphe nous verrons la possibilité de l'État victime de demander réparation à l'État responsable, selon les modalités prévues par le droit international.

215. Une fois le F.I.I. ayant cessé, et la responsabilité de l'État responsable étant engagée, l'État victime devra être en mesure de demander réparation à l'État qui a initié la cyberattaque constituant une agression contre lui. En effet, les agressions sont susceptibles de donner lieu à une réparation puisque *« l'État responsable est tenu de réparer intégralement le préjudice causé par le F.I.I., le préjudice comprenant tout dommage tant matériel que moral, résultant du F.I.I. de l'État* »[344]. Ce principe a été consacré par la C.P.J.I. dans l'affaire de l'usine de Chorzów (Allemagne *c*. Pologne) du 13 septembre 1928 où la Cour a déclaré que « *le principe essentiel qui découle de la notion même d'acte illicite et qui semble se dégager de la pratique internationale, notamment de la jurisprudence des tribunaux arbitraux, est que la réparation doit, autant que possible, effacer toutes les conséquences de l'acte illicite et rétablir l'État qui aurait vraisemblablement existé si ledit acte n'avait pas été commis* »[345].

216. En ce qui concerne l'obligation de réparation en cas d'agression conventionnelle, deux exemples peuvent être cités. En effet, cette obligation de réparation a été reconnue par trois organes de l'O.N.U. Le Conseil de sécurité a participé à la réparation des dommages de l'agression de l'Irak contre le Koweït et ses conséquences, la C.I.J. s'est plusieurs fois prononcée au sujet de l'agression d'un État contre un autre État notamment dans l'affaire des Activités armées sur le territoire du Congo (République démocratique du Congo *c*. Ouganda). Les décisions de ces deux organes de l'O.N.U. sont d'ailleurs en adéquation avec le développement de la C.D.I. sur la réparation lors d'un F.I.I. de son projet d'articles sur la responsabilité de l'État pour fait internationalement illicite.

[344] C.D.I., « *Projet d'articles sur la responsabilité de l'État pour fait internationalement illicite* », Documents officiels de l'Assemblée générale, cinquante-sixième session, Supplément n° 10 (A/56/10), article 31
[345] DUPUY Pierre-Marie et KERBRAT Yann, « *Droit International Public* », éditions Dalloz (13ème édition), 2016, p. 550

217. En effet, l'Irak, à la suite de son agression contre le Koweït en 1990, s'est vu obligé de réparer les dommages qui lui ont été imputés. Après l'intervention de la Coalition habilitée par le Conseil de sécurité[346], ce dernier a décidé de mettre en place un système destiné à rétablir la paix, comprenant l'organisation de la réparation des dommages causés lors de cette agression ainsi que lors des opérations de la Coalition contre l'Irak dans sa résolution 687. Cette résolution, « *véritable monument juridique* »[347] a « *pour objet de mettre fin au conflit international résultant de l'occupation et de l'annexion du Koweït* »[348]. Dans cette résolution, le Conseil de sécurité retient une responsabilité très étendue de l'Irak qui, selon le paragraphe 16 de la résolution 687, « *doit réparer toute perte, tout dommage […] et tous les autres préjudices subis par des États étrangers et des personnes physiques et sociétés étrangères du fait de son invasion et de son occupation illicite du Koweït* »[349].

218. Une commission de compensation est créée afin d'assurer la réparation des dommages et considère que l'Irak doit « *réparer tous les dommages causés non seulement par ses propres agissements, mais également par les opérations de la Coalition* »[350]. La résolution 687 « *concentre ainsi ses foudres sur l'Irak* »[351].

219. La C.I.J. reconnaît elle-même qu'un État responsable d'une agression doit réparer les dommages qu'il a causés. Dans l'affaire des Activités armées sur le territoire du Congo (République démocratique du Congo *c*. Ouganda)[352], la Cour a estimé que la « *question de la réparation devant être réglée* (par elle) *s'il n'y a pas d'accords entre les parties, et déterminée par la Cour lors d'une phase ultérieure de la procédure* »[353], *« l'Ouganda devra effectuer une réparation en nature lorsque cela s'avère encore matériellement possible, en particulier en ce qui concerne les biens et les richesses, et*

---

[346] En ce sens *v*. Partie I, Chapitre 1, Section 1, Paragraphe 2 § 63
[347] SUR Serge, *« La résolution 687 (avril 1991) du Conseil de sécurité dans l'affaire du Golfe : problèmes de rétablissement et de garantie de la paix »*, Annuaire français de droit international, XXXVII – 1991, éditions du CNRS, p. 27
[348] *Ibid*.
[349] C.S. Résolution 687 du 3 avril 1991, S/22454, §16
[350] HINDAWI Coralie, « *D'une guerre à l'autre ou un retour sur les ambiguïtés de la résolution 687 (1991) du Conseil de sécurité* », Revues Etudes Internationales, Editions Erudit, volume 37, n°3, septembre 2006, p. 357-487
[351] SUR Serge, « *La résolution 687 (avril 1991) du Conseil de sécurité dans l'affaire du Golfe : problèmes de rétablissement et de garantie de la paix »*, Annuaire français de droit international, XXXVII – 1991, éditions du CNRS
[352] C.I.J. « *Activités armées sur le territoire du Congo* » (République démocratique du Congo *c.* Ouganda), arrêt, Recueil 2005, p. 168
[353] *Ibid*. p. 173

à défaut, de fournir une somme couvrant l'intégralité des dommages subis ainsi que d'accorder une satisfaction pour les outrages subis par la République démocratique du Congo »[354].

220. La Cour entérine donc tout à fait le projet d'articles sur la responsabilité de l'État pour fait internationalement illicite et ses articles sur la réparation, notamment en ce qui qui concerne ses modalités (restitution *in integrum*, indemnisation, satisfaction)[355]. Par conséquent, il apparaît qu'un État responsable d'un F.I.I., et plus précisément dans le cas d'une agression, est tenu de réparer les dommages causés.

221. Si les agressions conventionnelles entraînent la responsabilité de l'État responsable, et donc l'obligation de réparation de ce dernier, il semble donc naturel qu'une agression constituée par une cyberattaque similaire à un recours à la force entraîne l'obligation de réparation de l'État responsable, comme n'importe quelle agression, voire F.I.I.

222. L'État responsable devra réparer intégralement le préjudice causé par une telle cyberattaque. *« La réparation pourrait ainsi se faire par restitution, indemnisation et satisfaction, séparément ou conjointement* »[356]. La C.P.J.I. dans l'affaire de l'usine de Chorzów (Allemagne *c*. Pologne) a précisé à ce sujet que la « *restitution en nature ou si elle n'est pas possible, paiement d'une somme correspondant à la valeur qu'aurait la restitution en nature* »[357]. En ce qui concerne la restitution, celle-ci a pour but de revenir au *statu quo ante*. L'objectif visé est de pouvoir revenir à la situation préexistant le F.I.I.[358], c'est-à-dire de « *restaurer la situation de fait et de droit prévalant antérieurement en s'acquittant de certaines prestations matérielles* »[359]. Cette réparation *in integrum* est à favoriser autant que possible car elle est considérée comme

[354] C.I.J. « *Activités armées sur le territoire du Congo* » (République démocratique du Congo *c.* Ouganda), arrêt, Recueil 2005, p. 182
[355] En ce sens *v*. C.D.I., « *Projet d'articles sur la responsabilité de l'État pour fait internationalement illicite* », Documents officiels de l'Assemblée générale, cinquante-sixième session, Supplément n° 10 (A/56/10), article 34 à 39
[356] *Ibid*. article 34
[357] DUPUY Pierre-Marie et KERBRAT Yann, « *Droit International Public* », éditions Dalloz (13ème édition), 2016, p. 550
[358] C.D.I., « *Projet d'articles sur la responsabilité de l'État pour fait internationalement illicite* », Documents officiels de l'Assemblée générale, cinquante-sixième session, Supplément n° 10 (A/56/10), article 35
[359] DUPUY Pierre-Marie et KERBRAT Yann, « *Droit International Public* », éditions Dalloz (13ème édition), 2016, p. 551

la « *réparation parfaite* »[360], sauf si elle atteint deux limites rappelées à l'article 35 du projet d'articles de la C.D.I. sur la responsabilité de l'État pour fait internationalement illicite : « *le fait qu'elle ne soit pas matériellement possible, ou qu'elle impose une charge hors de toute proportion avec l'avantage qui dériverait de la restitution plutôt que de l'indemnisation* »[361].

223. De manière générale, en matière de cyberattaque, la restitution *in integrum* semble difficile à entériner. En effet, tout dépend de la cyberattaque subie par l'État-victime. Dans le cadre d'une cyberattaque telle que l'a connue l'Estonie, une restitution *in integrum* ne semble pas adéquate étant donné que les dommages ont été réalisés dans un espace-temps réduit, puis ont cessé[362]. La cyberattaque contre la Géorgie, quant à elle, a permis à l'armée russe de détruire des cibles stratégiques[363]. Les dommages sont donc aussi matériels et définitifs. Et dans l'affaire Stuxnet, la cyberattaque a permis l'introduction d'un vers dans les réseaux iraniens de la centrale de Natanz, qui a abouti à la destruction de centrifugeuses[364]. Toutes les cyberattaques n'entraînent donc pas les mêmes dommages et si, dans un premier temps, les dommages vont être dans le cyberespace et le domaine cybernétique de l'État victime, ils peuvent ensuite avoir des conséquences matérielles. La réparation *in integrum* n'est donc pas toujours possible notamment dans les cas où les dommages ont été temporaires et uniquement cybernétiques. Il faut donc apprécier les règles de la réparation au cas par cas, et lorsque la réparation *in integrum* n'est pas possible, ou qu'elle serait disproportionnée, il faut recourir à l'indemnisation.

224. L'indemnisation est une « *réparation par équivalent qui peut être quant à elle exigée chaque fois que la restitution en nature s'avère impossible ou qu'elle est préférée par l'État lésé* »[365]. La C.D.I. a précisé dans l'article 36 de son projet d'articles que

---

[360] DUPUY Pierre-Marie et KERBRAT Yann, « *Droit International Public* », éditions Dalloz (13ème édition), 2016, p. 552
[361] C.D.I., « *Projet d'articles sur la responsabilité de l'État pour fait internationalement illicite* », Documents officiels de l'Assemblée générale, cinquante-sixième session, Supplément n° 10 (A/56/10), article 35
[362] En ce sens *v.* Le Monde Europe, « *L'Estonie tire les leçons des cyberattaques massives lancées contre elle pendant la crise avec la Russie* », 27.06.2007
[363] LIMONIER Kévin et GERARD Colin, « *La guerre hybride russe dans le cyberespace* », éditions Hérodote, 2017, n°166-167, pp 145-163, § 9
[364] En ce sens *v.* MONGIN Dominique, « *Les cyberattaques, armes de guerres en temps de paix* », éditions Esprit, 01/2013, p. 32-49, § 8-9
[365] DUPUY Pierre-Marie et KERBRAT Yann, « *Droit International Public* », éditions Dalloz (13ème édition), 2016, p. 553

« *l'indemnité couvre tout dommage susceptible d'évaluation financière, y compris le manque à gagner dans la mesure où celui-ci est établi* »[366]. L'indemnisation apparaît comme la réparation la plus facile à mettre en pratique en matière de cyberattaque car elle « *n'est pas exclusivement réservée à l'indemnisation des dommages matériels* »[367]. En effet, l'indemnisation peut aussi couvrir « *la réparation d'un préjudice immatériel dit moral, ou juridique* »[368]. L'indemnisation permet donc une réparation pour tous les dommages causés à un État dès lors qu'ils peuvent être évalués financièrement, ce qui, au vu de la complexité et de la nouveauté des cyberattaques, peut sembler une bonne base pour la réparation des dommages causés par des cyberattaques constituant des agressions.

225. D'ailleurs, la réparation octroyée par les États responsables d'agressions aux États victimes donnent souvent lieu à une indemnisation, seule ou en complément d'une autre forme. Par exemple, l'Irak a été condamné à indemniser tous les dommages causés lors de son agression ainsi que tous ceux causés par la Coalition. En effet, l'Irak, pays agresseur du Koweït dont les actes avaient entraîné la réaction de la Coalition menée par les États-Unis après l'habilitation du Conseil de sécurité, a été « *contraint de payer sur les produits de son pétrole contrôlés par les Nations unies toutes les réparations de la guerre* »[369]. L'Irak a donc dû indemniser tous les États ayant subi des dommages à la suite de cette guerre, qu'ils aient été causés directement ou indirectement par lui[370].

226. Enfin, une dernière forme de réparation est possible lorsque les dommages ne peuvent être réparés ni en nature, ni par équivalent, au moyen de la satisfaction. La satisfaction est une forme de réparation permettant de réparer « *les préjudices moraux ou juridiques* »[371] quand ceux-ci ne peuvent pas donner lieu à une estimation financière, ou parfois en complément d'une réparation *in integrum* ou d'une indemnisation. Elle peut « *prendre des formes diverses, en particulier des excuses, le versement de*

[366] C.D.I., « *Projet d'articles sur la responsabilité de l'État pour fait internationalement illicite* », Documents officiels de l'Assemblée générale, cinquante-sixième session, Supplément n° 10 (A/56/10), article 36
[367] DUPUY Pierre-Marie et KERBRAT Yann, « *Droit International Public* », éditions Dalloz (13ème édition), 2016, p. 554
[368] *Ibid*. p. 555
[369] CHEMILLIER-GENDREAU Monique, Le Monde, « *Dommages de guerres à géométrie variable* », octobre 2003, p. 25
[370] C.S. résolution 687 S/22454, § 16
[371] DUPUY Pierre-Marie et KERBRAT Yann, « *Droit International Public* », éditions Dalloz (13ème édition), 2016, p. 555

dommages et intérêts symboliques, le châtiment de personnes responsables »[372] […] voire la reconnaissance de l'illicéité par une cour ou un tribunal international[373]. Une satisfaction ne doit toutefois pas être humiliante pour l'État responsable[374]. En matière de cyberattaque, la satisfaction peut également être une forme de réparation appréciée par les États notamment afin de réparer les préjudices subis par l'État victime qu'aucune autre réparation ne pourrait satisfaire. Le caractère insidieux des cyberattaques étant une de leurs grandes caractéristiques, la reconnaissance du F.I.I. de l'État responsable ou des excuses pour avoir mené la cyberattaque contre l'État victime pourraient être une forme de réparation.

