CERGY PARIS UNIVERSITÉ

---

COUR INTERNATIONALE DE JUSTICE

*Activités et infrastructures numériques*
*Leoni c. Dole*

---

**COMMUNICATION ÉCRITE**

**déposée par**

**la République du Leoni**

Représentantes : Solène FLAMBEAUX - Sarah BYLL

Concours Charles Rousseau – Édition 2022

**SOMMAIRE**

## LISTE DES ABRÉVIATIONS

### Institutions

| | |
|---|---|
| AGNU | Assemblée Générale des Nations Unies |
| AMS | Agence Maritime de Sécurité des systèmes du Leoni |
| CIJ | Cour Internationale de Justice |
| CDI | Commission du Droit International |
| CEDH | Cour européenne des droits de l'homme |
| Cour IADH | Cour interaméricaine des Droits de l'Homme |
| CPJI | Cour Permanente de Justice Internationale |
| CS | Conseil de Sécurité |
| IUSCT | Iran United States Claims Tribunal |
| ONU | Organisation des Nations Unies |
| O.T.A.N. | Organisation du Traité de l'Atlantique Nord |
| TPI-Y | Tribunal Pénal International pour l'Ex-Yougoslavie |
| UNIDIR | United Nations Institute for Disarmament Research (Institut des Nations Unies pour la recherche sur le désarmement) |

### Publications

| | |
|---|---|
| *Ann. CDI* | *Annuaire de la Commission du Droit International* |
| *AFDI* | *Annuaire Français de Droit International* |
| *AFRI* | *Annuaire Français de Relations Internationales* |
| *Eur. J. Int'l L* | *European Journal of International Law* |
| LGDJ | Librairie Générale de Droit et de Jurisprudence |
| PUF | Presses Universitaires de France |
| *RBDI* | *Revue belge de droit international* |
| *RCADI* | *Recueil des Cours de l'Académie de droit international* |
| *RICR* | *Revue Internationale de la Croix-Rouge* |
| *Rec.* | *Recueil de la Cour International de Justice* |
| *RSA* | *Recueil des Sentences Arbitrales* |
| SA | Sentence Arbitrale |
| SFDI | Société Française de droit international |

**Locutions latines et autres abréviations**

| | |
|---|---|
| c. | contre |
| coll. | |
| dir. | Sous la direction de |
| Éd. | Édition |
| GE | *General Editor* (sous la direction de) |
| *Ibid.* | *ibidem* (cité ci-dessus) |
| N° | numéro |
| *Op. cit.* | *opus citatum* (cité précédemment) |
| *Per se* | en soi |
| p. | page |
| pp. | pages |
| § | paragraphe |
| §§ | paragraphes |
| Rés. | Résolution |
| Vol. | *Volume* |

## RÉSUMÉ DES FAITS

**1.** La République du Leoni entretient des relations mouvementées avec son voisin, la République fédérale du Dole, grande puissance économique et à la pointe du numérique et qui prétend défendre les valeurs démocratiques dans le monde. Pays émergent, le Leoni prône sa souveraineté numérique et investit massivement dans ce secteur au point de développer sur son territoire des services concurrents à ceux du Dole.

**2.** Le Dole encourage et soutient les activités d'un collectif d'internautes anonymes dolais, appelé NoVox, actif sur les réseaux sociaux, et notamment sur la plateforme dolaise Echo. NoVox prétend défendre les valeurs démocratiques dans le monde. À l'approche des élections leoniennes au printemps 2020, NoVox publie tous les trois jours des documents internes à l'administration leonienne. Ciblant le président leonien sortant, NoVox perturbe les élections présidentielles du Leoni et organise une large campagne de désinformation, avec le soutien du gouvernement dolais qui ne met pas un terme à ces agissements.

**3.** Le 28 septembre 2020, la cyberadministration leonienne annonce l'implantation d'un logiciel malveillant dénommé « Crépuscule » dans le système de gestion informatique du Port de Vaneti, port principal du Leoni dédié au déploiement d'activités maritimes industrielles et militaires. L'État du Dole reconnaît avoir installé ce logiciel malveillant au Leoni, à l'insu de celui-ci.

**4.** Le 1er octobre 2020, le Leoni procède au cloisonnement du réseau internet sur son territoire, avec l'aide de son fournisseur d'accès LeoWeb. Une erreur de routage prive les internautes, dont les internautes dolais, d'accès aux plateformes de PERK qui est une entreprise dolaise. Rétablie pourtant à la mi-journée, la Présidente du Dole annonce malgré tout l'adoption de sanctions économiques et diplomatiques contre le Leoni.

**5.** Le Leoni saisit la Cour International de Justice (ci-après la Cour) d'une requête introductive d'instance le 25 juillet 2021.

## RÉSUMÉ DES MOYENS

**1.** Premièrement, le Leoni démontrera que la responsabilité internationale du Dole est engagée sur le fondement des *Articles sur la responsabilité de l'État pour fait internationalement illicite*, en raison des activités menées par le collectif NoVox afin d'interférer dans le cours de la campagne électorale leonienne de 2020. En effet, les activités du collectif Novox sont imputables au Dole, et ces activités constituent des faits illicites d'une part, parce qu'elles constituent un non-respect du principe de non-ingérence et d'autre part parce que le Dole a manqué à son obligation de *due diligence* en laissant se dérouler sur son territoire des activités illicites, contraires aux droits du Leoni.

**2.** Deuxièmement, le Leoni établira que la responsabilité internationale du défendeur est engagée du fait de la violation de l'interdiction du recours à la force armée, la cyberattaque commise par le Dole étant constitutive d'une agression armée.
À titre subsidiaire, le Leoni démontrera que l'implantation du programme malveillant « Crépuscule » par le Dole contrevient au principe de non-intervention et entraîne la violation de la souveraineté du Leoni.

**3.** Enfin, le Leoni établira que le Dole engage sa responsabilité du fait de l'illicéité des sanctions qu'il a prises envers le Leoni. En effet, ces sanctions répondent à un acte qui n'est pas illicite, le détournement BGP n'étant pas une cyber attaque, et le Dole contrevient à la *Charte des Nations Unies* en édictant des sanctions unilatérales. Par ailleurs, ces mesures ne peuvent être qualifiées de mesures de rétorsions du fait de leur illicéité.

## OBSERVATIONS ÉCRITES DE LA RÉPUBLIQUE DU LEONI

**1.** La République du Leoni a l'honneur de présenter ses observations à la Cour internationale de Justice (ci-après la « CIJ » ou la « Cour ») dans l'*Affaire des Activités et infrastructures numériques,* consécutivement au dépôt d'une requête introductive d'instance le 25 juillet 2021.
**2.** La Cour est saisie sur le fondement de l'article 36§2 de son *Statut.* Le Leoni et le Dole ont tous les deux effectué une déclaration facultative de juridiction obligatoire et le défendeur n'a pas présenté d'exceptions préliminaires[1]. La Cour est donc compétente et la requête du Leoni recevable.
**3.** La République du Leoni démontrera que la responsabilité internationale du Dole est engagée d'une part, du fait des activités menées par le collectif NoVox afin d'interférer dans le cours de la campagne leonienne de 2020 (Partie 1), et d'autre part, du fait de l'implantation du programme malveillant « Crépuscule » par le Dole dans le port principal du Leoni (Partie 2). Enfin, le Leoni démontrera que les mesures prises par le Dole en réaction au détournement de BGP sont illicites au regard du droit international et engagent sa responsabilité (Partie 3).

### PARTIE 1. LA RESPONSABILITÉ INTERNATIONALE DU DOLE EST ENGAGÉE DU FAIT DES ACTIVITÉS MENÉES PAR LE COLLECTIF NOVOX AFIN D'INTERFÉRER DANS LE COURS DE LA CAMPAGNE ÉLECTORALE LEONIENNE DE 2020

**4.** Conformément aux *Articles sur la responsabilité de l'État pour fait internationalement illicite* (ci-après « *Articles de la CDI* »), « *tout fait internationalement illicite de l'État engage sa responsabilité internationale* »[2]. Deux conditions cumulatives doivent être réunies : ce comportement doit être attribuable à l'État en vertu du droit international et constituer une violation d'une obligation internationale incombant à l'État en question[3].

[1] *Exposé des faits*, annexes 3 et 4.
[2] AGNU, Rés. 56/83, *Responsabilité de l'État pour fait internationalement illicite*, 12 décembre 2001, annexe, article 1.
[3] *Ibid.,* article 2 ; CPJI, arrêt du 13 septembre 1928, *Usine de Chorzów,* série A, n°13, p. 29 ; CIJ, avis consultatif du 11 avril 1949, *Réparation des dommages subis au service des Nations Unies, Rec.* 1949, p. 174, p. 184 ; SA du 30 avril 1990, *Rainbow Warrior* (*Nouvelle-Zélande c. France*), *RSA*, vol. XX, 1990, p. 251, § 75.CRAWFORD (J.), *Les articles de la CDI sur la responsabilité de l'État*, Paris, Pedone, 2003, p.14 ; DAILLIER (P.), FORTEAU (M.), PELLET (A.), *Droit international public*, Paris, LGDJ, 8ème édition, 2009, p. 854 ; MORELLI (G.), *Notions de droit international public*, Paris, Pedone, 7ème édition, 2013, pp. 256 - 257 ; SHAW (M. N.), *International Law*, Cambridge, New-York, Cambridge University Press, 7ème édition, 2014, p. 568 ; COMBACAU (J.), SUR (S.), *Droit international public*, LGDJ, 13ème édition, 2019, p. 580.

**5.** La responsabilité internationale du Dole est engagée du fait des activités menées par le collectif NoVox afin d'interférer dans le cours de la campagne électorale leonienne de 2020. Le Leoni établira premièrement que les activités du collectif NoVox sont imputables au Dole (Chapitre 1) et deuxièmement, que le Dole a violé ses obligations internationales. En effet, ces activités constituent un non-respect du principe de non-ingérence et le Dole a manqué à l'obligation de *due diligence* qui lui incombait en laissant faire NoVox (Chapitre 2).

## CHAPITRE 1. LES ACTIVITÉS DU COLLECTIF NOVOX SONT IMPUTABLES AU DOLE

**6.** Un comportement illicite au regard du droit international peut âtre attribué à l'État et considéré comme consistant en ses propres actions ou omissions, lorsqu'il est considéré comme accompli par un de ses organes[4]. Le comportement d'une personne ou d'un groupe de personnes peut aussi être considéré comme un fait de l'État d'après le droit international si cette personne ou ce groupe de personnes agit en fait sur les instructions, les directives ou sous le contrôle de cet État[5] ou si, après la commission de ce fait, l'État reconnaît et adopte leur comportement[6].
**7.** Le Leoni établira que les activités du collectif NoVox sont imputables au Dole dans la mesure où le Dole exerce un contrôle sur les activités du collectif NoVox (Section 1), et reconnaît et adopte *a posteriori* le comportement du collectif NoVox comme étant le sien (Section 2).