227. Cette possibilité de réparation ne serait ouverte qu'à l'État victime ayant été directement lésé par la cyberattaque, les autres États, dits les États autres que l'État lésé, n'ayant qu'un intérêt à agir en vertu d'une obligation *erga omnes* ou *erga omnes partes* comme nous l'avons vu précédemment[375], ne pourront que demander la fin de l'illicéité voire des garanties de non-répétition. Ils ne peuvent toutefois pas demander de réparation car cela n'est pas un droit des États autres que l'État lésé : ils ne peuvent qu'exiger la réparation au profit de l'État lésé[376].

228. Ainsi, dès lors que les cyberattaques étant des recours à la force seront reconnues comme pouvant être des agressions, et donc des F.I.I., le droit international pourra les encadrer. En effet, il possède d'ores et déjà les moyens pour les États victimes de telles cyberattaques d'engager la responsabilité de l'État responsable afin de faire cesser le F.I.I. et d'obtenir réparation. Toutefois, étant donné que l'État victime ne subit pas n'importe quel F.I.I. mais une agression, se pose la question des mesures que peut prendre ce dernier pour mettre fin à cette agression au plus vite, avant d'engager la responsabilité de l'État responsable.

---

[372] DUPUY Pierre-Marie et KERBRAT Yann, « *Droit International Public* », éditions Dalloz (13ème édition), 2016, p. 555

[373] *Ibid*. p. 556

[374] En ce sens C.D.I., « *Projet d'articles sur la responsabilité de l'État pour fait internationalement illicite* », Documents officiels de l'Assemblée générale, cinquante-sixième session, Supplément n° 10 (A/56/10), article 37

[375] Partie II, Chapitre 1, Section 2, paragraphe 1, § 207-208

[376] En ce sens v. C.D.I., « *Projet d'articles sur la responsabilité de l'État pour fait internationalement illicite* », Documents officiels de l'Assemblée générale, cinquante-sixième session, Supplément n° 10 (A/56/10), article 48

Chapitre 2 : Deuxième conséquence : la possibilité de prendre des mesures en riposte à ces agressions cybernétiques.

Dans ce chapitre, nous allons étudier les mesures que l'État victime peut prendre face à une agression constituée par une cyberattaque, que ce soit les contre-mesures ou la légitime défense.

Section 1 : La possibilité de contre-mesures, voire de contre-mesures armées.

Au sein de cette section, nous aborderons la possibilité de l'État victime de prendre des contre-mesures face à une cyberattaque, voire des contre-mesures armées.

Paragraphe 1 : La prise de contre-mesures, un droit face à un fait internationalement illicite.

Dans ce paragraphe, il sera question du droit de prendre des contre-mesures face à une cyberattaque, étant donné que celle-ci est un fait internationalement illicite.

229. Une cyberattaque étant un recours à la force constituant une agression peut entraîner plusieurs réactions de la part de l'État victime. Ce type de cyberattaques étant des manquements aux obligations internationales d'un État, elles peuvent donner lieu à l'exercice du droit de recourir à des contre-mesures de la part de l'État victime.

230. Un État victime d'un F.I.I. est en droit de prendre des mesures afin de faire cesser au plus vite le F.I.I. S'ouvre donc à lui la possibilité de prendre des contre-mesures « *à l'encontre de l'État du fait internationalement illicite que pour amener cet État à s'acquitter des obligations qui lui incombent* »[377]. Le but de la contre-mesure est donc de dissuader l'État de poursuivre son F.I.I. voire de l'inciter à se remettre en conformité avec son obligation primaire.

[377] C.D.I., « *Projet d'articles sur la responsabilité de l'État pour fait internationalement illicite* », Documents officiels de l'Assemblée générale, cinquante-sixième session, Supplément n° 10 (A/56/10), article 49

231. Les contre-mesures sont des mesures décidées par les États agissant individuellement pour leur propre compte. Elles ont pour objet de permettre aux États lésés de défendre ou de rétablir leurs droits, et de faire pression sur l'État auteur du manquement pour qu'il se conforme au droit. Seul l'État « *créancier d'une obligation de réparer à qualité pour déclencher une contre-mesure* »[378] ce qui « *coïncide avec l'État lésé par le fait illicite* »[379]. Ce sont des sortes de mesures d'exécutions forcées. Il est nécessaire de bien différencier les contre-mesures de deux notions pouvant s'en approcher.

232. Les contre-mesures sont différentes des sanctions adoptées par le Conseil de sécurité. Des mesures peuvent être prises par le Conseil de sécurité en vertu du chapitre VII de la Charte des Nations unies[380] au nom de la paix et de la sécurité internationales. Décidées par le C.S, ces mesures s'inscrivent dans le système de sécurité collective de l'O.N.U. dont il est la *pierre angulaire*[381]. Les contre-mesures, elles, ne sont pas prises au sein de ce système de sécurité collective mais sont directement prises par les États, sans autorisation du Conseil de sécurité et en dehors du mécanisme de sécurité collective de la Charte des Nations unies, ce qui en fait, d'après Alexandre Sicilianos, des « *réactions décentralisées à l'illicite* »[382].

233. Il est ensuite nécessaire de différencier les contre-mesures des rétorsions. Les rétorsions sont des réactions licites des États face à des mesures illicites d'un autre État. Elles diffèrent donc des contre-mesures (aussi appelées des représailles), qui sont par nature illicites et qui ne deviennent licites que parce qu'elles répondent à des mesures illicites prises antérieurement par un autre État[383]. Cela permet ainsi de faire pression sur cet État afin qu'il cesse son comportement illicite. L'idée est donc qu'un État fasse respecter ses obligations internationales par un autre État en le dissuadant de violer ces dernières par la prise de contre-mesures.

---

[378] En ce sens *v*. RIVIER Raphaële, « *Droit International Public* », éditions Presses Universitaires de France, (2ème édition), 2012, p. 612
[379] *Ibid*.
[380] SIMONET Loïc, « *L'usage de la force dans le cyberespace et le droit international* », Annuaire de droit français international, 2012, 58, pp. 117-143, p. 130
[381] En ce sens *v*. COT Jean-Pierre, PELLET Alain, FORTEAU Mathias, « *La Charte des nations unies commentaire article par article* », éditions Economica (3ème édition), 2005, p. 1131
[382] En ce sens *v*. SICILIANOS Alexandre, « *Les réactions décentralisées à l'illicite : des contre-mesures à la légitime défense* », éditions LGDJ, 1990
[383] En ce sens *v*. RIVIER Raphaële, « *Droit International Public* », éditions Presses Universitaires de France, (2ème édition), 2012, p. 608

234. Lorsque les États prennent des contre-mesures, ils sont tenus de respecter certaines règles. Les contre-mesures doivent ainsi être réversibles[384] et doivent donc *« autant que possible être prises d'une manière qui permette la reprise des obligations de l'exécution en question »*[385] car elles doivent cesser dès lors que « *l'État responsable s'est acquitté de ses obligations* »[386]. De plus, les contre-mesures doivent respecter plusieurs principes dont le principe d'interdiction de recours à la force entre États, la protection des droits fondamentaux de l'Homme, le droit international humanitaire, les obligations découlant de normes impératives du droit international général[387], mais aussi des obligations procédurales telles qu'une obligation de demande de cessation de l'illicéité, une offre de négociation et une notification de prise de contre-mesure, sauf en cas d'urgence[388]. Enfin, les États doivent toujours respecter le principe de proportionnalité lorsqu'ils prennent des contre-mesures, comme la C.I.J. l'a rappelé dans l'affaire du barrage de Gabcikovo-Nagymaros [389].

235. Les États peuvent donc prendre des contre-mesures contre d'autres États ne respectant pas leurs obligations internationales dès lors qu'ils sont lésés par ce manquement. Or, une cyberattaque étant un recours à la force constituant une agression, viole deux obligations internationales.

236. Tout d'abord un tel acte est, comme toute cyberattaque, une violation du principe de non-intervention qui interdit à tout État d'intervenir dans les affaires intérieures d'un autre État.[390] Le système des Nations unies a consacré ce principe que violent les cyberattaques en son article 2 paragraphe 7 en précisant qu' « *aucune disposition de la présente Charte n'autorise les Nations unies à intervenir dans des affaires qui relèvent essentiellement de la compétence nationale d'un État* »[391].

---

[384] En ce sens *v*. RIVIER Raphaële, *« Droit International Public »*, éditions Presses Universitaires de France, (2ème édition), 2012, p. 608
[385] C.D.I., « *Projet d'articles sur la responsabilité de l'État pour fait internationalement illicite* », Documents officiels de l'Assemblée générale, cinquante-sixième session, Supplément n° 10 (A/56/10), article 49
[386] En ce sens *v*. RIVIER Raphaële, « *Droit International Public »*, éditions Presses Universitaires de France, (2ème édition), 2012, p. 610
[387] C.D.I., « *Projet d'articles sur la responsabilité de l'État pour fait internationalement illicite* », Documents officiels de l'Assemblée générale, cinquante-sixième session, Supplément n° 10 (A/56/10), article 50
[388] *Ibid*. article 52
[389] En ce sens *v*. SIMONET Loïc, « *L'usage de la force dans le cyberespace et le droit international* », Annuaire de droit français international, 2012, 58, pp. 117-143, p. 129
[390] En ce sens *v*. DAILLIER Patrick, FORTEAU Mathias, PELLET Alain, « *Droit International Public* », LGDJ Lextenso éditions (8è éditions) 2009, p. 486
[391] Charte des Nations Unies article 2 § 7

237. La C.I.J. a également consacré ce principe de non-ingérence et a condamné de telles interventions au nom dudit principe et du principe de souveraineté dans l'affaire du Détroit de Corfou en considérant que « *le prétendu droit d'intervention ne peut être envisagé par elle [la Cour] que comme une manifestation politique de force, politique qui a dans le passé donné lieu aux abus les plus graves et qui ne saurait, quelles que soient les déficiences présentes de l'organisation internationale, trouver aucune place dans le droit international* »[392].

238. La Cour a ensuite précisé dans l'affaire des Activités militaires et paramilitaires au Nicaragua et contre celui-ci que « *ce principe interdit à tout État ou groupe d'États d'intervenir directement ou indirectement dans les affaires intérieures ou extérieures d'un autre État. L'intervention interdite doit donc porter sur des matières à propos desquelles le principe de souveraineté des États permet à chacun d'entre eux de se décider librement. Il en est ainsi du choix du système politique, économique, social et culturel et de la formulation des relations extérieures. L'intervention est illicite lorsqu'à propos de ces choix qui doivent demeurer libres, elle utilise des moyens de contraintes* »[393].

239. Cela signifie par conséquent qu'une violation du principe de non-intervention doit avoir un élément essentiel tout à fait présent dans les cyberattaques : la contrainte[394]. Les cyberattaques permettent en effet d'exercer des pressions et des contraintes sur un État en prenant le contrôle de son réseau afin de le bloquer, le désactiver ou le détruire. Cela permet ainsi, au mieux, de faire peser une pression sur l'État, comme cela a été le cas lors des cyberattaques contre l'Estonie dans une période de tensions entre la Russie et l'Estonie ; mais cela peut également permettre des interventions dans le choix du système politique.

240. En effet, les cyberattaques sont aujourd'hui utilisées pour intervenir dans les affaires politiques d'un État. Cela est notamment le cas de la Russie qui est accusée par

---

[392] C.I.J. « *Affaire du Détroit de Corfou* », arrêt du 9 avril 1949 : C.I.J. Recueil 1949, p. 35 *in* DAILLIER Patrick, FORTEAU Mathias, PELLET Alain, « *Droit International Public* », LGDJ Lextenso éditions (8è éditions) 2009, p. 486

[393] C.I.J. « *Affaire des Activités militaires et paramilitaires au Nicaragua et contre celui-ci* » du 27 juin 1986 (Nicaragua *c.* États-Unis d'Amérique), fond, arrêt, Recueil 1986, p. 108 *in* DAILLIER Patrick, FORTEAU Mathias, PELLET Alain, « *Droit International Public* », LGDJ Lextenso éditions (8è éditions) 2009, p. 486

[394] En ce sens *v.* DAILLIER Patrick, FORTEAU Mathias, PELLET Alain, « *Droit International Public* », LGDJ Lextenso éditions (8è éditions) 2009, p. 488

plusieurs pays de s'ingérer dans leurs affaires intérieures et notamment dans leurs vie et élections politiques. Les États-Unis, par exemple, considèrent que la Russie, *via* des cyberattaques dans le but d'acquérir des informations et autres opérations, a réalisé une « *ingérence russe sur les réseaux sociaux et par le piratage d'informations* »[395] en piratant lors des présidentielles américaines de 2016 « *19 952 e-mails et 8 034 pièces jointes issus des serveurs du Comité national du parti démocrate (DNC) »*[396] grâce au groupe de hackers « *connu pour ses opérations ciblant en priorité des organisation ou des États hostiles à la Russie baptisé Advanced persitent threat n°28 ou APT28* »[397].

241. Les cyberattaques sont donc de plus en plus utilisées comme des ingérences dans les affaires intérieures. Cela explique qu'elles soient perçues, et souvent dénoncées, comme telles[398]. Les cyberattaques sont donc bien une violation du principe de non-intervention consacré en droit international comme la « *conséquence nécessaire et directe des deux piliers du droit des relations internationales, le principe de souveraineté et celui de l'égalité des États qui en est l'indissociable conséquence* »[399]. Le recours à des cyberattaques constitue donc bien un manquement à l'obligation internationale de s'abstenir d'intervenir dans les affaires intérieures d'un autre État, ce qui fonde la possibilité de l'État victime de prendre des contre-mesures.

242. Mais plus particulièrement, les cyberattaques étant des recours à la force violent non-seulement ce principe de non-intervention, mais aussi le principe de non-recours à la force puisqu'elles sont, comme nous l'avons vu précédemment, un nouveau moyen pour les États d'atteindre des objectifs qui seraient considérés comme des actes d'agression s'ils étaient réalisés par des moyens conventionnels.[400]

243. Ces cyberattaques peuvent également porter atteinte au principe de règlement pacifique des différends. En effet, les États se doivent de régler leurs différends par des moyens non-juridictionnels ou juridictionnels mais ne peuvent en aucun cas avoir

---

[395] Le Monde, « *États-Unis : la justice poursuite treize Russes pour ingérence dans l'élection présidentielle de 2016* », 16.02.2018 http://www.lemonde.fr/ameriques/article/2018/02/16/États-unis-la-justice-poursuit-treize-Russes-pour-ingerence-dans-l-election-presidentielle-de-2016_5258249_3222.html

[396] LIMONIER Kévin et GERARD Colin, « *La guerre hybride russe dans le cyberespace* », éditions Hérodote, 2017, n°166-167, pp 145-163, § 1

[397] *Ibid*. § 4

[398] En ce sens *v*. Le Monde, *« Washington annonce des sanctions contre Moscou pour son ingérence dans la présidentielle* », 15.03.2018

[399] DAILLIER Patrick, FORTEAU Mathias, PELLET Alain, « *Droit International Public* », LGDJ Lextenso éditions (8è éditions) 2009, p. 487

[400] Partie I, Chapitre 2, Section 2, Paragraphe 2, § 153

recours à la force[401] car cela contreviendrait à l' « *interdiction de régler les différends par des moyens non pacifiques, […] un corollaire ou un élément de principe de droit international général constitué sur la base de l'article 2 paragraphe 4 de la C.N.U.* »[402]. Par conséquent, si de telles cyberattaques exerçant une contrainte par la force ou étant un recours à la force sont prises lors d'un différend opposant l'État responsable à l'État victime, et ce afin de lui imposer ses vues dans la résolution du différend, cela peut également constituer une violation du principe de résolution pacifique des différends. Ce manquement aux obligations internationales de l'État pourrait donc, lui-aussi, donner lieu à des contre-mesures de la part de l'État victime.

244. Enfin, ces cyberattaques doivent être des violations d'obligations internationales conventionnelles. En effet, les États se doivent de développer des outils d'encadrement des cyberattaques afin d'éviter que le recours à de telles pratiques permette de contourner le droit international. Ce virage s'amorce déjà avec des cyberattaques à l'appui d'opérations militaires conventionnelles qui appelle un régime juridique spécifique répondant à un « *besoin de normativité spécifique, propre* »[403]. Ces nouvelles obligations internationales devront permettre d'interdire une instrumentalisation illicite des cyberattaques dans le but de contourner ou de violer le droit international, et notamment les principes de non-intervention et de non-recours à la force garanti par la Charte des Nations unies[404], principes fondamentaux pour le maintien de la paix et de la sécurité internationales.

245. Les cyberattaques peuvent violer des principes du droit international et sont donc bien des manquements à des obligations internationales. Elles sont bien des F.I.I. lésant les États qu'elles visent et doivent être considérées comme telles dans les futurs éventuels régimes juridiques spécifiques aux cyberattaques. *De facto*, les États victimes doivent effectivement avoir la possibilité de prendre des contre-mesures face à ces F.I.I. Toutefois, les cyberattaques étant des recours à la force ne sont pas que de simples manquements aux obligations internationales des États, mais violent tout de même le

[401] En ce sens v. *COMBACAU* Jean, SUR Serge, « *Droit International Public* », LGDJ Lextenso éditions (8ème édition), 2014 p. 560
[402] *Ibid*. p. 561
[403] BORIES Clémentine, « *Appréhender la cyberguerre en droit international, Quelques réflexions et mises au point* », La Revue des Droits de l'Homme, éditions Revue du centre de recherche et d'études sur les droits fondamentaux, 6.2014, § 13
[404] Charte des Nations unies, article 2, § 7 et 4

principe d'interdiction de recours à la force. Leurs réalisations par l'État responsable ne devraient-elles donc pas exceptionnellement permettre de recourir aux contre-mesures armées ?

Paragraphe 2 : La prise de contre-mesure armée, une conséquence possible ?

Dans ce paragraphe, nous aborderons la question de la possibilité et de l'intérêt d'autoriser exceptionnellement l'État victime à prendre des mesures de représailles face à une cyberattaque.

246. Si les cyberattaques étatiques, étant des recours à la force constituant des agressions, sont des manquements aux obligations internationales d'un État, elles ne violent pas n'importe quelles obligations internationales. En effet, ces cyberattaques violent le principe d'interdiction de recours à la force entre États. Dès lors, si les États victimes peuvent prendre des contre-mesures, il est légitime de se demander jusqu'où peuvent-ils aller ? Se pose donc la question de l'autorisation de recourir ou non à des contre-mesures armées en réponse à des cyberattaques.

247. Les contre-mesures armées, également nommées représailles, sont « *des actes de contraintes militaires contraires au droit international mis en œuvre pour répondre au comportement d'un autre État lui-même contraire au droit international* »[405]. Elles sont interdites dans le cadre de l'O.N.U. car elles sont contraires au mécanisme centralisé de sécurité collective dont le Conseil de sécurité est garant. L'interdiction des contre-mesures armées est ancienne. En effet, en 1928, l'Allemagne avait déjà été condamné dans l'affaire du Fort Naulilaa[406] pour avoir pris des contre-mesures armées contre le Portugal, ce qui avait été jugé disproportionné.

248. Par la suite, l'O.N.U. a estimé que les contre-mesures armées étaient interdites. L'article 50 du projet d'article de la C.D.I. précise que les contre-mesures doivent

[405] DAILLIER Patrick, FORTEAU Mathias, PELLET Alain, « *Droit International Public* », LGDJ Lextenso éditions (8è éditions) 2009, p. 1047

[406] En ce sens *v.* « *Sentence arbitrale du 31 juillet 1928 concernant la responsabilité de l'Allemagne à raison des dommages causés dans les colonies portugaises du Sud de l'Afrique* » (Portugal contre Allemagne), sentence arbitrale, recueil des sentences arbitrales, VOLUME II pp. 1011-1033

respecter l'interdiction du recours à la force de l'article 2 paragraphe 4[407]. Dès lors, cela interdit tout recours à la force en dehors la légitime défense et de l'autorisation du Conseil de sécurité[408].

249. Dans l'affaire des Activités militaires et paramilitaires au Nicaragua et contre celui-ci de 1986, la C.I.J. elle-même a estimé que les représailles non-militaires sont autorisées, les États ne devant s'abstenir que « *d'actes de représailles impliquant la force* »[409]. Cela induit que les représailles militaires, elles, ne sont pas autorisées. La C.I.J. a ensuite continué sur sa lancée en précisant qu'une réaction armée face un F.I.I. qui n'est pas constitutif d'une agression n'est pas justifiable, et que l'interdiction de non-recours à la force est un principe de *jus cogens*[410]. Les contre-mesures armées (ou représailles) sont donc interdites dans le cadre de l'O.N.U.

250. Pour autant, devant la particularité des cyberattaques étant des recours à la force, se pose la question de la possibilité (exceptionnelle) pour l'État victime de recourir à des représailles. En effet, si les contre-mesures armées sont considérées comme tout à fait illicites, ceci aurait pour conséquence qu'il n'y aurait donc que deux catégories : d'une part, les recours à la force armée autorisés et licites, et d'autre part les recours à la force illicites[411]. Toutefois, certains auteurs estiment que les contre-mesures armées devraient être autorisées dans certains cas, notamment en vertu du principe de proportionnalité.

251. En effet, pour Alexandre Sicilianos, les contre-mesures doivent toujours être proportionnées avec le F.I.I. dont est victime l'État et de ce fait, lors de violations graves d'un État, des contre-mesures armées peuvent se justifier à la condition qu'elles soient proportionnées[412]. Par conséquent, si une contre-mesure doit toujours être proportionnée aux dommages subis par l'État, alors un État victime d'une cyberattaque étant un recours à la force avec de graves conséquences pourrait avoir pour réponse

---

[407] En ce sens v. C.D.I., « *Projet d'articles sur la responsabilité de l'État pour fait internationalement illicite* », Documents officiels de l'Assemblée générale, cinquante-sixième session, Supplément n° 10 (A/56/10), article 50
[408] En ce sens *v.* [408] DAILLIER Patrick, FORTEAU Mathias, PELLET Alain, « *Droit International Public* », LGDJ Lextenso éditions (8è éditions) 2009, p. 1048
[409] C.I.J. « *Affaire des Activités militaires et paramilitaires au Nicaragua et contre celui-ci* » du 27 juin 1986 (Nicaragua *c.* États-Unis d'Amérique), fond, arrêt, Recueil 1986, § 190-191
[410] *Ibid*.
[411] En ce sens *v.* Waxman, Matthew C., « *Regulating Resort to Force: Form and Substance of the UN Charter Regime* » (September 21, 2012). European Journal of International Law, Vol. 24, 2013.
[412] SICILIANOS Alexandre, « *Les réactions décentralisées à l'illicite : des contre-mesures à la légitime défense* », éditions LGDJ, 1990

proportionnelle la prise de contre-mesures armées. Cela pourrait, par exemple, se traduire par le bombardement du bâtiment source des cyberattaques, d'où a été initiée la cyberattaque, ou des antennes-relais permettant cette dernière.

252. Ce constat est d'autant plus probant que, malgré cette interdiction des contre-mesures armées, celles-ci sont régulièrement utilisées par les États et demeurent « *une pratique fréquente dans les relations internationales* »[413]. En effet, la pratique étatique est truffée de représailles d'États contre d'autres États responsables de violations de leurs obligations internationales. Les États prenant de telles mesures invoquent parfois d'autres fondements juridiques pour justifier leurs représailles ; mais cela ne fait qu'illusion car ce sont véritablement des interventions armées « *qui ne se rattachent pas à la légitime défense* »[414]. Sont ainsi visées « *pour l'essentiel, des interventions unilatérales dans les guerres civiles, des interventions pour protéger un droit et des interventions visant à assurer la sauvegarde de particuliers* »[415].

253. A titre d'exemple, en ce qui concerne l'utilisation des représailles armées par les États face à des recours à la force illicites, citons la guerre du Kosovo. En 1999, la Serbie attaque massivement la région autonome du Kosovo. Face à ce comportement illicite (violation du droit international général, du droit international humanitaire et du droit international des droits de l'Homme), l'OTAN lance une campagne aérienne contre la Serbie et bombarde les forces serbes sans attendre d'autorisation préalable du Conseil de sécurité. De même, le 6 avril 2017, à la suite d'une attaque avec des armes chimiques en Syrie attribuée au gouvernement de Bachar Al-Assad, les États-Unis bombardent une base aérienne syrienne (lieu supposé de départ de l'attaque) sans autorisation préalable non plus du Conseil de sécurité.

254. Ces deux exemples démontrent ainsi le recours à des représailles par des États face aux manquements d'un autre État à ses obligations internationales lors d'un recours à la force. Si les contre-mesures armées sont interdites pour les autres violations du droit international mais sont tout de même utilisées par les États dans certaines circonstances, ne faudrait-il pas les autoriser pour les cyberattaques au vu de leurs spécificités ?

---

[413] DAILLIER Patrick, FORTEAU Mathias, PELLET Alain, « *Droit International Public* », LGDJ Lextenso éditions (8è éditions) 2009, p. 1047
[414] *Ibid*. p. 1046
[415] *Ibid*.

255. Il conviendrait d'envisager l'autorisation exceptionnelle de contre-mesures armées, limitée à la simple recherche de sa cessation de la cyberattaque étant un recours à la force. En effet, bien que la « *question de la licéité des interventions armées unilatérales des États pour la défense d'un droit est délicate […], l'argument de la défense du droit pour justifier des interventions armées proches de l'agression caractérisée* »[416] étant souvent soulevée, il est également argué qu' « *a priori, une action pour assurer le respect du droit ne serait pas illicite au regard de la Charte* »[417]. Dès lors, des représailles dans le but de mettre fin à une violation de l'interdiction du recours à la force entre États de l'article 2 paragraphe 4 de la Charte des Nations unies, transgressée par le biais d'une cyberattaque, ne deviendrait-elle pas non seulement licite, mais également tout à fait proportionnelle ?

256. Cette question se pose étant donné que les cyberattaques ne sont pas que de simples interventions dans les affaires intérieures de l'État. Si, habituellement, une intervention dans les affaires intérieures de l'État est constituée d'actions directes ou indirectes contre celui-ci telles que « *la subversion, le recrutement, l'envoi de mercenaires, ou la menace du refus d'assistance au développement économique* »[418], mais qui ne requiert par l'usage de la force. Les cyberattaques, elles, obéissent à une logique différente lorsqu'elles sont utilisées comme des recours à la force.

257. Les cyberattaques peuvent certes permettre de s'ingérer dans les affaires politiques d'un État en ne constituant qu'une simple intervention. En effet, « *l'explosion des cyberaffrontements* »[419] se produit à « *un niveau que la loi et la diplomatie considèrent comme inférieur à une attaque armée ou à l'usage de la force, allant du vol de secrets industriels et militaires à la déstabilisation des systèmes informatiques d'institutions financières ou de grandes entreprises* »[420]. Mais les cyberattaques peuvent également être de véritables recours à la force directe contre les États, source de contraintes voire de dégâts contre les États, comme cela a déjà été le cas en Estonie avec la cyberattaque massive destinée à paralyser le pays afin de le contraindre à agir de telle

[416] DAILLIER Patrick, FORTEAU Mathias, PELLET Alain, « *Droit International Public* », LGDJ Lextenso éditions (8è éditions) 2009, p. 1046
[417] *Ibid*.
[418] A.G.N.U., « *Déclaration sur l'inadmissibilité de l'intervention dans les affaires intérieures des États et la protection de leur indépendance et de leur souveraineté* », Résolution 2131 du 21 décembre 1965
[419] KELLO Lucas, « *Les cyberarmes : dilemmes et futurs possibles* », éditions Institut français des relations internationales (IFRI), 2014/4 (Hiver), p. 139-150
[420] *Ibid*.

ou telle manière selon une véritable stratégie de « *Realpolitik appuyée* »[421], ou encore lors de la destruction de centrifugeuses iraniennes du complexe nucléaire de Natanz par le virus Stuxnet[422].