### Section 1. Le Dole exerce un contrôle global sur les activités du collectif NoVox

**8.** Il est considéré que les termes « *instructions* », « *directives* » et « *contrôle* » utilisés dans l'article 8 des *Articles de la CDI* pour imputer à l'État les actes de personnes « *sont disjoints* » et « *il suffit donc d'établir la réalité de l'un d'entre eux* » pour que le dit fait soit imputable à l'État[7]. Bien que la Cour privilégie la théorie du contrôle effectif pour attribuer le comportement

[4] AGNU, Rés. 56/83, *op. cit.*, article 4 ; IUSCT, 18 et 19 février 1987, *Affaire Kenneth P. Yeager c. La République islamique d'Iran,* n° 10199, §37 ; CRAWFORD (J.), *op. cit.*, p. 113 et 115 ; (M.), « L'État selon le droit international : une figure à géométrie variable? », *RDGIP*, 2007, n°2, p. 742 ; SINKONDO (M.), *Droit international public*, Paris, Ellipses, 1999, p. 226 ; KEES (A.), *«* Responsibility of States for private actors *», in* WOLFRUM (R.), *The Max Planck Encyclopedia of public international law*, Oxford University Press, vol. VIII, 2012, p. 959 ; CANAL-FORGUES (E.), RAMBAUD (P.), *Droit international public*, Barcelone, Champs université, 3ème édition, 2016, p. 390 ; DUPUY (P.M.), KERBRAT (Y.), *Droit international Public*, Paris, Dalloz, 15ème édition, 2020, p. 547.
[5] AGNU, Rés. 56/83, *op. cit.*, article 8.
[6] *Ibid.*, article 11.
[7] CDI, « Projets d'articles sur la responsabilité de l'Etat pour fait internationalement illicite et commentaires y relatif », *Ann. CDI*, 2001, vol II, p. 114 ; DUPUY (P.M.), KERBRAT (Y.), *op. cit.*, p. 547.

de personnes privées à l'État[8], le Leoni invite la Cour à considérer le critère du contrôle global dans le cadre du différend qui l'oppose au Dole. Les rapports cybernétiques sont complexes, difficiles à imputer à l'État, et nécessitent d'être envisagés de la façon la plus large possible. Les critères du contrôle effectif dégagés par la Cour doivent être écartés au risque de permettre au Dole de se soustraire de sa responsabilité car ils sont trop stricts[9] et mal adaptés aux évènements particuliers[10] tels que l'ubiquité des activités effectuées sur Internet[11]. L'ère des cyber technologies et les menaces que représentent les activités du collectif NoVox rappellent ainsi que le droit international est nécessairement soumis à des fortes mutations et doit s'adapter en décloisonnant « *les catégories classiques sur lesquelles il s'est édifié* »[12] pour régler les litiges en accord avec notre temps et Internet[13].

**9.** Le critère du contrôle global permet de mieux prendre en considération la réalité de la relation entre le groupe et l'État[14] puisque l'imputabilité à l'État est rendu difficile du fait de la quantité de données à analyser et de leur dématérialisation[15]. La majorité des juridictions internationales et régionales privilégient par ailleurs le critère du contrôle global[16]. Il exige l'exercice d'une

---

[8] CIJ, arrêt du 27 juin 1986, *Affaire des activités militaires et paramilitaires au Nicaragua et contre celui-ci (Nicaragua c/ Etats-Unis d'Amérique)*, *Rec.* 1986, p.14, § 115.

[9] ASCENSIO (H), « La responsabilité selon la Cour internationale de Justice dans l'affaire du génocide bosniaque », *RGDIP*, 2007, pp. 290-292 ; SOREL (J.M.), « Les multiples lectures d'un arrêt : entre sentiment d'impunité et sentiment de cohérence, une décision à relativiser », *RGDIP*, 2007, p. 260 ; WECKEL (P.), « L'arrêt sur le génocide : le souffle de l'avis de 1951 n'a pas transporté la Cour », *RGDIP*, 2007, p. 317 ; FERRARO (T.), « La position juridique du CICR sur la qualification des conflits armés incluant une intervention étrangère et sur les règles du DIH applicables à ces situations », *RICR*, vol. 97, Sélection française 2015, p. 193.

[10] CIJ, arrêt du 26 février 2007, *Application de la convention pour la prévention et la répression du crime de génocide (Bosnie- Herzégovine c. Serbie et Monténégro)*, *Rec.* 2007, p. 43, opinion dissidente du juge AL-KHASAWNEH, p. 217, § 39.

[11] WOLTAG (J.-C.), *«* Internet *», in* WOLFRUM (R.), *The Max Planck Encyclopedia of public international law*, Oxford, Oxford University Press, vol. VI, 2012, p. 237 ; TURK (P.), VALLAR (C.) (dir.), *La souveraineté numérique, le concept, les enjeux*, Mare & Martin, 2017, p. 49 ; BESSON (S.), *La due diligence en droit international*, La Haye, Brill, Nijhoff, vol.46, 2021, p. 262 ; SZPUNAR (M.), « Territoriality of Union Law in the Era of Globalisation », *in* PETRLIK (D.), BOBEK (M.), PASSER (J.), MASSON (A.) (dir.), *Évolution des rapports entre les ordres juridiques de l'Union européenne, international et nationaux* : *liber Amicorum Jiří Malenovský*, Bruxelles, Bruylant, 2020, p. 149

[12] TOURME-JOUANNET (E.), *Le droit international,* Paris, P.U.F*,* 2013, p. 70.

[13] *Ibid.*, p. 70.

[14] CIJ, arrêt du 26 février 2007, *Application de la Convention pour la prévention et la répression du crime de génocide (Bosnie-Herzégovine c. Serbie-et-Monténégro)*, *op. cit.*, Opinion dissidente du juge MAHIOU, pp. 447 -449 ; CORTEN (O.), « L'arrêt rendu par la CIJ dans l'affaire du Crime de génocide (Bosnie-Herzégovine c. Serbie) : vers un assouplissement des conditions permettant d'engager la responsabilité d'un État pour génocide ? », *AFDI*, vol. 53, 2007, pp. 249-279 ; ASCENSIO (H.), *op. cit*., p. 302.

[15] CONDE (P. Y.), « L'Affaire du génocide : Bosnie et Serbie devant la Cour internationale de Justice ou la dénonciation à l'épreuve du droit international », *Droit et cultures*, 2009 - 2, p. 17, p. 140 ; YUYING LIU (I.), « La doctrine de la diligence raisonnable en vertu du Manuel de Tallinn 2.0 », *Computer Law and Security Review,* vol. 33, avril 2017, p. 394.

[16] TPI-Y, arrêt du 15 juillet 1999, *Le Procureur c. Dusko Tadic*, n°IT-94-1-A, §117, p. 49 ; CPI, arrêt du 29 janvier 2007, *Le Procureur c. Thomas Lubanga Dyilo*, § 210 ; CEDH, arrêt du 18 décembre 1996, *Loizidou c. Turquie*, fond, , pp. 2235 - 2236, § 56; arrêt du 10 mai 2001, *Chypre c. Turquie*, n o 25781/94, §77 ; IUSCT, 18 et 19 février 1987, *Affaire Kenneth P. Yeager c. La République islamique d'Iran*, n° 10199, §38, 42, 44 et 45; Cour IADH, 27 juin 2012, *Affaire du Peuple autochtone Kichwa de Sarayaku c. Équateur, Mérites et réparations*, Series C No.

certaine forme d'autorité sur l'entité considérée, « *qui est plus large et plus générale que le simple fait d'émettre des ordres et fait plutôt allusion à la direction et à la coordination générale des opérations en cause* »[17]. Le degré de ce contrôle varie en fonction des faits et circonstances de chaque cause[18] et implique de vérifier l'existence d'une relation de fait entre l'entité ou le groupe de personnes et l'État[19], c'est-à-dire si le soutien apporté ou le contrôle exercé sur des particuliers par un État permet de considérer que ceux-ci agissent « *en son nom* »[20].

**10.** En l'espèce, les activités de NoVox sont dématérialisées. Il existe une relation de fait évidente entre le collectif NoVox, qui s'est toujours présenté dans ses publications numériques comme constitué de citoyens dolais, et le Dole, dans la mesure où ce dernier a grandement participé à l'ascension du collectif NoVox sur les réseaux sociaux en lui offrant visibilité, encouragement, bénédiction, et en lui fournissant un soutien opérationnel. Le Secrétaire d'État du Dole avait déjà encouragé et félicité NoVox pour ses activités[21] et republié plusieurs fois sur son compte public *Echo* des révélations de NoVox relatives aux élections leoniennes[22]. De plus, invité dans l'émission phare d'une chaîne internationale le 1er juillet 2020, il a confirmé l'exactitude des informations publiées par NoVox[23]. Du fait de leur connexité et relation, il est indéniable que les activités de NoVox doivent être attribuées au Dole.

**11.** Au regard de ces éléments, le Dole exerce un contrôle global sur le collectif NoVox.

Section 2. Le Dole reconnaît et adopte le comportement du collectif NoVox

245 ; CASSESE (A.), « Les tests du Nicaragua et de Tadic réexaminés à la lumière de l'arrêt de la CIJ sur le génocide en Bosnie », *Eur. J. Int'l L,* vol 18, 2007, p. 653 ;DUPUY (P.M.), KERBRAT (Y.), *op. cit.,*p. 548.

[17] TPI-Y, arrêt du 15 juillet 1999, *Le Procureur c. Dusko Tadic*, *op. cit.*, § 131 ; FERRARO (T), « La position juridique du CICR sur la qualification des conflits armés incluant une intervention étrangère et sur les règles du DIH applicables à ces situations », *RICR,* Vol. 97 Sélection française 2015 /4, p. 191.

[18] TPI-Y, arrêt du 15 juillet 1999, *Le Procureur c. Dusko Tadic*, *op. cit.*, §117 ; CDI, « Projets d'articles sur la responsabilité de l'Etat pour fait internationalement illicite et commentaires y relatif », *op. cit.*, p. 112 ; CRAWFORD (J.), *op. cit.*, p. 112 ; ASCENSIO (H.), *op. cit.*, p. 289 ; TOUGAS (M.-L.), « Commentaire de la Partie 1 du Document de Montreux sur les obligations juridiques pertinentes et les bonnes pratiques pour les États en ce qui concerne les opérations des entreprises militaires et de sécurité privées pendant les conflits armés », *RICR*, 2014 / 1, vol. 96, p. 268 ;RIVIER (R.), *Droit international public,* Paris, PUF, 3ème édition, 2017, p. 721.

[19] CDI, « Projets d'articles sur la responsabilité de l'Etat pour fait internationalement illicite et commentaires y relatif », *op. cit.*, p. 109.

[20] CIJ, arrêt du 27 juin 1986, *Affaire des activités militaires et paramilitaires au Nicaragua et contre celui-ci*, *op. cit.*, §109 ; VERHOEVEN (J.), *Droit international public*, Bruxelles, Larcier, 2000, p. 623 ; GRANT (J.P.), CRAIG BARKER (J.), PARRY (C.), *Parry and Grant Encyclopaedic dictionary of International Law,* Oxford, New-York, Oxford University Press, 3ème édition, 2009, p. 51.

[21] *Exposé des faits*, § 13.

[22] *Ibid.*, §18.

[23] *Ibid.*

**12.** À titre subsidiaire, le Leoni établira que les actions menées par NoVox lui sont attribuables dans la mesure où il a reconnu et adopté celles-ci comme étant siennes. Les actes de personnes privées peuvent être attribuées à l'État lorsque celui-ci reconnaît et adopte ultérieurement ces actes comme étant siens[24]. Cette approbation n'a « *pas besoin d'être exprimée formellement* »[25] :la reconnaissance et l'adoption par l'État des actes d'entités privées peuvent être tacitement formulées par ce dernier ou s'illustrer à travers le comportement de ses organes[26] notamment par le maintien par l'État d'une infraction ou d'une situation engendrée qui est contraire au droit international[27]. Le Leoni rappelle que l'État peut être engagé du fait des déclarations d'un de ses agents, notamment lorsque cet agent fait une déclaration dans un domaine qui relève de sa compétence[28]. La forme de ces déclarations n'est pas décisive et doivent être pris en compte l'intention, les circonstances et le contexte de la déclaration[29].

**13.** En l'espèce, confronté aux faits illicites commis par le collectif NoVox menés depuis son territoire et violant les droits du Leoni, le Dole non seulement n'a pas agi pour empêcher la violation les droits du Leoni, mais a endossé *a posteriori* les actions du collectif NoVox à travers les déclarations du Secrétaire d'État Mike Richard. Ce dernier est un agent représentant le Dole qui avait déjà publiquement présenté la stratégie de défense et de sécurité numérique du Dole[30]. Le Dole ne s'est contenté pas de reconnaître les actes commis par NoVox et d'approuver explicitement ces derniers. Le défendeur a pris une position claire et sans équivoque en faveur

---

[24] AGNU, Rés. 56/83, *op. cit.*, article 11 ; CDI, « Projets d'articles sur la responsabilité de l'Etat pour fait internationalement illicite et commentaires y relatif », *op. cit.,* pp. 125 et 128 ; SHAW (M. N.), *op. cit.*, p. 576 ; CANAL-FORGUES (E.), RAMBAUD (P.), *op. cit.*, p. 410.

[25] AGO (R.), « Quatrième rapport sur la responsabilité des États », *Ann. CDI*, vol. II., 1972, p.110 *;* DE FROUVILLE (O.) « L'attribution d'un fait à l'Etat - Les personnes privées », *in* BODEAU (P.), CRAWFORD (J.), PELLET (A.), SZUNEK (S.) (dir.), *Le droit de la responsabilité internationale*, Paris, 2016, https://www.frouville.com/wp-content/uploads/2020/05/FROUVILLE-RESPONSABILITE-1.pdf: p. 22.

[26] CIJ, arrêt du 24 mai 1980, *Affaire relative au personnel diplomatique et consulaire des Etats-Unis et Téhéran (Etats-Unis d'Amérique c. Iran), Rec.* 1980, p. 3, §§ 57, 61 et 64 ; IUSCT, 18 et 19 février 1987, *Affaire Kenneth P. Yeager c. La République islamique d'Iran*, *op. cit.* §66 ; CDI, « Projets d'articles sur la responsabilité de l'Etat pour fait internationalement illicite et commentaires y relatif », *op. cit.*, p. 128

[27] CIJ, arrêt du 24 mai 1980, *Affaire relative au personnel diplomatique et consulaire des Etats-Unis et Téhéran*, *op. cit,* § 91; avis consultatif du 25 février 2019, *Effets juridiques de la séparation de l'archipel des Chagos de Maurice en 1965*, *Rec.* 2019, p. 95, § 177 ; SA du 24/27 juillet 1956, *Affaire relative à la concession des phares de l'Empire ottoman (Grèce c. France), RSA*, vol. II, p. 191; CDI, « Projets d'articles sur la responsabilité de l'Etat pour fait internationalement illicite et commentaires y relatif », *op. cit.,* pp. 126 et 128 ; DE FROUVILLE (O.), *op. cit.*, p. 23 ; SINKONDO (M.), *op. cit.*, p. 222.

[28] CIJ, arrêt du 3 février 2006, *Activités armées sur le territoire du Congo (nouvelle requête :2002) (République démocratique du Congo c. Rwanda),* compétence et recevabilité, *Rec.* 2006, p.6, § 47 ; CDI, « Principes directeurs applicables aux déclarations unilatérales des États susceptibles de créer des obligations juridiques et commentaires y relatifs », *Ann. CDI,* 2006, vol. II (2), p. 393 ; DUPUY (P.M.), KERBRAT (Y.), *op. cit.*, p. 547 ; FORTEAU (M.), *op. cit.*, p. 750.

[29] CIJ, arrêt du 26 mai 1961, T*emple de Préah Vihéar (Cambodge c. Thaïlande),* exceptions préliminaires, *Rec.* 1961, p. 31 ; arrêt du 22 décembre 1986, *Affaire du différend frontalier (Burkina Faso c. République du Mali), Rec.* 1986, p. 573, §39, CDI, « Principes directeurs applicables aux déclarations unilatérales des États susceptibles de créer des obligations juridiques et commentaires y relatifs », *op. cit.*, pp. 388, 394 et 396.

[30] *Exposé des faits*, § 11.

de leurs activités, et allant jusqu'à considérer que NoVox promeut à l'internationale les valeurs démocratiques défendues par le Dole[31]. Il a ainsi activement soutenu les activités de NoVox, et ce malgré la publication du rapport de Geo-Aphe[32], société composée d'experts dont la spécialité est l'analyse de données permettant d'identifier les manipulations de données en lignes et notamment celles visant à déstabiliser les États[33], qui démontre la campagne de désinformation menée par NoVox contre le Leoni[34].

**14.** Par conséquent, le Dole reconnaît et adopte les activités du collectif NoVox.

**15.** Au regard de tout ce qui précède, le Leoni prie la Cour de dire et juger que les activités menées par le collectif NoVox sont imputables au Dole.

## CHAPITRE 2. LE DOLE N'A PAS RESPECTÉ LE PRINCIPE DE NON-INGÉRENCE QUI LUI INCOMBAIT AINSI QUE SON OBLIGATION DE *DUE DILIGENCE*

**16.** La qualification du fait de l'État comme internationalement illicite relève du droit international[35]. La violation du droit international n'est établie que si elle peut être considérée comme ayant été commise par un sujet relevant de cet ordre, qui se voit à la fois destinataire de l'obligation violée et capable de se voir imputer un tel fait[36]. Ainsi, il y a violation d'une obligation internationale par un État lorsque son acte n'est pas conforme à ce qui est requis de lui en vertu de cette obligation[37], qu'elle soit de nature conventionnelle ou coutumière[38]. À ce jour, s'il n'existe pas de norme contraignante encadrant les cyber activités coercitives visant à influencer l'attitude de l'électorat à l'égard d'un candidat[39], un certain nombre de travaux doctrinaux offrent une position intéressante en la matière en se fondant sur des obligations et principes internationaux bien établis en droit tel que le respect de la souveraineté des États. Parmi ses travaux, se trouvent les travaux d'un comité d'experts internationaux spécialisés notamment en droit des conflits armés : leurs travaux ont été rendus sous l'égide de

[31] *Ibid.*, § 13.
[32] *Ibid.*, § 30.
[33] *Ibid.*, § 27.
[34] *Ibid*., § 28.
[35] AGNU, Rés. 56/83, *op. cit.*, article 3.
[36] DUPUY (P.M.), KERBRAT (Y.), *op. cit.*, p. 545.
[37] AGNU, Rés. 56/83, *op. cit.*, article 12.
[38] CIJ, arrêt du 25 septembre 1997, *Affaire relative au projet Gabčíkovo-Nagymaros (Hongrie c. Slovaquie)*, *Rec*. 1997, p.7, §52 ; DAILLIER (P.), FORTEAU (M.), PELLET (A.), *op. cit.*, p. 859 ; CANAL-FORGUES (E.), RAMBAUD (P.), *op. cit.*, p. 396.
[39] TALBOT JENSEN (E.), « The Tallin Manual 2.0: Highights and insights », *Georgetown Journal of International Law,* 2017*,* vol. 48, p. 778 ; SCHMITT (M. N.), « Foreign Cyber Interference in Elections »*, International Law Studies,* 2021, vol. 97, p. 313.

l'Organisation du Traité de l'Atlantique Nord (ci-après « OTAN »)[40], organisation dont l'État défendeur est membre[41]. Ces auteurs considèrent que les États exercent leur souveraineté dans l'espace numérique qui est nécessairement compris dans la souveraineté territoriale de l'Etat puisque le cyberespace est lié à son territoire sur lequel sont situés les technologies de l'information et communication[42]. De nombreux États prolongent donc déjà leur souveraineté dans le cyberespace[43], ce qui est également le cas du défendeur[44]. Il revient ainsi aux États d'éliminer toute ingérence indue dans leurs affaires internes et externes, ce y compris dans le contexte cybernétique,[45] permettant entre autres de préserver l'intégrité des processus électoraux[46].

**17.** Le Leoni démontrera ainsi que le Dole n'a pas respecté le principe de non-ingérence du fait des activités menées par NoVox qui lui sont imputables (Section 1) et a manqué à l'obligation de *due diligence* qui lui incombait en n'empêchant pas les actions de NoVox (Section 2).

## Section 1. Le Dole n'a pas respecté le principe de non-ingérence

**18.** L'interdiction d'intervenir dans les affaires internes ou externes d'un autre État qui relèvent essentiellement de sa compétence nationale est un principe fondamental des relations internationales[47] et une règle coutumière[48]. Cette interdiction est à la fois fondée sur l'indépendance des États, le respect de leur souveraineté nationale et de leur intégrité

---

[40] SCHMITT (M. N) (GE), *Tallinn Manual on the international law applicable to cyber warfare,* Cambridge, Cambridge University Press 2013 ; SCHMITT (M. N.) (GE), *Tallinn Manual 2.0 on the International Law applicable to cyber operations,* Cambridge, Cambridge University Press, 2017.