258. L'intérêt de la reconnaissance d'une telle possibilité pour les États victimes est donc de permettre leur réaction en cas de cyberattaques étant des recours à la force mais non reconnues, ou pas encore, comme des agressions. En effet, la légitime défense n'est possible que « *dans le cas où un Membre des Nations unies est l'objet d'une agression armée* »[423]. Or, si d'aventure, une cyberattaque étant un recours à la force n'était pas reconnue comme telle, ou tardait à être qualifiée d'agression, la possibilité d'exercer des représailles proportionnées se limitant à mettre fin à la cyberattaque permettrait aux États de recourir, dans une moindre mesure que dans un cas de légitime défense, à une action militaire.

259. Un autre intérêt peut résider à reconnaître la possibilité pour les États victimes de recourir à des représailles contre un État responsable d'une cyberattaque : cela pourrait également remplir un rôle de dissuasion. En effet, « *les opérations sur les réseaux informatiques étant difficiles à contrecarrer […] pour dissuader les attaquants, les cibles potentielles ont donc tenté d'affirmer qu'elles sont prêtes à répondre à une cyberattaque par la force, y compris par des représailles militaires conventionnelles* »[424]. Or, le rôle de la dissuasion des cyberattaques dans le but de les prévenir au lieu de devoir réagir face à celles-ci est d'importance étant donné qu'en matière de cyberattaque *« il n'y a pas d'accord sur les seuils définissant une attaque armée ou l'usage de la force dans ce nouveau domaine et encore moins sur le niveau de proportionnalité d'une réponse en cas de cyberattaque* »[425] et il est donc difficile de parvenir à exactement *« définir ce que serait une réponse proportionnée* »[426] à une cyberattaque.

---

[421] Le Monde Europe, « *L'Estonie tire les leçons des cyberattaques massives lancées contre elle pendant la crise avec la Russie* », 27.06.2007
[422] En ce sens *v.* Le Monde, « *Les risques de cyberattaques contre les centrales nucléaires se multiplient* », 06.10.2015.
[423] Charte des Nations unies, article 51
[424] KELLO Lucas, « *Les cyberarmes : dilemmes et futurs possibles* », éditions Institut français des relations internationales (IFRI), 2014/4 (Hiver), p. 139-150
[425] *Ibid*.
[426] *Ibid*.

260. Cette fonction dissuasive de la reconnaissance des représailles face à une cyberattaque est d'autant plus importante que les autres moyens de dissuasion sont inefficaces. En effet, la dissuasion par déni, qui « *fonctionne en réduisant l'efficacité des armes de l'adversaire* »[427] comme cela est le cas en matière nucléaire en développant « *un glacis défensif pouvant neutraliser les missiles ennemis en vol* »[428] ou en réduisant mutuellement « *les forces stratégiques à un niveau si bas que les compétiteurs peuvent se protéger même contre les armes atteignant leurs cibles* »[429], n'est pas aisé en matière de cyberattaque. En effet, beaucoup trop de contraintes techniques allant de « *l'abondance des vecteurs d'accès que l'assaillant peut employer* »[430], à « *la difficulté à détecter la simple présence d'une telle arme même après sa pénétration dans le système logique d'un ordinateur* »[431] ou encore de « *l'impossibilité d'atténuer le plein effet d'une cyberattaque empêche de la bloquer au moyen de la redondance ou de la résilience* »[432], tous ces facteurs rendent cette dissuasion par déni extrêmement difficile, voire impossible.

261. C'est pourquoi les États eux-mêmes cherchent à « *dissuader les cyberattaques par des représailles* »[433] comme une sanction qui « *est au fond un mécanisme psychologique* »[434]. Il est d'ailleurs estimé que n'autoriser que des représailles limitées « *serait moins dissuasif* »[435]. Bien que des représailles ne soient pas toujours possibles notamment en raison de la difficulté actuelle de localiser la provenance des cyberattaques[436], la reconnaissance de la possibilité de recourir à des contre-mesures armées de l'État victime permettrait peut être de dissuader les autres États de réaliser des cyberattaques contre lui. Pour le moment, cela se limiterait à de la dissuasion dans le cas où il parviendrait à identifier leur provenance. Mais cette fonction dissuasive des représailles armées serait aussi efficace dans l'avenir, au vu du développement actuel

[427] KELLO Lucas, « *Les cyberarmes : dilemmes et futurs possibles* », éditions Institut français des relations internationales (IFRI), 2014/4 (Hiver), p. 139-150
[428] *Ibid*.
[429] *Ibid*.
[430] *Ibid*.
[431] *Ibid*.
[432] *Ibid*.
[433] *Ibid*.
[434] *Ibid*.
[435] En ce sens *v*. DOUZET Frédéric, « *La géopolitique pour comprendre le cyberespace* », éditions Hérodote, 2014, n°152-153, pp. 3-21, § 39
[436] KELLO Lucas, « *Les cyberarmes : dilemmes et futurs possibles* », éditions Institut français des relations internationales (IFRI), 2014/4 (Hiver), p. 139-150

de virus destiné à tracer les cyberattaques tel l'antivirus de traçage en cours de développement au Japon[437]. Cette technique de dissuasion pourrait également fonctionner étant donné que « *plus une cyberattaque est sophistiquée, plus il est facile d'identifier sa source. Les attaques les plus puissantes -en particulier celles qui ont des effets destructeurs directs – requièrent une longue préparation et d'énormes ressources, ce qui réduit le nombre de ceux qui peuvent lancer une cyberattaque cataclysmique* »[438].

262. La dissuasion contre le recours à des cyberattaques étant des recours à la force, par le droit de recourir aux représailles, peut véritablement avoir des résultats car, dès lors que les États savent que l'exercice de représailles par l'État victime est possible, « *le risque d'une attaque à fort impact diminue, tandis que celui d'une agression plus légère augmente* »[439]. Comme le constate Lucas KELLO, « *la rareté des cyberattaques majeures et la croissance exponentielle de celles de moindre ampleur attestent de ce paradoxe* »[440].

263. La reconnaissance du droit de recourir aux contre-mesures armées pourrait donc bel et bien permettre une réaction de l'État victime dans le but faire cesser la cyberattaque, mais cela pourrait également dissuader les États de recourir à des cyberattaques étant des recours à la force étant donné que « *la crainte des représailles peut inciter les compétiteurs les plus redoutables (États-Unis, Russie, Chine etc.) à ne pas exploiter les failles de la défense pour un effet destructeur maximal* »[441]. Cela éviterait donc que les États contournent l'interdiction du recours à la force et commettent des agressions à travers l'utilisation de cyberattaques. Toutefois, il est évident qu'une telle autorisation serait à encadrer, cette prise de position des États n'étant pas sans risque et pouvant avoir « *pour effet de faire escalader rapidement une crise en cas d'échec de la dissuasion* »[442]. Etant donné que cela pourrait donc, en cas d'échec de la dissuasion, contribuer à la survenance d'un conflit, le « *risque d'escalade*

[437] BAUD Michel, « *La cyberguerre n'aura pas lieu, mais il faut s'y préparer* », Revue de l'institut français des relations internationales, Politique étrangère, volume 77, été 2012, p. 305 à 314 *in* BAUDIN Laura, « *Les cyberattaques dans les conflits armées* », éditions L'Harmattan, 2014, p. 41
[438] *Ibid*.
[439] *Ibid*.
[440] *Ibid*.
[441] *Ibid*.
[442] *Ibid*.

est donc à prendre au sérieux »[443]. Il faut cependant noter que « *les compétitions traditionnelles entre États sont modérées et régulées par un intérêt commun à la survie ainsi que par des procédures établies qui permettent souvent d'éviter l'escalade* »[444].

264. Les États victimes d'une cyberattaque étant un recours à la force peuvent donc prendre des contre-mesures contre les États responsables. Il serait également souhaitable que, de manière exceptionnelle, ils puissent avoir recours aux contre-mesures armées pour, d'une part, mettre fin à la cyberattaque dont ils sont victimes, et d'autre part, contribuer à la prévention et à la dissuasion du recours aux cyberattaques étatiques. Toutefois, dans le cas de cyberattaques étant un recours à la force constituant une agression, les États victimes d'une cyberattaque peuvent aussi invoquer leur droit à la légitime défense.

Section 2 : La possibilité de recourir au droit à la légitime défense des États.

Dans cette section, nous aborderons la possibilité pour l'État victime et ses alliés de recourir à la légitime défense face à une agression constituée par une cyberattaque.

Paragraphe 1 : L'exigence de répondre à une agression armée pour tout exercice de la légitime défense.

Dans ce paragraphe, il sera question de l'ouverture du droit à la légitime défense face à une cyberattaque constituant une agression, ouverture nécessitant comme condition *sine qua non* que cela soit en réponse à une agression armée.

265. En matière de cyberattaque étant des recours à la force constituant une agression, il est nécessaire d'analyser la possibilité des États de recourir à la légitime défense. En effet, cela requiert *de facto* la condition *sine qua non* que doit remplir tout exercice du droit à la légitime défense : le fait de répondre à une agression armée[445]. L'État qui

[443] En ce sens *v*. DOUZET Frédéric, « *La géopolitique pour comprendre le cyberespace* », éditions Hérodote, 2014, n°152-153, pp. 33-21, § 40
[444] *Ibid*.
[445] Charte des Nations unies, article 51

souhaiterait « *recourir à la légitime défense pour riposter face à une cyberattaque devra donc d'abord prouver qu'il faisait légitimement face à une agression armée* »[446].

266. Si le système des Nations unies prohibe « *la menace ou l'emploi de la force … de toute autre manière incompatible avec les buts des Nations unies* »[447], la légitime défense est une des deux possibilités de recours à la force autorisée par la C.N.U., la seconde possibilité étant les recours à la force autorisés au préalable par le C.S. La Charte des Nations unies consacre la légitime défense en son article 51 comme un « *droit naturel de légitime défense, individuelle et collective dans le cas où un membre des Nations unies est victime d'une agression armée* »[448]. La C.I.J. elle-même a reconnu le fondement conventionnel, mais aussi coutumier, reconnu par la C.N.U. avec l'expression « *droit naturel* »[449] en son arrêt des Activités militaires et paramilitaires au Nicaragua et contre celui-ci de 1986[450] en précisant que « selon *le libellé de l'article 51 de la Charte des Nations unies, le droit naturel (ou droit inhérent) que tout État possède dans l'éventualité d'une agression armée s'entend de la légitime défense, aussi bien collective qu'individuelle* »[451].

267. La légitime défense individuelle doit toutefois remplir plusieurs conditions. Tout d'abord, la légitime défense n'est possible que si l'État est victime d'une agression armée[452]. En effet, « *seule l'agression armée – et non toute contrainte – justifie le recours à la force au titre de la légitime défense* »[453], une agression étant considérée comme « *l'emploi de la force armée par un État contre la souveraineté, l'intégrité territoriale ou l'indépendance politique d'un État, ou de toute autre manière incompatible avec la Charte des Nations unies* »[454]. Toutefois, il faut noter que cette

[446] LOUIS-SIDNEY Barbara, « *La dimension juridique du cyberespace* », éditions revue internationale et stratégique, 2012/3 (n°87), p. 73-82, § 13
[447] DAILLIER Patrick, FORTEAU Mathias, PELLET Alain, « *Droit International Public* », LGDJ Lextenso éditions (8è éditions) 2009, p. 1037
[448] Charte des Nations unies, article 51
[449] DAILLIER Patrick, FORTEAU Mathias, PELLET Alain, « *Droit International Public* », LGDJ Lextenso éditions (8è éditions) 2009, p. 1038
[450] *Ibid*. p. 1039
[451] C.I.J. « *Affaire des Activités militaires et paramilitaires au Nicaragua et contre celui-ci* » du 27 juin 1986 (Nicaragua *c.* États-Unis d'Amérique), fond, arrêt, Recueil 1986, § 193
[452] Charte des Nations unies, article 51
[453] DAILLIER Patrick, FORTEAU Mathias, PELLET Alain, « *Droit International Public* », LGDJ Lextenso éditions (8ème édition) 2009, p. 1039
[454] A.G.N.U résolution A/RES/3314 (XXIX), article 1er

définition ne « *concerne que l'agression armée* »[455] au sens de la Charte des Nations unies et de son article 51 et non la simple agression au sens du droit coutumier. Cela sous-entend donc que tout recours à la force, qu'il soit dû à une cyberattaque ou à une attaque cinétique, peut être une agression, mais n'est pas obligatoirement une agression armée. En effet, la notion d'agression armée de l'article 51 de la C.N.U. « *est beaucoup plus restreinte que celle d'agression de l'article 39 de la C.N.U. […] un acte d'agression armée est une agression, mais la proposition inverse n'est pas toujours vrai*e »[456].

268. La C.I.J. a insisté sur ce critère d'agression armée dans son arrêt lors de l'affaire des Activités militaires et paramilitaires au Nicaragua et contre celui-ci en estimant que « *ce droit ne peut être exercé que si l'État intéressé a été victime d'une agression armée* »[457]. Toutefois, il est nécessaire de préciser que la Cour est restée « *floue s'agissant du seuil de gravité pour qu'un recours à la force puisse être qualifié d'acte d'agression* »[458].

269. La notion d'agression armée implique « *à l'instar de celle d'emploi de la force prévue à l'article 2 paragraphe 4 de la C.N.U., l'exercice d'une force armée* »[459]. Ce recours à la force, qu'il soit issu d'une attaque cinétique ou d'une cyberattaque, doit atteindre un « *certain seuil de gravité pour déclencher une riposte en légitime défense* »[460] et doit donc avoir un « *caractère armé* »[461]. Ce caractère armé ne s'estime uniquement pas selon « *la nature des moyens utilisés pour son exercice* »[462] car « *la nature non militaire des moyens à l'origine d'une violence […] ne suffit pas à qualifier cette violence comme n'étant pas armée* »[463].