[41] *Exposé des faits*, § 37.

[42] AGNU, A/70/174, *Rapport du Groupe d'experts gouvernementaux chargé d'examiner les progrès de la téléinformatique dans le contexte de la sécurité internationale*, 22 juillet 2015, p. 14 ; BESSON (S.), *op. cit.*, pp. 265-266.

[43] EHRIEL (C.), « Souveraineté et innovation : trouver l'équilibre », *in* BLANDIN-OBERNESSER (A.) (dir.), *Droits et souveraineté numérique en Europe*, Bruxelles, Bruylant, 2016, p. 92 ; (P.), VALLAR (C.) (dir.), *La souveraineté numérique, le concept, les enjeux*, Paris, Mare & Martin, 2017, p. 31 et 32

[44] *Exposé des faits*, §§ 9-12.

[45] AGNU, A/70/174, *op. cit.*, pp. 5-7

[46] Observation électorale et l'appui à la démocratie, *Recueil des normes internationales pour les élections*, Luxembourg, Office des publications de l'Union Européenne, 4ème éd., 2016, p. 27

[47] AGNU, Rés. 2625 (XXV), *Déclaration relative aux principes du droit international touchant les relations amicales et la coopération entre les Etats conformément à la Charte des Nations Unies*, 24 octobre 1970 ; VERHOEVEN (J.), *op. cit.,* p. 144 ; CARREAU (D.), MARRELLA (F.), *Droit international public*, Paris, Pedone, 12ème édition, 2018, p. 331 ; DECAUX (E.), DE FROUVILLE (O.), *Droit International Public*, Dalloz, 12ème édition, 2020, p. 12.

[48] CPJI, arrêt du 7 septembre 1927, *Affaire du Lotus*, Série A, n°10, p.18 ; CIJ, arrêt du 9 avril 1949, *Affaire du Détroit de Corfou (Royaume-Uni de Grande-Bretagne et d'Irlande du Nord c. Albanie), Rec.* 1949, p.4, p. 35 ; arrêt du 27 juin 1986, *Affaire des activités militaires et paramilitaires au Nicaragua et contre celui-ci*, *op. cit.*, §202 ; ordonnance du 22 novembre 2013*, Certaines activités menées par le Nicaragua dans la région frontalière (Costa Rica c. Nicaragua)*, *Rec.* 2013, p. 354, § 26 ; arrêt du 9 février 2022, *Affaire Activités armées sur le territoire du Congo (République démocratique du Congo c. Ouganda),* § 65; VERHOEVEN (J.), *op. cit.*, p. 350 ; RIVIER (R.), *op. cit.,* p. 277 ; CARREAU (D.), MARRELLA (F.), *op. cit.*, p. 380.

politique[49], ainsi que sur le principe d'égalité des États[50], tel qu'énoncé dans l'article 2§1 de la *Charte des Nations-Unies* (ci-après « *Charte* »)[51].

**19.** La souveraineté territoriale d'un État est exclusive et absolue[52]. Elle est indissociable de son indépendance[53] et implique que l'État exerce sa compétence nationale ou réservée comme son système politique[54], sans interférence extérieure[55], et ce y compris à travers des moyens cybernétiques[56]. Ainsi, et conformément à l'article 2 § 7 de la *Charte*, nul ne peut s'immiscer dans les domaines que le droit international reconnaît comme relevant exclusivement des Etats sans leur accord[57]. L'ingérence est donc prohibée en droit internationale. Elle consiste en tout acte d'un État interférant avec la conduite des affaires intérieures d'un État tiers, sans nécessaire

---

[49] AGNU, Rés. 36/103, *Déclaration sur l'inadmissibilité de l'intervention et de l'ingérence dans les affaires intérieures de l'Etat*, 9 décembre 1981, p. 1 ; VERHOEVEN (J.), *op. cit.*, p. 125.

[50] DAILLIER (P.), FORTEAU (M.), PELLET (A.), *op. cit.*, p. 472 ; ALEDO (L.-A.), *Le droit international public*, Dalloz, 4ème édition, 2021 p. 39.

[51] *Charte des Nations-Unies*, adoptée le 26 juin 1945 à San Francisco, entrée en vigueur le 24 octobre 1945, Article 2 § 1.

[52] SALMON (J.) (dir.), *Dictionnaire de droit international public*, Bruxelles, Bruylant, 2001, p. 1045 ; FLEURY GRAFF (T.), *Manuel de droit international public*, Paris, PUF, vol. II, 1ère édition, 2016, p. 31 ; SINKONDO (M.), *op. cit.*, p. 270.

[53] SA du 4 avril 1928, *Affaire de l'Île de Palmas, Pays-Bas c/ Etats-Unis d'Amérique*, *RSA*, vol.II, p. 838 ; SINKONDO (M.), *op. cit.* p. 360 ; VERHOEVEN (J.), *op. cit.*, p. 126 ; DAILLIER (P.), FORTEAU (M.), PELLET (A.), *op. cit.*, p. 467 ; BESSON (S.), *«* Sovereignty *», in* WOLFRUM (R.), *op. cit.*, p. 382 ; BLIN (O.), *Droit International public général*, Bruylant, 2ème édition, 2019, p. 51.

[54] AGNU, Rés. 2131 (XX), *Déclaration sur l'inadmissibilité de l'intervention dans les affaires intérieures des États et la protection de leur indépendance et de leur souveraineté*, 21 décembre 1965, §3 ; Rés. 2625 (XXV), *op. cit.*; CPJI, avis consultatif du 7 février 1923*, Décrets de nationalité promulgués en Tunisie et au Maroc,* Série B. n°4, pp. 22-23 ; CIJ, arrêt du 27 juin 1986, *Affaire des activités militaires et paramilitaires au Nicaragua et contre celui-ci, op. cit.,* § 288 ; SA du 4 avril 1928, *Affaire de l'Île de Palmas, (Pays-Bas c/ États-Unis d'Amérique)*, *RSA,* vol.II, p. 838 ; SA du 1er mai 1925, *Affaire des Réclamations britanniques dans la zone espagnole du Maroc, (Grande Bretagne c. Espagne*), *RSA*, vol. II, p. 649 ; CDI, *La commission du droit international et son œuvre – septième édition*, New-York, Nations Unies, vol. I, 2009, p. 303 ; SINKONDO (M.), *op. cit.*, p. 270 ; FLEURY GRAFF (T.), *op. cit.*, p.31; CRAWFORD (J.), KOSKENNIEMI (M.), *The Cambridge Companion to International Law*, Cambridge, Cambridge University Press, 2012, p. 120 ; CONFORTI (B.), « Le principe de non-intervention » *in* BEDJAOUI (M.) (dir.), *Droit international : bilan et perspectives*, Paris, Pedone, 1991, p. 492.

[55] AGNU, Rés. 2131 (XX), *op. cit.*, §3 ; Rés. 26/25 (XXV), *op. cit.* ; CPJI, arrêt du 7 septembre 1927, *Affaire du « Lotus », Série A, n°10*, p. 18 ; SALMON (J.), *op. cit.*, p. 770 et p.1045 ; DAILLIER (P.), FORTEAU (M.), PELLET (A.), *op. cit.*, p. 486 ; DUPUY (P.-M.), KERBRAT (Y.), *op. cit.*, p. 92 ; COMBACAU (J.), SUR (S.), *op. cit.*, p. 272 ; TALBOT JENSEN (E.), *op. cit.*, p.775.

[56] AGNU, A/70/174, *op. cit.*, §27 ; Rés. 73/27, *Progrès de l'informatique et des télécommunications et sécurité internationale*, 5 décembre 2018 ; p. 3 ; SCHMITT (M. N.) (GE), *Tallinn Manual 2.0 on the International Law applicable to cyber operations, op. cit.*, p. 312 ; SCHMITT (M. N.), « Foreign Cyber Interference in Elections *», op. cit.*, p. 744 ; O.T.A.N., « Trends in international law for cyberspace », CCDCOE Nato Cooperative Cyber defence centre of excellence, mai 2019, p. 1 ; SCHONDORF (R.) « Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations », *International Law Studies*, 2021, vol. 97 p. 403.

[57] CPJI, avis consultatif du 7 février 1923, *Décrets de nationalité promulgués en Tunisie et au Maroc, op. cit.*, p. 25 ; ROUSSEAU (C.), « L'indépendance de l'État dans l'ordre international », *RCADI*, 1948, vol. 73, p. 71 ; SINKONDO (M.), *op. cit.*, p. 338 ; PREUSS (L.), *«* Article 2, paragraph 7 of the Charter of the United Nations and Matters of domestic juridiction *», RCADI*, vol. I, tome 74, 1949, p. 556 ; VERHOEVEN (J.), *op. cit.*, p. 148 ; SALMON (J.), *op. cit.*, p. 356 ; CANAL-FORGUES (E.), RAMBAUD (P.), *op. cit.*, p. 192 ; RIVIER (R.), *op. cit.*, p. 277 ; FLORY (M.), « Souveraineté », *Répertoire de droit international*, décembre 1998 (actualisation : juin 2015), § 10.

emploi de la force[58]. Cela revient à s'immiscer sans en avoir le droit dans les affaires des autres[59].

**20.** Une interférence qui vise à influencer la conduite des affaires internes d'un État et à porter atteinte à la stabilité de son gouvernement est une ingérence illicite[60]. Elle peut prendre la forme d'une pression politique par exemple et n'implique pas nécessairement l'utilisation de moyens militaires[61]. L'application du principe de non-ingérence dans le contexte cybernétique[62] permet de prévenir l'avènement de « *menaces hybrides* » qui perturbent le bon déroulement des processus électoraux[63] en privant un nombre important d'électeurs ou en causant le dysfonctionnement des élections. Ces opérations sont considérées comme coercitives[64], leur pour but étant de fragiliser la souveraineté des États et de les déstabiliser[65]. Ces formes de déstabilisation moderne que sont la diffusion d'informations erronées ou déformées et les opérations de campagnes de désinformation et de diffamation consistent à délibérément tromper le public et à influer sur son choix électoral, afin d'influencer la politique de l'État ciblé[66].

**21.** Les États ne doivent donc pas s'immiscer dans les affaires des États tiers à l'aide des technologies de l'information et des communications, ni mener ou soutenir une activité informatique qui est contraire aux obligations qu'il a contractées en vertu du droit international[67]. L'interférence dans les élections d'un autre État revient à s'immiscer dans le domaine réservé de l'État victime alors que la capacité de mener à bien des élections renvoie à la compétence souveraine et à ses affaires intérieures[68]. Chaque État doit rester libre de décider

---

[58] AGNU, Rés. 2131 (XX), *op. cit.*, §1 ; CONFORTI (B.), *op. cit.*, 492

[59] AGNU, Rés. 36/103, *op. cit.*, p. 98 ; SALMON (J), *op. cit.*, p. 579

[60] KUNIG (P.), *«* Intervention, Prohibition of *», in* WOLFRUM (R.), *op. cit.*, p. 293 ; RIVIER (R.), *op. cit.*, p. 280

[61] SCHMITT (M. N.), « Foreign Cyber Interference in Elections »*, op. cit.*, pp 745-746

[62] AGNU, Rés. 70/174, *op. cit.*, p.4; Rés. 73/27, *op. cit.*, p.3.

[63]TALBOT JENSEN (E.), *op. cit.*, p.746

[64] SCHMITT (M. N.), « Foreign Cyber Interference in Elections »*, op. cit.*, p. 313

[65] FRANCESCHINI (L.), *Analyse juridique de la proposition de la loi française relative à la lutte contre la manipulation de l'information au regard des principes internationaux régissant la liberté de l'information,* novembre 2018 ; NDIOR (V.), *Dictionnaire de l'actualité internationale*, Paris, Pedone, 2021, p. 181 ; « Slovénie : démission du Premier Ministre et déstabilisation du pays », *Visegrad Post*, 15 mars 2018.

[66] AGNU, Rés. 36/103, *op. cit.*, p. 100 ; Rés. 73/27, *op. cit.*, p.3 ; Commission Européenne, *Plan d'action contre la désinformation, Communication conjointe au Parlement européen, au Conseil européen, au Conseil, au Comité économique et social européen, et au Comité des régions*, Bruxelles, 5 décembre 2018 ; GEBEL (M.), « Misinformation vs. Disinformation: What to Know about Each Form of False Information, and How to Spot Them Online », *Business Insider*, 15 Janvier 2021 ; SCHMITT (M. N.), « Foreign Cyber Interference in Elections », *op. cit.*, pp.745-746 ; « Déstabilisation du Venezuela, une opération de piraterie internationale », *Sputnik France*, 22 mars 2019.

[67] AGNU, A/70/174, *op. cit.*, § 13 (c) et (f); Rés. 73/27, *op. cit.*, §1.3.

[68] PREUSS (L.), *op. cit.*, p. 556 ; VERHOEVEN (J.), *op. cit*, p. 103 ; GUILLAUME (G.), « Article 2, § 7 » *in* COT (J.P.), FORTEAU (M.), PELLET (A.) (dir.), *La Charte des Nations Unies, Commentaire article par article*, Economica, 3ème édition, vol. I, p. 498.

des conséquences données à l'atteinte portée à ce qu'il estime être ses droits dans une situation donnée[69].

**22.** La capacité du Leoni de mener à bien ses élections relève de sa compétence souveraine et pourtant, dès le 6 avril 2020, le collectif NoVox s'est livré sur les réseaux sociaux à une campagne de désinformation en publiant tous les trois jours des documents internes à l'administration leonienne et qui dépeignent un invraisemblable complot du candidat Wigram pour écarter son principal adversaire politique, pourtant déjà présenté comme largement favori par l'ensemble des observateurs internationaux[70]. La société Geo-Aphe, spécialisée dans l'analyse des opérations d'influence sur les réseaux sociaux, a dénoncé la création, par NoVox, de plus de 4 000 comptes factices qui ont contribué à cette campagne de désinformation et la plateforme *Echo* a annoncé avoir supprimé des milliers de publications émanant de plus de 10 000 comptes factices liés à la campagne « *VigramLeaks* »[71]. Cette campagne de désinformation a visé à influencer l'attitude du corps électoral leonien, à nuire à la crédibilité de la campagne électorale leonienne et constitue donc une cyber opération coercitive. Elle a en effet privé l'électorat leonien d'un nombre important d'électeurs en conséquence des affabulations du collectif NoVox pour lequel il a été confirmé qu'il a dangereusement créé un nombre immuable de faux profils d'utilisateurs, et ce avec la « *bénédiction du gouvernement dolais* »[72]. Le Dole a sciemment permis que son territoire soit utilisé pour commettre une grave ingérence dans les affaires internes du Leoni à l'aide de technologies de l'information et des communications, et a soutenu une activité informatique contraire à ses obligations internationales. Par conséquent, il ne fait aucun doute que les activités de NoVox, imputables au Dole[73], ont perturbé le bon déroulement des élections présidentielles leoniennes, et constituent une ingérence dans les affaires internes du Leoni, et violent sa souveraineté nationale.

**23.** Au regard des précédents éléments, le Leoni invite donc la Cour à dire et juger que le Dole contrevient au principe de non-ingérence.

[69] DUPUY (P.M.), KERBRAT (Y.), *op. cit.*, p.18.
[70] *Exposé des faits*, §16.
[71] *Ibid.,* § 28.
[72] *Ibid.*, §19.
[73] V. *supra*, §§ 8-13.

Section 2. Le Dole n'a pas respecté l'obligation de due diligence qui lui incombait

**24.** Le droit international est fondé sur le principe de l'égalité souveraine des États[74], chaque État ayant ainsi le devoir de respecter la personnalité des autres États[75]. La Cour a précisé que le droit coutumier impose aux États de veiller à ce que des activités se déroulant sur son territoire ne portent pas atteinte aux droit d'autres d'États[76]. L'État doit donc faire cesser toute activité illicite qui se déroule sur son territoire, que cette activité soit menée par l'État lui-même ou par d'autres entités[77]. La responsabilité de l'État qui laisse utiliser son territoire aux fins d'actes contraires aux droits d'autres États est ainsi engagée, que cela résulte d'un défaut de prévention ou de contrôle du territoire sous sa juridiction ou sous son contrôle, ou bien d'une négligence de la part de ses organes[78].

**25.** Deux situations permettent d'engager la responsabilité de l'État dans ce cadre: soit l'État était en mesure de s'acquitter de ses obligations mais n'a pas agi, soit l'État n'a pas puni les auteurs de l'acte illégal et les a approuvés[79]. L'obligation de vigilance est donc composée d'une obligation de prévention et d'une obligation de répression des actes illicites[80] : la responsabilité internationale d'un État est engagée dès lors qu'il est démontré qu'il n'a pas mis tout en œuvre pour empêcher ou réprimer, voire a encouragé et soutenu une situation ou une action contraire au droit international[81] pour laquelle il a ou aurait dû avoir connaissance[82] ou prévoir raisonnablement[83].

---

[74] *Charte des Nations-Unies*, *op. cit.*, article 2§1.
[75] AGNU, Rés. 2131 (XX), *op. cit.*, § 1 ; DECAUX (E.), DE FROUVILLE (O.), *op. cit.*, p. 205 ; FLEURY GRAFF (T.), *op. cit.*, p. 31 ; FLORY (M.), « Souveraineté », *Répertoire de droit international*, décembre 1998 (actualisation : juin 2015), § 9 ; YUYING LIU (I.), *op. cit.*, p. 392.
[76] CIJ, arrêt du 9 avril 1949, *Affaire du Détroit de Corfou, op. cit.*, p. 22 ; arrêt du 20 avril 2010, *Affaire relative aux Usines de pâte à papier sur le fleuve Uruguay (Argentine c. Uruguay)*, *Rec.* 2010, p. 14, § 101.
[77] SALMON (J.) (dir.), *op. cit.*, p. 770 ; KOIVUROVA (T.), *«* Due diligence *»,* in WOLFRUM (R.), *op. cit.*, p. 245.
[78] CIJ, arrêt du 9 avril 1949, *Affaire du Détroit de Corfou, op. cit.*, p. 22 ; arrêt du 9 février 2022, *Affaire Activités armées sur le territoire du Congo (République démocratique du Congo c. Ouganda), op. cit.*, § 52 ; KOIVUROVA (T.), *op. cit.*, p. 236 ; SALMON (J.), « L'intention en matière de responsabilité internationale », *in Mélanges Michel Virally. Le droit international au service de la paix, de la justice et du développement,* Paris, Pedone, 1991, pp. 416-417 ; SINKONDO (M.), *op. cit.*, p. 226 ; VERHOEVEN (J.), *op. cit.*, p. 619 ; RIVIER (R.), *op. cit.*, p. 722 ; DUPUY (P.M.), KERBRAT (Y.), *op. cit.*, p.555.
[79] CIJ, arrêt du 24 mai 1980, *Affaire relative au personnel diplomatique et consulaire des Etats-Unis et Téhéran, op. cit.*, § §67 - 68; CONDORELLI (L.), « L'imputation à l'Etat d'un fait internationalement illicite: solutions classiques et nouvelles tendances », *RCADI,* 1984, vol. 189, p. 96 ; GRANT (J. P.), BARKER (J. C.), PARRY (C.), *op. cit.*, p. 51 ; ALLAND (D.), *Manuel de droit international public,* Paris, PUF, 8ème éd., 2021, p. 265.
[80] SALMON (J.) (dir.), *Dictionnaire de droit international public*, *op. cit.*, p. 770.
[81] CONDORELLI (L.), « L'imputation à l'Etat d'un fait internationalement illicite : solutions classiques et nouvelles tendances », *RCADI,* 1984, vol. 189, p. 101 ; SALMON (J.), *Dictionnaire de droit international public*, *op. cit.*, pp. 770-771
[82] CIJ, arrêt du 9 avril 1949, *Affaire du Détroit de Corfou*, *op. cit*, pp. 19-20.
[83] SALMON (J.), « L'intention en matière de responsabilité internationale », *op. cit.*, p. 416-417.

**26.** Cette obligation de vigilance s'applique également au cyberespace[84], une telle obligation ayant vocation à s'appliquer à toute branche du droit[85]. Les États souverains ne peuvent pas raisonnablement, négliger, mésestimer, méjuger tout ce qui se passe sur leur territoire[86], et ce même en matière numérique[87]. La souveraineté territoriale implique que les États prennent toutes les mesures nécessaires afin d'empêcher que des opérations cybernétiques menées à partir de leur territoire ou de leurs infrastructures ne violent les droits des autres États[88] : cela concerne également les cyberattaques en cours ou imminentes, menées à partir de leur territoire, pouvant avoir des conséquences « *sérieuses* »[89]. Par ailleurs, une cyber opération, même de faible intensité, qui pénètre dans le système informatique d'un État et ce même sans causer de dommage ou de perte de fonctionnalité, peut constituer la violation de sa souveraineté[90].