---

[455] DAILLIER Patrick, FORTEAU Mathias, PELLET Alain, « *Droit International Public* », LGDJ Lextenso éditions (8ème édition) 2009, p. 1040
[456] AKOTO Evelyne, « *Les cyberattaques étatiques constituent-elles des actes d'agression en vertu du droit international public* » : Deuxième partie*. Revue de droit d'Ottawa - Ottawa Law Review, Faculty of Law, Common Law Section, University of Ottawa, 2015, 46 (2), pp. 199. http://www.rdoolr.uottawa.ca/subsite/olr/ . <hal-01244601> p. 209
[457] C.I.J. « *Affaire des Activités militaires et paramilitaires au Nicaragua et contre celui-ci* » du 27 juin 1986 (Nicaragua *c.* États-Unis d'Amérique), fond, arrêt, Recueil 1986, § 190, p. 100
[458] DAILLIER Patrick, FORTEAU Mathias, PELLET Alain, « *Droit International Public* », LGDJ Lextenso éditions (8ème édition) 2009, p. 1041
[459] VAN STEENBERGHE Raphaël, « *La légitime défense en droit international public* », éditions Larcier, 2012, p. 196
[460] *Ibid*.
[461] *Ibid*.
[462] *Ibid*. p. 201
[463] *Ibid*. p. 201

270. En effet, il est reconnu qu' « *une attaque armée peut avoir lieu avec des objets ou des forces qui ne sont pas des armes à feu mais qui dégagent des effets de contrainte et de destruction équivalents* »[464]. Comme nous l'avons vu précédemment, les cyberattaques sont tout à fait à même d'entraîner des effets de contrainte et de destruction équivalents[465]. Cela a notamment été le cas pour l'Estonie, la Géorgie, mais aussi pour l'Iran, où chaque cyberattaque a été soit un élément de contrainte et de subversion[466], soit de destructions matérielles pour les États victimes[467].

271. Les cyberattaques et les attaques cinétiques, ayant les mêmes effets et les mêmes conséquences et étant dès lors des recours à la force similaire, doivent obéir à la même logique d'appréciation pour déterminer s'ils ont atteint le seuil de gravité nécessaire pour être une agression armée. De même que cette méthode a été utilisée pour déterminer si les cyberattaques étaient des recours à la force[468], il faut encore une fois s'attacher à la nature des effets que va avoir pour conséquence ce recours à la force[469], la notion de force armée ne s'appréciant pas au sens de « *force armée militaire ou paramilitaire mais au sens d'une violence physique se traduisant par une atteinte matérielle à des biens ou à des personnes* »[470].

272. Dès lors, pour constituer une agression, du moment que les effets et les conséquences ont atteint le seuil de gravité requis, il importe peu que le recours à la force soit issu d'une attaque cinétique ou d'une cyberattaque pour ouvrir à un État le droit à l'exercice de la légitime défense[471]. En effet, il suffit que cet usage de la force illicite préexistant soit dirigé contre un État c'est-à-dire contre son intégrité territoriale ou contre son « indépendance politique[472] selon la définition consacrée de l'article 2 paragraphe 4 de la C.N.U. Cette limitation à l'intégrité territoriale ou l'indépendance politique n'est pas limitative car, en réalité, est prohibé tout recours à la

[464] VAN STEENBERGHE Raphaël, « *La légitime défense en droit international public* », éditions Larcier, 2012, p. 201
[465] En ce sens *v*. Partie I, Chapitre 2, Section 1, Paragraphe 1, § 101 à 103
[466] En ce sens *v*. TAILLAT Stéphane, « *un mode de guerre hybride dissymétrique ? Le cyberespace* », éditions Institut de Stratégie Comparée, 2016/1 (n°111), p. 89-106, § 1
[467] Partie I, Chapitre 2, Section 1, Paragraphe 1, § 96 à 105
[468] Partie I, Chapitre 2, Section 2, Paragraphe 2, § 154 à 164
[469] En ce sens *v*. VAN STEENBERGHE Raphaël, « *La légitime défense en droit international public* », éditions Larcier, 2012, p. 201
[470] *Ibid*. p. 202
[471] En ce sens *v*. SIMONET Loïc, « *L'usage de la force dans le cyberespace et le droit international* », Annuaire de droit français international, 2012, 58, pp. 117-143, p. 117
[472] En ce sens *v*. VAN STEENBERGHE Raphaël, « *La légitime défense en droit international public* », éditions Larcier, 2012, p. 203

force contre les États. En effet, « *il apparaît clairement à la lumière de l'intention des auteurs de la Charte que ces notions ne vis(ai)ent nullement à réduire le champ d'application de l'interdiction qui y était prévue* »[473]. Telle est la position de l'A.G.N.U. mais aussi celle du Conseil de sécurité ainsi que de la pratique internationale qui abonde « *en actes de violences physiques qui ont été qualifiés d'emploi de la force voire d'agression armée alors qu'ils n'avaient pas entraîné de modification de frontières ni de chute de gouvernement* »[474]. D'ailleurs, il faut souligner le fait que le « *Conseil de sécurité n'a pas hésité à attribuer la qualification d'agression armée ou une qualification similaire comme celle d'acte agressif ou d'acte d'agression à des incursions (para)militaires ponctuelles* »[475]. Il ressort de ce constat qu'au même titre que les recours à la force par attaque cinétique, toute cyberattaque étant un recours à la force contre un État est susceptible de constituer une agression fondant l'exercice du droit à la légitime défense. Ce dernier n'étant toutefois possible que si l'agression par cyberattaque remplit le seuil de gravité exigé, le recours à la force pouvant être dirigé (tout en n'y étant pas limité) contre l'intégrité territoriale ou l'indépendance politique de l'État. Les États pourraient alors recourir « *à des armes conventionnelles en réponse à une cyberattaque qui constituerait une agression armée* »[476].

273. La C.I.J. a confirmé l'interdiction générale des recours à la force dans son affaire des Activités armées en R.D.C. en affirmant que l'emploi de la force de l'Ouganda contre la R.D.C. et l'occupation de certains territoires constituaient une agression armée alors même que cela n'avait pas entraîné de « *changement de gouvernement ni de modifications des frontières* »[477] . Cette mention spéciale à l'intégrité territoriale et l'indépendance politique a pour objectif d'assurer « *l'inviolabilité territoriale* »[478]. Par conséquent, la légitime défense a *« pour objet premier de protéger un État contre la violation de sa souveraineté territoriale par une force armée d'une certaine gravité* »[479], que les atteintes à l'intégrité territoriale et l'indépendance politique « *impliquent*

[473] VAN STEENBERGHE Raphaël, « *La légitime défense en droit international public* », éditions Larcier, 2012, p. 207
[474] *Ibid*. p. 207
[475] *Ibid*. p. 207
[476] En ce sens *v*. DOUZET Frédéric, « *La géopolitique pour comprendre le cyberespace* », éditions Hérodote, 2014, n°152-153, pp. 3-21, § 40
[477] En ce sens *v*. VAN STEENBERGHE Raphaël, « *La légitime défense en droit international public* », éditions Larcier, 2012, p. 207
[478] *Ibid*. p. 209
[479] *Ibid*. p. 209

nécessairement »[480], leur violation indiquant un « *degré maximum de gravité* »[481] étant donné que cela « *porte directement atteinte à la survie d'un État* »[482]. Mais elle n'est pas limitée à ces deux cas. En effet, « *si toute agression n'a pas pour effet d'anéantir directement l'État agressé, une agression armée comporte [...] le risque d'atteintes toujours plus graves à la souveraineté de cet État, atteintes pouvant tendre vers un but ultime, la modification du territoire ou la chute du gouvernement* »[483], ce qui peut être le cas des cyberattaques, notamment celles complémentaires d'actions classiques.

274. De même, des « *attaques commises depuis l'étranger contre les ressortissants d'un État sur le territoire de cet État entraînent nécessairement une violation de la souveraineté territoriale, violation qui est, a priori, qualifiable d'agression armée si elle est suffisamment grave* »[484]. L'État victime aura alors le droit « *d'y réagir en légitime défense si ces attaques sont d'une certaine gravité [...] sa souveraineté ayant été violée par un emploi de la force [...] exercé contre des militaires, des représentants de l'État [...] ou contre des civils, présentant une gravité particulièrement importante* »[485]. L'exercice de la légitime défense pourrait ainsi être tout à fait possible dans le cas d'une cyberattaque étatique dès lors que celle-ci est un recours à la force contre la souveraineté d'un autre État. Par exemple, mais non exclusivement, contre son intégrité territoriale comme cela a été le cas en Géorgie lorsque les cyberattaques ont permis de soutenir des miliciens revendiquant l'indépendance de l'Ossétie du Sud[486]. Cela pourrait également être le cas lors de recours à la force contre sa population et le fonctionnement même du pays tel que l'a connu l'Estonie[487], voire en entraînant des destructions matérielles contre des biens comme l'Iran dans l'affaire Stuxnet[488], ou encore comme en Géorgie en les combinant à des opérations militaires[489].

---

[480] VAN STEENBERGHE Raphaël, « *La légitime défense en droit international public* », éditions Larcier, 2012, p. 209
[481] *Ibid*. p. 210
[482] *Ibid*. p. 210
[483] *Ibid*. p. 211
[484] *Ibid*. p. 212
[485] *Ibid*. p. 213
[486] Le Monde Europe, « *Russie et Géorgie en guerre pour l'Ossétie du Sud* », 05.08.2008
[487] En ce sens *v*. MONGIN Dominique, « *Les cyberattaques, armes de guerres en temps de paix* », éditions Esprit, 01/2013, p. 32-49, § 7
[488] *Ibid*. § 8-9
[489] En ce sens *v*. DOUZET Frédéric, « *La géopolitique pour comprendre le cyberespace* », éditions Hérodote, 2014, n°152-153, pp. 3-21, § 19

275. Enfin, dans son avis consultatif sur la Licéité de la menace ou de l'emploi d'armes nucléaires, la C.I.J. a estimé que, l'interdiction de l'emploi de la force édictée par la C.N.U., tout comme la reconnaissance du droit naturel de légitime défense (individuelle ou collective) en cas d'agression armée, ainsi que la reconnaissance de la licéité du recours à la force conformément au chapitre VII de la Charte, ne préjugeait pas de l'usage d'armes particulières et s'appliquait à n'importe quel emploi de la force, indépendamment des armes employées. Dès lors, le recours à la légitime défense face à une cyberattaque constituant un tel acte paraît justifié. Il faudra, cependant, que ce recours à la force remplisse le seuil de gravité exigé, le même que celui exigé pour les attaques cinétiques.

276. Cette gravité peut s'apprécier selon les moyens utilisés (militaires etc.) ou les dégâts causés aux personnes et aux biens (pertes en vies humaines, dommages économiques etc.)[490]. La C.I.J. a d'ailleurs « *affirmé dans l'arrêt Nicaragua que la gravité d'une opération paramilitaire dépendait de la dimension et des effets de l'opération* »[491].

277. N'importe quel recours à la force n'entraîne pas la qualification d'agression et seule « *la forme la plus grave et la plus dangereuse de l'emploi illicite de la force* »[492] entraîne la qualification d'agression. Un « *certain degré de gravité* »[493] est donc requis pour que le recours à la force soit qualifié d'agression. Ce degré de gravité du recours à la force tient d'ailleurs compte de « *l'intention de poursuivre un objectif illicite contre un État déterminé* »[494]. Toutefois, cette question du seuil de gravité est assez discutée en droit international. En ce qui concerne les recours à la force cinétique, cette question étant « *abondamment controversée tant les termes de l'article 51 de la C.N.U. et la pratique des États ne fournissant pas d'éléments de réponses explicites* »[495]. Nous nous rattacherons par conséquent à l'analyse de la C.I.J. et les cyberattaques étant des recours à la force devront donc être soumis au même seuil de gravité requis que les recours à la force issus d'attaques cinétiques, à savoir devraient être considérés comme des

[490] En ce sens *v.* VAN STEENBERGHE Raphaël, « *La légitime défense en droit international public* », éditions Larcier, 2012, p. 215
[491] *Ibid.* p. 216
[492] *Ibid.* p. 217
[493] *Ibid.* p. 217
[494] *Ibid.* p. 228
[495] *Ibid.* p. 242

agressions armées les cyberattaques étant des recours à la force sous « *la forme la plus grave et la plus dangereuse de l'emploi illicite de la force* »[496], mettant en péril *« la souveraineté de cet État* »[497] comme nous l'avons mentionné dans la présente partie. Dès lors, que ce seuil serait atteint, toute « *riposte à une telle agression visant à repousser cette dernière* »[498] entrerait dans le cadre de la légitime défense.

278. En matière de cyberattaque, il est considéré qu'un tel seuil serait atteint pour « *toute cyberattaque entraînant la destruction physique de biens ou la mort de personnes pourrait automatiquement être assimilée à une attaque armée* »[499]. Cela est d'ailleurs la position des États-Unis qui ont affirmé que « *de tels actes, dans la mesure où ils provoqueraient la paralysie ou la destruction partielle du fonctionnement de l'État, de l'économie nationale ou des systèmes civils collectifs, seraient désormais considérés comme des actes de guerre, ouvrant la voie à une riposte militaire de même nature que celle que s'attirerait une agression armée* »[500].

Paragraphe 2 : Les conditions d'exercice d'une riposte en légitime défense.

Dans ce paragraphe, nous aborderons les autres conditions que doivent respecter les mesures prises dans le cadre de la légitime défense en riposte à une cyberattaque.