**27.** En l'espèce, les activités de NoVox constituent une cyber opération coercitive et agressive en ce qu'elles impliquent la pénétration du système informatique du Leoni, sans son autorisation[91]. Le Dole savait que les activités principales du collectif NoVox avaient essentiellement lieu sur la plateforme de microblogging *Echo*, entreprise numérique dominante de la technopole dolaise[92]. Les activités du collectif NoVox ont bénéficié de la bienveillance du

---

[84] AGNU, A/68/98, *Rapport du Groupe d'experts gouvernementaux chargé d'examiner les progrès de la téléinformatique dans le contexte de la sécurité internationale*, 24 juin 2013, §23 ; SCHMITT (M. N.) (GE), *Tallinn Manual 2.0 on the International Law applicable to cyber operations, op. cit.*, p. 30 ; KOIVUROVA (T.), *op. cit.*, p. 245 ; BANNELIER (K.), « Le standard de due diligence et la cyber-sécurité », *in* CASELLA (S.), *Le standard de due diligence et la responsabilité internationale*, Paris, Pedone, 2018, p. 90 ; TALBOT JENSEN (E.), *op. cit.*, p.746 ; SCHMITT (M. N.), « Foreign Cyber Interference in Elections », *op. cit.*, p. 759 ; O.T.A.N., « Trends in international law for cyberspace », *CCDCOE Nato Cooperative Cyber defence centre of excellence*, mai 2019, p. 1 ; BESSON (S.), *La due diligence en droit international*, *op. cit.*, p. 97.

[85] PISILLO MAZZESCHI (R.), « Le standard de due diligence comme extension ou limite de la responsabilité internationale », *in* SFDI, *Le standard de due diligence et la responsabilité internationale*, Paris, Pedone, 2018, p. 226 ; BANNELIER (K.), *op. cit.*, p. 75 ; ILA, *Study Group on Due Diligence International Law - Second Report*, juillet 2016, p. 6, file:///home/chronos/u-2aec3df9fcae26be235e20b1df6aa72ef32e0805/MyFiles/Downloads/Draft%20Study%20Group%20Report%20Johannesburg%202016.%20(2).pdf

[86] CIJ, arrêt du 9 avril 1949, *Affaire du Détroit de Corfou*, *op. cit.*, p. 18 ; BANNELIER (K.), CHRISTAKIS (T.), *Cyberattaques - Prévention-réactions : rôle des États et des acteurs privés*, Paris, Les Cahiers de la Revue Défense Nationale, 2017, p. 22.

[87] BANNELIER (K.), *op. cit.*, p. 79.

[88] AGNU, A/68/98, *op. cit.*, §§ 20, 27 et 28(b) ; A/70/174, *op. cit.*, §13 (h) ; Rés. 73/27, *op. cit.*, p. 3 ; SCHMITT (M. N) (GE), *Tallinn manual on the international law applicable to cyber warfare, op.cit.,* pp. 29-34 ; SCHMITT (M. N.) (GE), *Tallinn Manual 2.0 on the International Law applicable to cyber operations, op. cit.*, p. 17 et pp. 30-31 ; C.E.I.S., « Analyse du Manuel de Tallinn 2.0 sur le droit international applicable aux cyber-opérations », *Étude prospective et stratégique*, 29 novembre 2017, p. 21

[89] SCHMITT (M. N.) (GE), *Tallinn Manual 2.0 on the International Law applicable to cyber operations, op. cit.*, p. 34 ; CHOUKRI (I.), « Remarques sur les Manuels de Tallinn (1.0 et 2.0) et le droit international applicable aux cyber-opérations. Paix et sécurité européenne et internationale », *PSEI*, 2018, https://halshs.archives-ouvertes.fr/halshs-03156559, pp. 11-13.

[90] AGNU, A/68/98, *op.cit.*, §20 ; A/70/174, *op. cit.*, p.23 ; C.E.I.S., *op. cit.*, p. 21.

[91] *Exposé des faits*, § 16.

[92] *Ibid.*, § 13.

Dole qui a toléré, salué puis encouragé la violation de la souveraineté du Leoni[93], allant jusqu'à confirmer la véracité de certaines des informations relayées par NoVox sur une chaîne télévisuelle internationale[94]. Le Secrétaire d'Etat du Dole était informé des opérations de NoVox relatives aux élections présidentielles du Leoni de 2020, celles-ci étant publiées sur un réseau utilisé par ce dernier comme l'indique ses multiples republications sur la plateforme Echo[95]. Le Dole avait très largement les moyens de s'acquitter de son obligation de *due diligence*, grande « puissance économique mondiale »[96] et « à la pointe en matière numérique »[97]. Il n'a pourtant pris aucune mesure pour empêcher, prévenir ni même réprimer les actions de NoVox. Le Dole a laissé son territoire être utilisé pour la conduite de cyber opérations contraire aux droits du Leoni : les actions de NoVox constituent une ingérence dans les affaires internes du Leoni dans un domaine réservé -les élections nationales- et donc une violation de sa souveraineté. Le seul fait que le Dole avait connaissance, ou aurait dû avoir connaissance, des opérations du collectif NoVox constitue une base suffisante pour établir qu'il a manqué sciemment à son obligation de vigilance.

**28.** Par conséquent, le Dole n'a pas respecté son obligation de *due diligence*, ce qui engage sa responsabilité.

**29.** En conclusion, le Dole n'a respecté ni le principe de non-ingérence, ni l'obligation de *due diligence* qui lui incombait au regard des actions du collectif NoVox qui lui sont imputables.

**30.** Au regard de tout ce qui précède, le Leoni prie la Cour de dire et juger que la responsabilité internationale du Dole est engagée du fait des activités menées par le collectif NoVox afin d'interférer dans le cours de la campagne électorale leonienne de 2020.

## PARTIE 2. LA RESPONSABILITÉ INTERNATIONALE DU DOLE EST ENGAGÉE DU FAIT DE L'IMPLANTATION DU PROGRAMME MALVEILLANT "CRÉPUSCULE" DANS LE SYSTÈME INFORMATIQUE DU PORT DE VANETI, À DES FINS D'ESPIONNAGE ET DE SABOTAGE D'UNE INFRASTRUCTURE CRITIQUE

**31.** À titre liminaire, il convient de rappeler que le cyberespace relève de la souveraineté des États[98]. Le cyberespace est une création de l'humanité et les éléments qui composent et

[93] *Ibid.*
[94] *Ibid.*
[95] *Réponses aux questions d'éclaircissement*, n°3.
[96] *Exposé des faits*, § 2.
[97] *Ibid.*, § 3.
[98] AGNU, A/70/174, *op. cit.*, §28 (a) ; FRANZESE (P.W.) « Sovereignty in cyberspace : Can it exist? », *The Air Force Law Review,* vol. 64, 2009, p. 12 ; MELZER (N.), *Cyberwarfare and International Law*, Institut des Nations Unies pour la recherche sur le désarmement (UNIDIR), Genève, coll. Ressources, 2011, p. 5 ; BARAT-GINIES

soutiennent l'infrastructure Internet tels que les câbles, commutateurs ou routeurs, ainsi que les activités qui y sont liées, se trouvent physiquement sur le territoire de l'État, et donc soumis à sa juridiction ou sous son contrôle[99]. Le cyberespace constitue donc une ressource inépuisable et relève de la souveraineté des États. La pratique des États illustre cela comme en témoigne la *Convention de Budapest sur la cybercriminalité*[100] , ratifiée par le Dole[101]. Dès lors, les droits et obligations des États qui découlent de leur souveraineté sont également applicables au cyberespace, et leur non-respect entraîne la responsabilité de l'État auteur du fait illicite. En effet, la violation d'une obligation internationale par un État entraîne sa responsabilité internationale[102]. Les règles de droit international sont ainsi transposées au cyberespace afin d'appréhender les activités des États ou celles qui leur sont imputables aux États[103].

**32.** Le Leoni démontrera que l'installation du programme malveillant « Crépuscule » par le Dole entraîne sa responsabilité internationale. L'attribution de l'installation du programme « Crépuscule » dans le système informatique du port de Vaneti par le Dole n'est pas à démontrer puisque la Présidente du Dole l'a expressément reconnue[104]. Le Leoni établira que l'installation de ce programme par le défendeur constitue une violation de l'interdiction du recours à la force (Chapitre 1) et à titre subsidiaire, si cela n'était pas reconnu par la Cour, que cela constitue une violation du principe de non-intervention (Chapitre 2).

## CHAPITRE 1. LE DOLE A MANQUÉ À SON OBLIGATION INTERNATIONALE DE NON RECOURS À LA FORCE

**33.** L'article 2 § 1 de la *Charte* consacre l'égalité souveraine des États. Cela se traduit notamment par l'interdiction générale de recours à la force entre les États consacré à l'article

(O.), « Existe-t-il un droit international du cyberespace?», *Hérodote*, 2014, n°152-153, p. 201-204 ; WATTS (S.), RICHARD (T.), « Baseline territorial sovereignty and cyberspace », *Lewis and Clark Law Review*, 2018, p. 851

[99] WOLTAG (J.-C.), *Cyber Warfare: computer network operations outside of armed conflict*, Cambridge, Intersentia, 1ère édition, 2014, pp. 56-57 ; BANNELIER (K.), « Obligations dans de diligence dans le cyberespace : qui a peur de la cyber-diligence », *RBDI*, 2017/2, p. 615.

[100] *Convention de Budapest sur la cybercriminalité*, adoptée à Budapest le 23 novembre 2001, entrée en vigueur le 1er juillet 2004.

[101] *Exposé des faits*, § 37.

[102] AGNU, Rés. 56/83, *op. cit.*, article 2 ; CIJ, arrêt du 27 juin 1986, *Affaire des activités militaires et paramilitaires au Nicaragua et contre celui-ci, op. cit.*, § 57 et § 226 ; arrêt du 25 septembre 1997, *Affaire relative au projet Gabčíkovo-Nagymaros (Hongrie c. Slovaquie), op. cit.*, § 78 ; arrêt du 26 février 2007, *Application de la convention pour la prévention et la répression du crime de génocide (Bosnie-Herzégovine c. Serbie-et-Monténégro*), *op. cit.*, § 385 ; arrêt du 30 novembre 2010, *Ahmadou Sadio Diallo (République de Guinée c. République démocratique du Congo)*, *Rec*. 2010, p. 691, § 160 ; arrêt du 20 juillet 2012, *Questions concernant l'obligation de poursuivre ou d'extrader (Belgique c. Sénégal)*, *Rec.* 2012, p. 461, § 121.

[103] SCHMITT (M. N.) (GE), *Tallinn Manual on the International Law Applicable to Cyber Warfare, op. cit.*, pp. 42 et 45.

[104] *Exposé des faits*, § 25.

2 § 4 de la *Charte*. L'interdiction générale de recours à la face est une norme de *jus cogens* et une norme coutumière[105] . Le recours à la force au sens de l'article 2 § 4 de la *Charte* revêt un seuil de gravité particulier et suppose qu'un État ait la volonté de recourir à la force contre un autre État[106]. Quatre critères doivent être réunis pour caractériser l'agression armée: un État agissant en premier doit être à l'initiative de l'opération, cette opération doit lui être imputable, être dirigée contre un autre État dans le cadre de la conduite des relations internationales et enfin, relever d'un recours à la force armée[107].

**34.** Le Leoni démontrera que l'installation du programme malveillant Crépuscule constitue une agression armée. Les trois premiers critères ne sont pas à démontrer puisque le Dole a reconnu avoir procédé à l'implantation du logiciel Crépuscule au sein de « l'infrastructure numérique leonienne »[108]. Toute opération cybernétique, offensive ou défensive, susceptible de tuer ou blesser des personnes ou de détruire ou endommager des biens constitue une cyberattaque[109]. Une cyberattaque peut donc constituer une agression armée grâce à l'examen d'un faisceau d'indices, la qualification dépendant de la dimension et des effets de l'attaque[110]..

**35.** Le Leoni démontrera d'une part que le logiciel Crépuscule est une arme par destination (Section 1) et d'autre part que l'implantation du logiciel « Crépuscule » par le Dole constitue un recours à la force armée compte tenue de la sévérité et l'invasivité de l'opération (Section 2) et du caractère direct et de la mesurabilité des effets de l'opération (Section 3).

Section 1. Le logiciel Crépuscule est une arme par destination

**36.** L'agression implique « *l'usage de toutes armes par un État contre le territoire d'un autre État »*[111]. La CIJ adopte également une conception souple de la notion d'arme et a considéré que l'interdiction générale de l'emploi de la force ne préjugeait pas de l'usage « *d'armes*

[105] AGNU, Rés. 2625 (XXV), *op. cit.* ; CIJ, arrêt du 27 juin 1986, *Affaire des activités militaires et paramilitaires au Nicaragua et contre celui-ci, op. cit.*, §§187-190 ; avis consultatif du 9 juillet 2004, *Conséquences juridiques de l'édification d'un mur dans le territoire palestinien occupé, Rec.* 2004, p. 136, § 87 ; HOFMANN (R.), « International Law and the Use of Military Force Against Iraq », *in* DELBRÜCK (J.), HOFMANN (R.), ZIMMERMANN (A.), *German Yearbook of International Law*, Duncker & Humblot GmbH, vol. 45, 2003, p. 11 ; ORAKHELASHVILI (A.), « Changing *Jus Cogens* through State practice? The case of the Prohibition of the Use of Force and its Exceptions », *in* WELLER (M.), RYLATT (J.W.), SOLOMOU (A.), *The Oxford Handbook of the Use of Force in International Law*, Oxford, Oxford University Press, 2015, pp. 157-175.

[106] CORTEN (O.), *Le droit de la guerre - L'interdiction du recours à la force en droit international contemporain*, Paris, Pedone, 3ème édition, 2020, pp. 126-127 et p. 142.

[107] AGNU, Rés. 3314 (XXIX) *Définition de l'agression*, 14 décembre 1974, articles 1er et 2 ; CORTEN (O.), *Le droit de la guerre - L'interdiction du recours à la force en droit international contemporain, op. cit.*, p. 171; BARAT-GINIES (O.), *op. cit.*, pp. 208-209.

[108] *Exposé des faits*, § 25.

[109] SCHMITT (M. N) (GE), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, *op. cit.*, p. 106.

[110] *Ibid.*, p. 48 ; *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, *op. cit.*, p. 339.

[111] AGNU, Rés. 3314 (XXIX), *op. cit.*, § 3 b).

*particulières et s'appliquait à n'importe quel emploi de la force, indépendamment des armes employées* »[112]. Ainsi dans l'affaire des *Activités militaires et paramilitaires*, la Cour a qualifié l'armement et l'entraînement de groupes armés d'usage de la force, alors même que ces actes ne constituaient pas en tant que tels, physiquement ou directement, des usages de la force armée[113]. De même, la doctrine admet que certains objets ou matières peuvent être détournés de leurs destinations habituelles pour être utilisés comme des armes, couvertes par la prohibition du recours à la force[114]. Elles doivent ainsi être « *identifiées par leurs effets et non par les mécanismes à travers lesquels elles provoquent des destructions ou des dommages* »[115]. Les logiciels malveillants qui « *perturb*[ent] *les fonctions normales de l'ordinateur* » en sont un exemple[116]. La Cour considère également que les principes juridiques qui « *imprègnent tout le droit des conflits armés* » s'appliquent « *à toutes les formes de guerre et à toutes les armes, celles du passé, comme celles du présent et de l'avenir* »[117].

**37.** C'est le cas des moyens cybernétiques qui ne sont pas des armes traditionnelles et doivent être considérés comme des armes de « *l'avenir* ». La guerre cybernétique implique l'utilisation de cyberarmes et tout moyen équivalent[118], à savoir tout dispositif, mécanisme, ou logiciel conçu ou destiné à être utilisé pour interférer avec le fonctionnement cybernétique ciblé et pouvant causer des dommages, blesser, entraîner la mort de personnes, ou la détérioration ou la

---

[112] CIJ, avis consultatif du 8 juillet 1996, *Licéité de la menace ou de l'emploi des armes nucléaires*, *Rec.* 1996, p. 226, § 39.
[113] CIJ, arrêt du 27 juin 1986, *Affaire des activités militaires et paramilitaires au Nicaragua et contre celui-ci*, *op. cit.*, § 228.
[114] CORTEN (O.), *Le droit de la guerre - L'interdiction du recours à la force en droit international contemporain, op. cit.*, p. 164 ; ROSCINI (M.), *Cyber operations and the Use of Force in International Law*, Oxford, Oxford University Press, 2014, 1ère édition, 2014, p. 50.
[115] DÖRMANN (K.), « Applicability of the Additional Protocols to Computer Network Attacks », *in International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law*, Stockholm, 17-19 novembre 2004, p. 4, disponible sur : http://www.icrc.org/eng/resources/documents/misc/68lg92.htm; ZEMANEK (K.), « Armed attack » *in* LACHENMANN (F.), WOLFRUM (R.), *The law of armed conflict and the use of force . Max Planck Encyclopedia of Public International Law,* Oxford, Oxford University Press, 1ère édition, 2017, p. 30 ; ZIOLKOWSKI (K.), « Computer Network Operations and the Law of Armed Conflict », *Military Law and Law of War Review*, vol. 49, 2010, p. 69 ; ROSCINI (M.), *Cyber operations and the Use of Force in International, op. cit.*, p. 50 ; BAUDIN (L.), *Les cyberattaques dans les conflits armés : qualification juridique, imputabilité et moyens envisagés en droit humanitaire,* Paris, L'Harmattan, 2014, p. 119 ; BANNELIER-CHRISTAKIS (K.), « Is the principle of distinction still relevant in cyberwarfare? From doctrinal discourse to States' practice », *in* TSAGOURIAS (N.), BUCHAN (R.), *Research Handbook on International Law and Cyberspace*, Edward Elgar , 2015, 2ème éd., pp. 439-440.
[116] SCHAAP (A. J.), « Cyber Warfare Operations: Development and Use Under International Law » *Air Force Law Review,* vol. 64, 2009, pp. 121-173.
[117] CIJ, avis consultatif du 8 juillet 1996, *Licéité de la menace ou de l'emploi des armes nucléaires*, *op. cit.*, §86.
[118] SCHMITT (M. N.) (GE), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, *op. cit.*, p. 452.

destruction de biens[119]. Selon la doctrine majoritaire, l'identification d'une cyberattaque dépend des conséquences que peut avoir l'acte et non de sa nature[120].

**38.** Le logiciel malveillant Crépuscule demeure une cyberarme hautement invasive, dotée de fonctionnalités de sabotage de nature à endommager voire neutraliser le système de gestion informatique du Port de Vaneti. Sans l'intervention rapide des autorités locales, le port était exposé à une perte de fonctionnalité certaine. Le rapport d'experts qualifie « Crépuscule » de « *bombe à retardement* » indique que l'implant « *aurait pu être utilisé à des fins dévastatrices pour paralyser les chaînes d'approvisionnement du pays ou réduire à néant sa capacité de défense navale* »[121]. Le Logiciel Crépuscule est donc une arme pouvant être utilisée par le Dole pour causer des dommages au Leoni.

## Section 2. L'implantation du logiciel Crépuscule est une opération hautement invasive qui aurait pu causer des dommages sévères au Leoni

**39.** Le recours à la force est appréhendé en se référant à un seuil ou un standard de gravité, apprécié de manière souple, l'emploi de la force ou l'attaque armée devant être distingué des autres formes de coercition qui sont, elles, moins brutales[122]. Une cyber opération constitue un usage de la force lorsque sa gravité et ses effets sont comparables à une opération non cybernétique équivalente à un usage de la force[123]. Le critère de l'invasivité de l'attaque renvoie au niveau d'intrusion et à l'instabilité que pourrait provoquer par la cyberopération dans l'État ciblé[124]. Plus un système est sécurisé, plus l'intrusion sera qualifiée d'invasive[125]. Par ailleurs, le fait que la cyber opération soit cantonnée au territoire d'un État en particulier augmente son caractère invasif puisque si l'intrusion s'étendait sur plusieurs territoires, ses effets seraient

---

[119] *Ibid.*, p. 452 et p. 415.
[120] DINSTEIN (Y.), *The Conduct of Hostilities under the Law of International Armed Conflict,* Cambridge, Cambridge University Press, 2004, p. 84 ; WAXMAN (M.C.), « Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4) », *Yale Journal of International Law*, vol. 36, 2010, p. 437; HARRISON DINNISS (H.), « Attacks and Operations: The debate over computer network "attacks"», *The Minerva Center for Human Rights,* 28-29 November 2011, p. 2, ; SCHMITT (M. N.) (GE), *Tallinn Manual on the international Law applicable to Cyberwarfare*, *op. cit.*, pp. 106-107 ; ROSCINI (M.), *Cyber operations and the Use of Force in International, op. cit.*, p. 47 ; WOLTAG (J.-C.), *Cyber Warfare: computer network operations outside of armed conflict*, *op. cit.*, pp. 143-146 ;
[121] *Exposé des faits*, §20.
[122] SA du 11 mars 1941, *Affaire de la Fonderie du Trail (Canada c. États-Unis), RSA,* vol. III, p. 1965 ; SA du 16 novembre 1957, *Affaire du lac Lanoux* (*Espagne c. France*), *RSA*, vol. XII, p. 308 ; CIJ*,* arrêt du 27 juin 1986, *Affaire des activités militaires et paramilitaires au Nicaragua et contre celui-ci, op. cit*, § 191.
[123] SCHMITT (M. N.) (GE), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, *op. cit.*, p. 45.
[124] BAUDIN (L.), *op. cit.*, p. 104.
[125] SCHMITT (M. N.) (GE), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, *op. cit.*, p. 49.

répartis et supportés par plusieurs États, et seraient donc amoindris[126]. Le fait que l'opération se concentre sur un État indique par ailleurs l'intention de l'auteur de l'acte d'attaquer l'État cible.