279. S'il est nécessaire de faire face à une agression armée afin de pouvoir « *répliquer sur la base de la légitime défense* »[501], cela n'est cependant pas la seule condition à remplir pour l'État victime. En effet, la légitime défense doit obéir à plusieurs règles concernant ses modalités de mise en œuvre. L'article 51 précise notamment que l'État peut exercer son droit de légitime défense « *jusqu'à ce que le Conseil de sécurité ait pris les mesures nécessaires pour maintenir la paix et la sécurité internationales* »[502] et que les mesures prises « *doivent être portées à la connaissance du Conseil de*

[496] VAN STEENBERGHE Raphaël, « *La légitime défense en droit international public* », éditions Larcier, 2012, p. 217
[497] *Ibid*. p. 211
[498] *Ibid*. p. 211
[499] SIMONET Loïc, « *L'usage de la force dans le cyberespace et le droit international* », Annuaire de droit français international, 2012, 58, pp. 117-143, p. 125
[500] *Ibid*.
[501] *Ibid*.
[502] Charte des Nations unies, article 51

sécurité »[503]. Toutefois, les modalités d'exercice de la légitime défense « *ne sont pas définies de manière complète par l'article 51 de la Charte et doivent être précisées par des normes coutumières* » [504].

280. A ce titre, la C.I.J a consacré dans l'affaire des Activités militaires et paramilitaires au Nicaragua et contre celui-ci de 1986, la règle de droit coutumier selon laquelle « *la légitime défense ne justifierait que des mesures proportionnées à l'agression subie* »[505]. Cette condition de proportionnalité est « *reconnue depuis longtemps comme une condition fondamentale inhérente à la légitime défense* »[506].

281. Cette condition implique pour la C.I.J. que la mesure prise dans le cadre de la légitime défense doit être proportionnée à l'atteinte subie par l'État[507]. Il est donc requis un certain « *équilibre entre l'ampleur matérielle de l'agression armée et l'ampleur matérielle de l'action en légitime défense qui y répond* »[508]. Tout comme l'analyse opérée lors de la détermination du seuil de gravité du recours à la force opéré par l'État agresseur afin de déterminer si cela correspond à une agression armée ou non, l'analyse de la proportionnalité de l'action en légitime défense doit prendre en compte « *les moyens utilisés et les cibles visées par chacune des parties* »[509] mais également « *les dommages (pertes humaines et matérielles) qu'elles se sont réciproquement infligés* »[510].

282. C'est donc une appréciation quantitative qui est réalisée pour déterminer si l'exercice de la légitime défense a été proportionnée car c'est cette « *mise en balance de deux éléments de même nature* »[511] qui va permettre d'établir le « *rapport quantitatif qui met en œuvre la relation de proportionnalité proprement dite* »[512]. La C.I.J. a consacré cette exigence de proportionnalité quantitative de la légitime défense dans toutes ses affaires puisque, à chaque fois qu'elle « *s'est référé à la condition de*

[503] Charte des Nations unies, article 51
[504] DAILLIER Patrick, FORTEAU Mathias, PELLET Alain, « *Droit International Public* », LGDJ Lextenso éditions (8ème édition) 2009, p. 1042
[505] *Ibid.*
[506] En ce sens *v.* VAN STEENBERGHE Raphaël, « *La légitime défense en droit international public* », éditions Larcier, 2012, p. 446
[507] *Ibid.* p. 448
[508] *Ibid.*
[509] *Ibid.*
[510] *Ibid.*
[511] *Ibid.*
[512] *Ibid.*

proportionnalité dans l'analyse de la légitime défense, elle a envisagé cette condition de manière quantitative ou […] comme imposant de mettre en balance l'action en légitime défense avec l'agression armée à laquelle cette action répondait »[513]. Notamment, dans l'affaire des Plates-formes Pétrolières, la C.I.J. a tenu compte du fait que, pour un navire endommagé par une mine n'ayant ni coulé ni causé de pertes humaines, les Américains ont détruit deux frégates iraniennes, d'autres navires et aéronefs et deux plates-formes pétrolières[514]. *De facto,* la C.I.J. a estimé que « *ni l'opération Praying Mantis dans son ensemble, ni même le volet de celle-ci qu'a constitué la destruction des plates-formes de Salman et Nasr ne sauraient être considérés, dans les circonstances de l'espèce, comme un emploi proportionné de la force au titre de la légitime défense* »[515].

283. Dès lors, bien que la légitime défense soit justifiée par la préexistence d'une agression armée, l'État victime d'une cyberattaque constituant une agression armée ne peut pas répondre avec n'importe quelle mesure. Il devra toujours respecter le principe de proportionnalité et son approche quantitative consacrée par la C.I.J.[516] ainsi que répondre de manière équilibrée à la cyberattaque. Par exemple, cela peut induire l'exclusion du recours à l'arme nucléaire contre un pays si celui-ci ne combine pas sa perturbation des systèmes vitaux de l'État victime d'une opération militaire classique. Ce type de cyberattaque, comme l'a connu le Brésil[517], ne peut justifier un recours à l'arme nucléaire étant donné que si l'État et ses systèmes vitaux sont perturbés, la destruction totale de l'État, elle, n'est pas imminente. Il faut cependant noter que la C.I.J n'a pas pu dégager d'autorisation ou d'interdiction complète du recours à la menace ou à l'usage de l'arme nucléaire, qu'elles soient conventionnelles ou coutumières[518], ne faisant qu'envisager les cas « *où la survie de l'État est en cause* »[519]. Toutefois, un tel acte peut cependant justifier un recours à la force proportionné, c'est-à-dire ciblé contre l'origine de la cyberattaque, par des moyens conventionnels (bombardements aériens, missiles).

---

[513] VAN STEENBERGHE Raphaël, « *La légitime défense en droit international public* », éditions Larcier, 2012, p. 450
[514] *Ibid.*
[515] *Ibid.*
[516] *Ibid.*
[517] En ce sens *v.* BAUDIN Laura, « *Les cyberattaques dans les conflits armées* », éditions L'Harmattan, 2014, p. 54
[518] C.I.J. « *Licéité de la menace ou de l'emploi d'armes nucléaires* », avis consultatif, Recueil 1996, p. 226, § 105
[519] *Ibid.* § 96 et 105

284. De même, comme cela fut le cas en Géorgie[520], un État victime d'une opération combinée, où une cyberattaque est utilisée en complément d'une attaque classique, pourrait recourir à la force de manière ciblée (bombardements contre le centre d'où est émise la cyberattaque ou contre les forces ennemies). Cependant, il ne pourrait bombarder massivement le pays. En ce sens, la France elle-même prône « *la nécessité pour les forces françaises de définir une doctrine et un cadre d'emploi qui devront respecter le principe de riposte proportionnelle à l'attaque* »[521].

285. Toutefois, le développement des cyberattaques attaques autonomes capables de détruire elles-mêmes des infrastructures, ainsi que d'avoir un fort potentiel de destructions matérielles (contre des biens comme contre des personnes) peut rendre cet exercice de « *mise en balance* »[522] plus délicat. L'État devra donc tenter d'avoir la riposte la plus proportionnée possible. Pour cela il pourra notamment s'appuyer sur le respect des règles du *jus in bello*, dont toute violation tend à considérer une action disproportionnée, mais aussi sur les autres conditions d'exercice de la légitime défense telles que la nécessité et l'immédiateté.

286. En effet, au sujet du *jus in bello*, certains auteurs ont constaté que, bien que le *jus ad bellum* et le *jus in bello* soient bien distincts (le premier définissant « *les conditions dans lesquelles un État est en droit de recourir à la force dans ses relations avec les autres États* »[523] et le second déterminant « *les obligations des belligérants lorsque ceux-ci sont engagés dans un conflit armé* »[524]), il est cependant possible de relever que « *de nombreux exercices du droit de légitime défense ont été jugés disproportionnés, ou à tout le moins illicites, parce que les mesures prises à cette occasion avaient engendré des pertes civiles et des dégâts aux infrastructures civiles jugés excessifs* »[525]. Bien que le *jus ad bellum* et le *jus in bello* soient bien distincts, le *jus in bello* peut donc cependant permettre aux États de choisir des mesures ou, tout au

[520] En ce sens *v*. LIMONIER Kévin et GERARD Colin, « *La guerre hybride russe dans le cyberespace* », éditions Hérodote, 2017, n°166-167, pp 145-163, § 9
[521] En ce sens *v*. MONGIN Dominique, « *Les cyberattaques, armes de guerres en temps de paix* », éditions Esprit, 01/2013, p. 32-49, § 16
[522] VAN STEENBERGHE Raphaël, « *La légitime défense en droit international public* », éditions Larcier, 2012, p. 448
[523] *Ibid*. p. 459
[524] *Ibid*. p. 459
[525] *Ibid*. p. 461

moins, lui indiquer celles qui rendraient son action en légitime défense disproportionnée, et donc à surtout éviter de sélectionner.

287. L'État en situation de légitime défense peut également s'aider des autres conditions d'exercice de la légitime défense. En effet, l'action en légitime défense doit également être nécessaire. Ce principe de « *nécessité de l'exercice* »[526] a été rappelé par la C.I.J. dans l'affaire des Activités militaires au Nicaragua et contre celui-ci où la Cour a précisé que « *la légitime défense ne justifierait que des mesures proportionnées à l'agression subie, et nécessaires pour y mettre fin* »[527]. Ce principe de nécessité implique que « le recours à la force soit la seule solution pour mettre un terme à l'agression ». De ce fait, la mesure prise doit être la seule possible face à l'agression et son objectif « *ne peut consister qu'à mettre un terme à l'agression* »[528].

288. Le principe de nécessité a été réaffirmé par la C.I.J. dans l'affaire des Plates-formes pétrolières (République d'Iran *c.* États-Unis d'Amérique)[529] en précisant que « *les caractères de nécessité et de proportionnalité constituaient deux conditions sine qua non dans l'exercice de la légitime défense* »[530]. Outre d'être bien posé en droit international et d'imposer *de facto* une condition supplémentaire à l'exercice de la légitime défense, le principe de nécessité peut également permettre aux États de choisir une mesure adéquate à la cyberattaque constituant une agression qu'il subit. En effet, une riposte qui n'aurait pas pour seul objectif de « *mettre un terme à l'agression* »[531], mais par exemple, de mettre fin à la cyberattaque et de détruire le gouvernement de l'État responsable, violerait le principe de nécessité et *de facto* pourrait indiquer que la riposte est disproportionnée.

---

[526] VAN STEENBERGHE Raphaël, « *La légitime défense en droit international public* », éditions Larcier, 2012, p. 448

[527] C.I.J. « *Affaire des Activités militaires et paramilitaires au Nicaragua et contre celui-ci* » du 27 juin 1986 (Nicaragua *c.* États-Unis d'Amérique), fond, arrêt, Recueil 1986, § 195, p. 122 in DAILLIER Patrick, FORTEAU Mathias, PELLET Alain, « *Droit International Public* », LGDJ Lextenso éditions (8ème édition) 2009, p. 1042

[528] POMES Eric, « *Droit International Publi*c », éditions Panorama du droit, 2012, p. 279

[529] En ce sens *v.* C.I.J. « *Plates-formes pétrolières* » (République islamique d'Iran c. États- Unis d'Amérique), arrêt, Recueil 2003, p. 161

[530] POMES Eric, « *Droit International Publi*c », éditions Panorama du droit, 2012, p. 279

[531] *Ibid*.

289. En effet, le fait que les actions entreprises au nom du droit de légitime défense soient « *nécessaires à la réalisation de l'objectif de protection* »[532] permet de « *déterminer si cette action est proportionnée* »[533]. Telle était d'ailleurs la conception de Roberto Ago qui précisait que « *les exigences de la nécessité et de la proportionnalité de l'action menée en légitime défense ne sont que les deux faces d'une même médaille. L'état de légitime défense ne vaudra […] que si ce dernier ne pouvait pas atteindre le résultat visé par un comportement […] ne pouvant se réduire à un emploi plus restreint de la force armée* »[534]. Face à une cyberattaque constituant une agression, un État peut donc prendre des mesures de force armée au nom de la légitime défense mais ne devra pas excéder ce qui est nécessaire à sa cessation. Il devra aussi remplir une dernière condition d'exercice *rationae temporis*.

290. La dernière modalité de mise en œuvre de la responsabilité impose à un État une condition *rationae temporis*. En effet, un État ne peut prendre des mesures dans le cadre de la légitime défense que « *tant que l'attaque n'a pas pris fin ou que la force demeure indispensable pour s'en protéger* »[535]. L'action en légitime défense doit donc être immédiatement réalisée lorsqu'a lieu l'agression armée. Une fois celle-ci terminée, ou lorsque la force n'est plus nécessaire, l'action en légitime défense n'est plus une solution possible.

291. Les cyberattaques constituant des agressions devraient donc permettre aux États victimes, comme n'importe quelle agression, de prendre des mesures armées dans le cadre de la légitime défense afin d'y mettre fin. Les États exerçant leur droit de légitime défense devront cependant respecter, en sus des conditions de l'article 51 de la C.N.U., les mêmes conditions coutumières de proportionnalité, de nécessité et d'immédiateté, conditions qui une fois réunies permettraient à l'État de déterminer (avec d'autres facteurs tel que le D.I.H.) les mesures adéquates pour mettre fin à l'agression, tout en respectant les exigences du droit international. Toutefois, si le droit individuel de

[532] VAN STEENBERGHE Raphaël, « *La légitime défense en droit international public* », éditions Larcier, 2012, p. 451
[533] *Ibid*.
[534] AGO Roberto, « *Projet d'articles sur la responsabilité de l'État pour fait internationalement illicite* » *in* VAN STEENBERGHE Raphaël, « *La légitime défense en droit international public* », éditions Larcier, 2012, p. 451
[535] POMES Eric, « *Droit International Publi*c », éditions Panorama du droit, 2012, p. 279

légitime défense est pertinent en matière de cyberattaque, celui de la légitime défense collective prend une importance toute particulière en la matière.

292. La légitime défense collective est le droit « *pour un État non directement atteint par une agression d'intervenir au nom des accords de défense le liant au pays agressé* »[536]. Dès lors qu'un tel accord existe, cela « *autorise tout État partie, et non pas seulement sa première victime, à invoquer le droit à la légitime défense collective pour entrer dans le conflit armé* »[537]. L'article 51 de la C.N.U. permet en fait à « *chaque État d'exercer son droit propre, mais il le fait sur demande de l'État victime* »[538]. Il faut cependant noter qu'il n'est « *pas nécessaire que l'accord sur lequel se fondent les États soit antérieur au déclenchement de l'agression, on admet qu'une intervention sollicitée par un État victime d'une agression armée, seulement au moment de l'agression, reste soumise au droit de légitime défense* »[539]. Ce droit de légitime défense collective a été consacré par la Cour Internationale de Justice dans l'affaire des Activités militaires et paramilitaires au Nicaragua et contre celui-ci de 1986 dans laquelle elle a rappelé l'existence du droit de légitime défense collective des États reposant à la fois sur le droit coutumier mais aussi sur l'article 51 de la C.N.U.[540]. La C.I.J. a réaffirmé le principe selon lequel la légitime défense collective est un droit qui *« peut être mis en œuvre collectivement* » dans l'affaire des Activités armées sur le territoire du Congo[541]. La mise en œuvre de ce droit de légitime défense collective devra cependant répondre « *aux mêmes conditions que celles de la légitime défense individuelle* »[542].

293. Le droit de légitime défense prend une importance particulière en termes de cyberattaques puisque celles-ci peuvent avoir pour objectif et pour conséquence de paralyser totalement un pays, et ainsi de l'empêcher de prendre des mesures dans le cadre de la légitime défense individuelle. Les États peuvent alors demander assistance à leurs alliés, ou ceux-ci peuvent le faire d'eux-mêmes en invoquant le droit à la légitime

---

536 DUPUY Pierre-Marie et KERBRAT Yann, « *Droit International Public* », éditions Dalloz (13ème édition), 2016, p. 666

537 DAILLIER Patrick, FORTEAU Mathias, PELLET Alain, « *Droit International Public* », LGDJ Lextenso éditions (8ème édition) 2009, p. 1043

538 *Ibid*.

539 *Ibid*.

540 En ce sens *v*. DUPUY Pierre-Marie et KERBRAT Yann, « *Droit International Public* », éditions Dalloz (13ème édition), 2016, p. 666

541 C.I.J. *Activités armées sur le territoire du Congo »* (République démocratique du Congo *c.* Ouganda), arrêt, Recueil 2005, p. 16

542 DAILLIER Patrick, FORTEAU Mathias, PELLET Alain, « *Droit International Public* », LGDJ Lextenso éditions (8ème édition) 2009, p. 1043

défense collective. Cela a d'ailleurs été l'une des possibilités envisagées par l'Estonie en 2007, qui a émis la possibilité de demander l'aide de l'OTAN[543]. La légitime défense collective peut donc être un moyen supplémentaire de mettre fin à une cyberattaque constituant une agression, et ce même si l'État victime est paralysé. Elle peut également remplir un objectif de dissuasion au même titre que la possibilité des représailles armées[544], permettant ainsi d'éviter un recours massif à ce type de cyberattaques d'une ampleur aussi dévastatrice, évitant *de facto* que les États contournent l'interdiction du recours à la force et de l'agression par ce biais. Les États-Unis ont d'ailleurs accordé une « *place importante au concept de dissuasion, qu'il soit nucléaire ou conventionnel […] ainsi que dans ce domaine* ».[545]

294. Un dernier pan de la légitime défense doit être abordé concernant les cyberattaques : celui de la possibilité d'user de la légitime défense préventive ou préemptive afin d'éviter une agression par cyberattaque d'un autre État. En effet, se pose la question de la possibilité pour un État d'employer la force afin de « *prévenir une agression armée à son encontre* »[546], c'est-à-dire de se placer en situation de « *légitime défense préventive* », terme générique regroupant les actions préventives[547]. En effet, deux types de légitime défense préventive ont été dégagés[548], dont les États n'hésitent pas à se servir. Citons le cas d'Israël en 1981 contre l'Irak, et celui des États-Unis qui, en 1998, avaient hésité à invoquer la légitime défense préventive contre des camps d'entraînement terroristes en Afghanistan[549]. Il existe ainsi la légitime défense préventive « *anticipative* »[550], réalisée *« en vue de se protéger contre une menace non imminente d'agression armée* »[551], que seuls quelques États entérinent[552]. A l'inverse,

[543] En ce sens *v*. MONGIN Dominique, « *Les cyberattaques, armes de guerres en temps de paix* », éditions Esprit, 01/2013, p. 32-49, § 22
[544] En ce sens *v*. KELLO Lucas, « *Les cyberarmes : dilemmes et futurs possibles* », éditions Institut français des relations internationales (IFRI), 2014/4 (Hiver), p. 139-150
[545] MONGIN Dominique, « *Les cyberattaques, armes de guerres en temps de paix* », éditions Esprit, 01/2013, p. 32-49, § 24
[546] VAN STEENBERGHE Raphaël, « *La légitime défense en droit international public* », éditions Larcier, 2012, p. 358
[547] *Ibid*.
[548] *Ibid*. p. 398
[549] SIMONET Loïc, « *L'usage de la force dans le cyberespace et le droit international* », Annuaire de droit français international, 2012, 58, pp. 117-143, p. 137
[550] VAN STEENBERGHE Raphaël, « *La légitime défense en droit international public* », éditions Larcier, 2012, p. 402
[551] *Ibid*.
[552] *Ibid*. p. 404

la légitime défense « *préemptive* »[553], réalisée quant à elle « *pour se protéger contre une menace imminente d'agression armée* »[554], est soutenue par un grand nombre d'États qui se sont prononcés en sa faveur[555].

295. Toutefois, bien que les États se soient positionnés pour ou contre ces possibilités de légitime défense préventive, cette question n'a pas été tranchée clairement, ni par la C.N.U., ni par les juridictions internationales, et une position nuancée est donc de rigueur[556]. La C.I.J. ne s'est pas prononcée explicitement sur la question mais, dans son avis consultatif sur la Licéité de la menace ou de l'emploi d'armes nucléaires [557], a tout de même envisagé indirectement « *une telle possibilité quand elle considère le cas extrême dans lequel la survie même de l'État est en cause* »[558]. Il n'existe pas non plus de consensus à ce sujet dans la pratique, celle-ci témoignant plutôt « *clairement de l'absence de consensus à son sujet* »[559]. Il est donc nécessaire en matière d'agression par cyberattaque de ne pas autoriser ou interdire catégoriquement de telles actions, et d'adopter la position nuancée de rigueur pour cette question, comme cela est le cas lors de risques d'agression par des moyens conventionnels.

296. Face aux cyberattaques constituant des agressions armées, la légitime défense peut donc être une solution afin d'y mettre un terme, voire de les dissuader en laissant cette possibilité ouverte aux États victimes et à leurs alliés, à l'instar des agressions armées réalisées par des moyens classiques. La légitime défense pourrait donc contribuer à encadrer et réguler les cyberattaques étatiques, ce qui est plus que jamais nécessaire étant donné que *« la cyberguerre comme nouvelle arme de guerre secrète (et comme moyen d'action combiné aux offensives conventionnelles)*[560] » voire comme moyen d'action autonome de destruction, « *existe dès le temps de paix et est appelée à prendre des proportions importantes* »[561].

---

[553] VAN STEENBERGHE Raphaël, « *La légitime défense en droit international public* », éditions Larcier, 2012, p. 406
[554] *Ibid*.
[555] *Ibid*.
[556] *Ibid*. p. 360
[557] C.I.J. « *Licéité de la menace ou de l'emploi d'armes nucléaires* », avis consultatif, Recueil 1996, p. 226, § 96 et 105
[558] VAN STEENBERGHE Raphaël, « *La légitime défense en droit international public* », éditions Larcier, 2012, p. 360
[559] *Ibid*. p. 390
[560] En ce sens *v*. MONGIN Dominique, « *Les cyberattaques, armes de guerres en temps de paix* », éditions Esprit, 01/2013, p. 32-49, § 23
[561] *Ibid*.

Conclusions

297. Il existe donc un véritable décalage entre la notion d'agression actuelle, qui ne prend en compte que les attaques conventionnelles, et la pratique des États qui ont de plus en plus recours aux cyberattaques pour contourner l'interdiction du recours à la force.

298. Ce décalage est en partie dû au fait que les cyberattaques ne sont pas encore encadrées par le droit international. Même si dans certains cas il est possible de leur appliquer des règles et des principes généraux du droit international, l'absence de textes spécifiques en la matière ouvre une brèche juridique que les États n'hésitent pas à saisir. Les États profitent donc du flou juridique actuel pour recourir à des cyberattaques pouvant aller parfois à l'encontre de principes essentiels du droit international coutumier et conventionnel. Les États développent ainsi une véritable militarisation des cyberattaques.

299. Les cyberattaques, naguère uniquement utilisées pour de l'espionnage, sont de plus en plus utilisées comme des moyens de guerre ou au sein de méthodes de guerre. Les États se servent des cyberattaques pour paralyser d'autres États, les déstabiliser, leur occasionner des dommages matériels voire même pour les attaquer, que ce soit de manière autonome ou de manière complémentaire, à l'appui d'une attaque conventionnelle ou non.

300. En témoigne la pratique étatique en la matière puisque les récentes cyberattaques ont démontré que, de plus en plus, elles sont à même de compléter voire remplacer les recours à la force classique, leur prodiguant une meilleure efficacité ou un palliatif efficace au principe d'interdiction du recours à la force entre États.

301. La volonté des États de développer les cyberattaques en ce sens va de pair avec leur prise de conscience de l'utilité actuelle des cyberattaques au vu du droit international actuel, ou plutôt au vu de l'absence de droit actuel en la matière. Les États se tournent donc de plus en plus vers les cyberattaques, accélérant leur développement et leur militarisation au sein de centres militaires nationaux voire régionaux.

302. Il est donc essentiel de développer le droit international afin qu'il puisse encadrer ces nouveaux comportements étatiques, ce qui nécessitera la mise en place d'un régime juridique spécifique aux cyberattaques en adéquation avec le droit international et ses principes fondamentaux, tels que l'interdiction du recours à la force et le règlement pacifique des différends ainsi que, *de facto*, l'interdiction de l'agression.

303. Ce développement du droit international afin d'encadrer les cyberattaques étatiques devra passer par l'extension de la notion d'agression pour que celle-ci puisse englober ces dernières et éviter que les États ne contournent l'interdiction de toute agression par le recours à des cyberattaques.

304. Cette extension de la notion d'agression est essentielle car le développement des cyberattaques étatiques a démontré que celles-ci peuvent être des recours à la force étant donné la similarité dans la perception des cyberattaques et des attaques classiques par les États, mais aussi dans les objectifs que ces deux types d'attaques permettent d'atteindre, dans la manière dont elles sont utilisées ainsi que dans leurs effets et leurs conséquences. Les cyberattaques pouvant être des recours à la force, elles doivent donc pouvoir constituer des agressions dès lors que le recours à la force qu'elles réalisent atteint le seuil de gravité d'une agression.

305. Dès lors que les cyberattaques pourront juridiquement être des recours à la force constituant des agressions, se posera la question des conséquences de cette reconnaissance et notamment de la mise en œuvre de la responsabilité internationale et des mesures que les États peuvent prendre face à de telles agressions.

306. Les États auront donc la possibilité d'invoquer la responsabilité internationale de l'État responsable de la cyberattaque et d'engager sa responsabilité pour fait internationalement illicite puisque ce type de cyberattaque viole déjà des principes du droit international, notamment l'interdiction du recours à la force et l'obligation de règlement pacifique des différends. De plus, ces cyberattaques étant étatiques, elles sont donc théoriquement attribuables à des États même si, en pratique, l'attribution est très difficile à réaliser. Toutefois, le développement et les avancées actuelles des technologies, notamment en matière de traçage, devraient, à terme, rendre possible cette attribution.

307. Cela devrait donc permettre d'engager la responsabilité d'un État auteur d'une cyberattaque constituant une agression pour fait internationalement illicite par l'État victime, voire par l'ensemble de la communauté internationale. Cette possibilité n'est pas exclue puisque l'interdiction du recours à la force entre États a été reconnue comme une obligation *erga omnes* en droit international. Cela permettra également aux États non lésés de demander la cessation de la cyberattaque, et aux États victimes d'exiger une réparation.

308. Cette reconnaissance de l'agression par cyberattaque permettra également aux États de réagir face à ces agressions. Ils pourront ainsi prendre des contre-mesures en réponse à ces cyberattaques puisque celles-ci sont à même de constituer un fait internationalement illicite. Au vu des particularités des cyberattaques, les États victimes pourraient même être autorisés, de manière exceptionnelle en droit international, à exercer des représailles proportionnées, ciblées, orientées et limitées à un objectif de cessation de la cyberattaque.

309. Enfin, cela ouvrira aux États la voie de l'exercice de la légitime défense s'il s'avère que cette agression par cyberattaque a atteint le seuil de gravité d'une agression armée. Les États devront cependant respecter toutes les conditions de la légitime défense qui, réunies et avec l'aide de certaines règles du droit international tel que le D.I.H., leur permettra de choisir une mesure adéquate pour répondre à cette agression armée par cyberattaque dans le cadre de la légitime défense.

310. La légitime défense collective sera également une possibilité pour les États comme pour n'importe quelle agression armée subie par un État et dans les mêmes conditions. En effet, afin d'éviter tout abus de la part des États, il sera essentiel d'appliquer les conditions de la légitime défense qui s'appliquent déjà pour les attaques conventionnelles, d'autant que les cyberattaques, du fait de leur spécificité, peuvent faciliter les abus de la part des États, d'où la nécessité de les assortir des mêmes règles que pour les ripostes face aux agressions par des moyens conventionnels. Toutefois, une position plus nuancée sera de rigueur pour la légitime défense préventive anticipative ou la légitime défense préemptive, comme cela est le cas pour ce type de légitime défense face à une menace d'agression armée conventionnelle.

311. L'extension de la notion d'agression permettant la reconnaissance d'agression par cyberattaque est donc essentielle et justifiée au vu du développement actuel des cyberattaques, et ce afin d'encadrer au mieux ces nouvelles pratiques étatiques. Cela est en effet crucial car les cyberattaques sont, d'une part, de plus en plus reconnues comme un nouveau tournant dans les relations internationales géopolitiques et géostratégiques des États et, d'autre part, apparaissent comme des nouveautés à même de redéfinir les rapports de force interétatiques. C'est pourquoi le droit international se doit d'évoluer afin de continuer d'encadrer au mieux ces nouveaux comportements étatiques en pleine émergence. L'encadrement juridique de ces cyberattaques sera le défi juridique de ce siècle, défi que le droit international se doit de relever.

BIBLIOGRAPHIE

Ouvrages

BAUDIN Laura, « *Les cyberattaques dans les conflits armés* », édition L'Harmattan, 2014

BETTATI Mario, « *Droit Humanitaire* », éditions Dalloz, 2012

COMBACAU Jean, SUR Serge, « *Droit International Public* », LGDJ Lextenso éditions (8ème édition), 2014

COT Jean-Pierre, PELLET Alain, FORTEAU Mathias, « *La Charte des nations unies commentaire article par article* », éditions Economica (3ème édition), 2005

DAILLIER Patrick, FORTEAU Mathias, PELLET Alain, « *Droit International Public* », LGDJ Lextenso éditions (8ème édition) 2009

DUPUY Pierre-Marie et KERBRAT Yann, « *Droit International Public* », éditions Dalloz (13ème édition), 2016

KAMTO Maurice, « *L'agression en droit international* », éditions Pédone, 2010

Manuel de Tallin paru en 2013 2.0

MARBEAU Michel, « *La Société des Nations, vers un monde multilatéral 1919-1946* », éditions Presses Universitaires François Rabelais de Tours, 2017

Nations unies, « *Analyse historique des faits relatifs à l'agression* », éditions Nations unies, 2003

PERRIN DE BRICHAMBAUT Marc, DOBELLE Jean-François, COULEE Frédérique, « *Leçons de droit international public* », éditions Dalloz (2ème édition), 2011

POMES Eric, « *Droit International Public* », éditions Panorama du droit, 2012

RIVIER Raphaële, « *Droit International Public* » (2ème édition), éditions Presses Universitaires de France, 2012, p. 627

SALMON Jean, « *Dictionnaire de Droit International Public* », éditions Bruylant, 2001, p. 81 Section, University of Ottawa, 2015, 46 (1), pp.1. http://www.rdoolr.uottawa.ca/subsite/olr/ <hal-01244603>

SICILIANOS Alexandre, « *Réactions décentralisées à l'illicite* », éditions LGDJ, 1990

TERTRAIS Bruno, « *La guerre* », éditions Presses Universitaires de France, 2010

VAN STEENBERGHE Raphaël, « *La légitime défense en droit international public* », éditions Larcier, 2012

VENTRE Daniel, « *Cyberespace et acteurs du cyberconflit* », éditions Lavoisier, 2011

Articles

AKOTO Evelyne, « *Les cyberattaques étatiques constituent-elles une agression en droit international public ?* » : Première partie. Revue de droit d'Ottawa - Ottawa Law Review, Faculty of Law, Common Law

AKOTO Evelyne. « *Les cyberattaques étatiques constituent-elles des actes d'agression en vertu du droit international public* » : Deuxième partie partie. Revue de droit d'Ottawa - Ottawa Law Review, Faculty of Law, Common Law Section, University of Ottawa, 2015, 46 (2), pp.199. p. 221

BAUD Michel, « *La cyberguerre n'aura pas lieu, mais il faut s'y préparer* », éditions Politique étrangère, 2012, p. 305-316

BORIES Clémentine, « *Appréhender la cyberguerre en droit international. Quelques réflexions et mises au point* », éditions La revue des Droits de l'Homme, juin 2014

C.I.C.R., « *Déclaration du C.I.C.R. aux Nations unies sur les armes, 2017* », 10.10.2017

C.I.C.R., « *Quelles limites le droit de la guerre impose-t-il aux cyberattaques ?* », 28.06.2013 https://www.icrc.org/fre/resources/documents/faq/130628-cyber-warfare-q-and-a-eng.htm

COUSTILLIERE Arnaud, « *La cyberdéfense : un enjeu global et une priorité stratégique pour le ministère de la Défense* », Revue Sécurité Globale, éditions ESKA, 2013/I (n°23), p. 27-32

D'ELIA Danilo, « *La guerre économique à l'ère du cyberespace* », Revue Hérodote, éditions La Découverte, 2014/I (N°152-153), p. 240-260

DOUZET Frédéric, « *Chine, États-Unis : la course aux cyberarmes a commencé* », éditions sécurité globale, 2013, n°23, pp 43-51

DOUZET Frédéric, « *La géopolitique pour comprendre le cyberespace* », éditions Hérodote, 2014, n°152-153, pp. 3-21

DROEGE Cordula, « *Pas de vide juridique dans le cyberespace* », C.I.C.R., 16.08.2011

FONTAINE Pierre, « *Virus et cyberattaques, le Japon soigne le mal par le mal* », 04.01.2012

GHERNAOUTI-HELIE Solange, « *Menaces, conflits dans le cyberespace et cyberpouvoir* », Revue Sécurité et Stratégie, éditions Club des directeurs de Sécurité des Entreprises, 2011/3 (7), p. 61-67

HINDAWI Coralie, « *D'une guerre à l'autre ou un retour sur les ambiguïtés de la résolution 687 (1991) du Conseil de sécurité* », Revues Etudes Internationales, Editions Erudit, volume 37, n°3, septembre 2006, p. 357-487

HIRIDJEE Kévin, « *Le modèle westphalien* », IEP Paris http://sciences-po.macrocosme.net/cr_exposes/Hiridjee_Wesphalie.pdf

HUYGHE François Bernard, « *Stratégie dans le cyberespace* », éditions Médium, 2012, N°31, pp 129-146

KELLO Lucas, « *Les cyberarmes : dilemmes et futurs possibles* », éditions Institut français des relations internationales (IFRI), 2014/4 (Hiver), p. 139-150

LAGOT Daniel, « *Le droit international et les guerres de notre temps* », éditions L'Harmattan, 2016

LIMONIER Kévin et GERARD Colin, « *La guerre hybride russe dans le cyberespace* », éditions Hérodote, 2017, n°166-167, pp. 145-163

LOUIS-SIDNEY Barbara, « *La dimension juridique du cyberespace* », éditions revue internationale et stratégique, 2012/3 (n°87), p. 73-82

MONGIN Dominique, « *Les cyberattaques, armes de guerres en temps de paix* », éditions Esprit, 01/2013, p. 32-49

MULLET-FEUGA Philippe, « *Cyberespace, nouvelles menaces et nouvelles vulnérabilités* », éditions sécurité globale, 2017/I n°9, pp. 83-95

Nations unies, « *Les cyberconflits et la sécurité nationale* », éditions Chronique O.N.U., Vol. L No. 2 09/2013

ROUSSEAU Charles, « *Chronique des faits internationaux* », RGDIP, 1986

SIMONET Loïc, « *L'usage de la force dans le cyberespace et le droit international* », Annuaire de droit français international, 2012, 58, pp. 117-143

SUR Serge, « *La résolution 687 (avril 1991) du Conseil de sécurité dans l'affaire du Golfe : problèmes de rétablissement et de garantie de la paix* », Annuaire français de droit international, XXXVII – 1991, éditions du CNRS

TAILLAT Stéphane, « *Un mode de guerre hybride dissymétrique ? Le cyberespace* », éditions Institut de Stratégie Comparée, 2016/1 (n°111), p. 89-106

TRUDEL Pierre, « *Droit du cyberespace* », éditions Thémis, 1997, p. 1-15

Waxman, Matthew C., « *Regulating Resort to Force: Form and Substance of the UN Charter Regime* » (September 21, 2012). European Journal of International Law, Vol. 24, 2013.

Arrêts et Avis Consultatif

Cour International de Justice (C.I.J.)

C.I. J. « *Barcelona Traction, Light and Power Company* », Limited, arrêt, Recueil 1970, p. 3.

C.I.J. « *Activités armées sur le territoire du Congo* » (République démocratique du Congo *c.* Ouganda), arrêt, Recueil 2005, p. 16

C.I.J. « *Activités militaires et paramilitaires au Nicaragua et contre celui-ci* » (Nicaragua *c.* États-Unis d'Amérique), fond, arrêt, Recueil 1986, p. 14

C.I.J. « *Affaire du temple de Préah Vihéar* » (Cambodge *c.* Thaïlande), Fond, Arrêt du 15 juin 1962 : Recueil 1962, p. 6

C.I.J. « *Affaires du Sud-Ouest africain* » (Éthiopie *c.* Afrique du Sud ; Libéria *c.* Afrique du Sud), Exceptions préliminaires, Arrêt du 21 décembre 1962 : Recueil 1962, p. 319

C.I.J. « *Application de la convention internationale sur l'élimination de toutes les formes de discrimination raciale* » (Géorgie c. Fédération de Russie), exceptions préliminaires, arrêt, Recueil 2011, p. 70

C.I.J. « *Application de la convention pour la prévention et la répression du crime de génocide* » (Bosnie-Herzégovine *c.* Serbie-et-Monténégro), arrêt, Recueil 2007, p. 43

C.I.J. « *Licéité de la menace ou de l'emploi d'armes nucléaires* », avis consultatif, Recueil 1996, p. 226

C.I.J. « *Personnel diplomatique et consulaire des États-Unis à Téhéran* », arrêt, Recueil 1980, p. 3.

C.I.J. « *Plates-formes pétrolières* » (République islamique d'Iran c. États- Unis d'Amérique), arrêt, Recueil 2003, p. 161

Cour Permanente de Justice Internationale

C.P.J.I. « *Affaire des concessions Mavrommatis en Palestine du 30 août 1924 »* (Grèce contre Grande-Bretagne), Recueil 1924, Série A - n°2

Sentence arbitrale

« *Sentence arbitrale du 31 juillet 1928 concernant la responsabilité de l'Allemagne à raison des dommages causés dans les colonies portugaises du Sud de l'Afrique* » (Portugal contre Allemagne), sentence arbitrale, recueil des sentences arbitrales, VOLUME II pp. 1011-1033

Tribunal pénal international pour l'Ex-Yougoslavie (T.P.I.Y.)

T.P.I.Y « *Le Procureur c/ Dusko Tadic* », arrêt du 15 juillet 1999

Textes, documents officiels, rapports cités (Convention, Résolutions C.D.I.)

Convention

Charte des Nations unies

Résolutions du Conseil de sécurité (C.S.)

C.S. résolution 687 S/22454 (1991)

C.S. résolution C.S. S/RES/1373 (2001)

Résolutions de l'Assemblée générale des Nations unies (A.G.N.U.)

A.G.N.U résolution A/37/590 (IX),

A.G.N.U résolution A/RES/3314 (XXIX),

A.G.N.U, « *Déclaration sur l'inadmissibilité de l'intervention dans les affaires intérieures des États et la protection de leur indépendance et de leur souveraineté* », Résolution 2131 du 21 décembre 1965

Documents de la Commission du droit international (C.D.I.)

C.D.I., « *Projet d'articles sur la responsabilité de l'État pour fait internationalement illicite* », Documents officiels de l'Assemblée générale, cinquante-sixième session, Supplément n° 10 (A/56/10)

Articles de presse

CHEMILLIER-GENDREAU Monique, Le Monde, « *Dommages de guerres à géométrie variable* », octobre 2003

Le Monde Diplomatique, « *Ingérences russes, de l'obsession à la paranoïa* », 12.2017

Le Monde Diplomatique, Archives de décembre 1986, p. 24-25, https://www.monde-diplomatique.fr/1986/12/CONCHIGLIA/39702

Le Monde Europe, « *L'Estonie tire les leçons des cyberattaques massives lancées contre elle pendant la crise avec la Russie* », 27.06.2007

Le Monde Europe, « *La Russie préparait de longue date la guerre en Géorgie* », 13.08.2012

Le Monde Europe, « *Russie et Géorgie en guerre pour l'Ossétie du Sud* », 05.08.2008

Le Monde Technologies, « *La seule façon de gagner la cyberguerre, c'est de l'éviter* », 03.02.2010

Le Monde, « *États-Unis : la justice poursuite treize russes pour ingérence dans l'élection présidentielle de 2016* », 16.02.2018

Le Monde, « *États-Unis : Poutine promet une riposte après l'attaque contre la chaîne de télévision RT* », 11.11.2017

Le Monde, « *Israël revendique la destruction d'un réacteur nucléaire en Syrie en 2007* », 21.03.2018

Le Monde, « *L'Allemagne attaquée par des hackeurs russes* », 01.03.2018

Le Monde, « *L'Ouganda condamné par la Cour Internationale de Justice pour son action en R.D.C.* », 19 décembre 2005

Le Monde, « *Les risques de cyberattaques contre les centrales nucléaires se multiplient* », 06.10.2015

Le Monde, « *Les sous-marins russes près des câbles transatlantiques inquiètent les Américains* », 26.10.2015

Le Monde, « *Penser la cyberpaix* », 04.2016

Le Monde, « *Washington annonce des sanctions contre Moscou pour son ingérence dans la présidentielle* », 15.03.2018

The Huffington post, « *Ce que nous dit le tableau de chasse de Fancy Bear, les hackers russes qui ont attaqué Macron* », 25.04.2017

Déclaration de l'Union International des Télécommunications (U.I.T.)

Déclaration du Secrétaire Général de l'U.I.T. Houlin Zhao au Conseil de l'U.I.T. de Genève « *State Of the Union Adress* », 15.05.17

Déclaration d'Hamadoun Touré, secrétaire général de l'Union Internationale des Télécommunications, au Forum Mondial de Davos, 2010

Sitographie

Site officiel de l'Assemblée des Nations unies : http://www.un.org/fr/ga/

Site officiel de l'OTAN, https://www.nato.int/cps/fr/natohq/index.htm

Site officiel de l'U.I.T. : https://www.itu.int/fr/pages/default.aspx

Site officiel de la Cour International de Justice : http://www.icj-C.I.J..org/fr

INDEX

A

B

C

D

E

F

G

I

L

N

P

R

S

TABLE DES MATIERES