**40.** En outre, il est largement admis qu'une cyberattaque n'a pas à causer de destruction matérielle à la cible attaquée pour constituer un usage de la force, voire une attaque armée[127]. Les conséquences d'une opération pouvant causer des dommages physiques aux personnes ou aux biens permettent de qualifier l'opération d'usage de la force. L'étendue, la durée et l'intensité des conséquences potentielles sont des facteurs de nature à influencer le niveau de sévérité de l'attaque[128]. La survenance d'un dommage physique n'est pas nécessaire pour identifier un recours à la force armée dans ce cadre dès lors que l'opération vise et perturbe l'infrastructure critique d'un État de manière significative[129]. Ainsi, la « *neutralisation d'un objet comme résultat éventuel d'une attaque »*[130] ou encore les nuisances causées à la population du fait de l'interférence avec les chaînes d'approvisionnement[131] doivent être considérés comme des attaques relevant de la force armée. Une cyber opération qui ne cause aucun dommage peut donc être considérée comme une attaque en tenant compte des conséquences grave que l'opération aurait pu causer si celle-ci n'avait pas été interceptée à temps[132].

**41.** La nature de la cible visée et son importance aux yeux de l'État visé sont aussi des facteurs déterminants[133]. En effet, une offensive lancée contre un point stratégique de l'État comme un bien à objectif militaire est nécessairement significative[134]. En l'absence de dommage direct (mort, blessures, destruction matérielle), il convient de se référer à l'infrastructure critique visée

---

[126] *Ibid.*; WOLTAG (J.-C.), *Cyber Warfare: computer network operations outside of armed conflict, op. cit.*, p. 145.

[127] TALBOT JENSEN (E.), « Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense », *Stanford Journal of International Law,* vol. 38, 2002, pp. 206-207 ; DROEGE (C.), «Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians», *International Review of the Red Cross,* Vol. 94, n° 886, 2013, p.557 ; ROSCINI (M.), *Cyber operations and the Use of Force in International, op. cit.*, p. 222 ; GEISS (R.), LAHMANN (H.), « Cyber warfare: applying the principle of distinction in an interconnected spac*e », Israel Law Review*, vol. 45, 2012, p. 397.

[128] SCHMITT (M. N.) (GE), *Manuel de Tallinn sur le droit international applicable à la cyberguerre*, *op. cit.*, p. 48.

[129] ROSCINI (M.), *Cyber operations and the Use of Force in International, op. cit.*, p. 135 ; SCHMITT (M. N.) (GE), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, *op. cit.*, p. 419 ; Program on Humanitarian Policy and Conflict Research at Harvard University, *H.P.C.R. Manual on International Law Applicable to Air and Missile Warfare*, Cambridge, Cambridge University Press, 2013, pp. 27-28.

[130] DÖRMANN (K.), *op. cit.*, p. 4 ; BANNELIER-CHRISTAKIS (K.), *op. cit.*, pp. 439-440.

[131] BROWN (D.), « A Proposal for an International Convention To Regulate the Use of Information Systems in Armed Conflict », *Harvard International Law Journal*, vol. 47, 2006, p. 188 ; SHARP (W. G.), *Cyberspace and the Use of Force*, Ageis Research Corp, 1999, p. 102 ; WOLTAG (J.-C.), *Cyber Warfare: computer network operations outside of armed conflict*, *op. cit.*, p. 144.

[132] *Ibid.* ; BANNELIER-CHRISTAKIS (K.), *op. cit.*, p. 439-440 ; SCHMITT (M. N.) (GE), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, *op. cit.*, p. 110.

[133] *Ibid.*, p. 51.

[134] *Ibid.*, p. 125.

afin d'appréhender la dimension et les effets de la cyberattaque[135]. Une cyberattaque constitue donc une agression armée si elle vise à neutraliser une infrastructure critique du ressort de la souveraineté d'un État[136]. Chaque État détermine ce qui constitue pour lui une infrastructure critique[137]. Cette notion désigne essentiellement les infrastructures utilisées « *pour la production, la transmission et distribution d'énergie, les transports aériens et maritimes, l'approvisionnement en eau*»[138]. Autrement dit, il s'agit d'une infrastructure si vitale pour l' État que toute perturbation aurait un impact significatif sur sa sécurité nationale ou des secteurs majeurs tels que l'économie, la santé publique, la finance, l'énergie, ou encore les télécommunications[139]. C'est ainsi le cas des ports maritimes commerciaux[140].

**42.** En l'espèce, l'action menée par le Dole vise un réseau sécurisé, le système de gestion informatique de Vaneti, port principal du Leoni qui participe à l'approvisionnement de l'ensemble du pays, et au déploiement d'activités maritimes, industrielles et militaires[141]. Le port de Vaneti est donc un point stratégique du Leoni et joue un rôle de premier plan pour la défense du pays et de ses ressortissants. L'attaque du Dole visait donc une infrastructure critique léonienne. Certes, l'implantation du logiciel « Crépuscule » n'a pas eu de conséquences physiques ou matérielles directes mais ce logiciel menaçait de paralyser les chaînes d'approvisionnement du pays et cela concernait plusieurs secteurs tels que la santé publique ou l'économie. Ce logiciel aurait aussi pu être à l'origine d'une série de pénuries, mettant ainsi en danger la vie de toutes les personnes vivant au Leoni *a priori* sur une période longue et indéterminée. L'effondrement des capacités de défense navale est aussi un dommage qu'aurait pu causer ce logiciel, si le Leoni ne l'avait pas intercepté à temps. Contrairement à ce qu'affirme le défendeur, une opération de sabotage d'une telle envergure doit dès lors être qualifiée de sévère et constituer un recours à la force armée, la survenance d'un dommage n'étant pas

---

[135] TALBOT JENSEN (E.), « Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense », *op. cit.*, p. 227 ; CONDRON (S. M.), « Getting it right: Protecting American critical infrastructure in cyberspace », *Harvard Journal of Law & Technology,* Vol. 20, n° 2, 2007, pp. 406-407 ; MELZER (N.), *op. cit.*, p. 14.

[136] *Ibid.*, p. 16.

[137] CS, S/RES/2341, *Protection des infrastructures essentielles contre les attaques terroristes*, 13 février 2017, p. 2.

[138] AGNU, Rés. 58/199, *Création d'une culture mondiale de la cybersécurité et protection des infrastructures essentielles de l'information*, 30 janvier 2004, p. 1, § 3.

[139] Organisation de Shanghai pour la coopération, *Agreement between the governments of state members of the Shanghai Cooperation Organization on cooperation in the field of ensuring international information security,* 16 juin 2009, annexe 1, p. 10 ; Commission Européenne, COM(2005) 576 final, *Livre Vert sur un Programme Européen de Protection des Infrastructures Critiques*, 17 novembre 2005, p. 22 ; MELZER (N.), *op. cit.*, pp. 14-16.

[140] POLEMI (N.), *Port Cybersecurity: Securing Critical Information Infrastructures and Supply Chains*, Elsevier, 1ère édition, 2017, p. 1.

[141] *Exposé des faits*, § 20.

nécessaire qualifier une cyberattaque de recours à la force armée. Ce logiciel malveillant, installé par le Dole, menaçait donc la sécurité du Leoni.

**43.** Par conséquent, le Leoni demande à la Cour de reconnaître que le logiciel malveillant « Crépuscule » constitue une opération hautement invasive.

## Section 3. Les potentiels effets de l'implantation du logiciel Crépuscule sur le Leoni sont directs et mesurables

**44**. Les conséquences de la cyberattaque doivent être directes[142] et résulter directement de l'intention de l'auteur de l'acte[143]. Il faut donc un lien de cause à effet entre la survenance de la cyber opération et ses conséquences, à savoir les souffrances causées ou pouvant être causées par la cyber opération. Même lorsqu'elle est interceptée à temps, l'opération peut constituer un recours à la force[144] lorsque les effets potentiels de l'attaque sont graves et mesurables[145]. Ainsi, lorsque la cause et les effets sont établis et identifiés, et que ces derniers sont graves, la cyber opération relève de l'emploi de la force[146]. L'atteinte à l'intégrité du système cybernétique doit être intentionnelle[147], grave et viser à interférer avec le fonctionnement du système informatique ciblé en introduisant, endommageant, altérant ou supprimant des données informatiques. Le fait de pouvoir identifier et quantifier les conséquences de la cyber opération permet ainsi déterminer si celle-ci a atteint le seuil de gravité caractéristique d'un recours à la force armée[148].

**45.** Le logiciel Crépuscule est une arme qui a été implantée intentionnellement dans le système informatique du port leonien depuis juin 2020, comme l'a reconnu la présidente du Dole[149]. Le programme « Crépuscule » porte atteinte à l'intégrité du système informatique de l'infrastructure critique et est l'équivalent d'une « bombe à retardement »[150]. Les effets de la cyberattaque sont bien identifiables. Le rapport des experts de l'Agence Maritime de Sécurité des systèmes (ci-après AMS) fait état d'une paralysie potentielle des chaînes d'approvisionnement du pays et de l'anéantissement de la capacité de défense navale du

---

[142] SCHMITT (M. N.) (GE), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, *op. cit.*, p. 49.
[143] BAUDIN (L.), *op. cit.*, p. 103.
[144] SCHMITT (M. N.) (GE), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, *op. cit.*, p. 110 ; ROSCINI (M.), *op. cit.*, p. 135 ; SCHMITT (M. N.) (GE), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, *op. cit.*, p. 419 ; Program on Humanitarian Policy and Conflict Research at Harvard University, *op. cit.*, pp. 27-28.
[145] BAUDIN (L.), *op. cit.*, p. 104.
[146] SCHMITT (M. N.) (GE), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, *op. cit.*, p. 49.
[147] *Convention de Budapest sur la cybercriminalité*, *op. cit.*, article 5 ; SHARP (W. G.), *op. cit.*, p. 133 ; TALBOT JENSEN (E.), « Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense », *op. cit.*, p. 223.
[148] SCHMITT (M. N.) (GE), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, *op. cit.*, p. 49.
[149] *Exposé des faits*, §25.
[150] *Ibid.*, §20

Leoni[151]. Lesdits effets n'ont pas eu lieu car les équipes léoniennes ont empêché à temps le sabotage entrepris par le Dole. Le mode opératoire utilisé par le Dole ressemble d'ailleurs à celui d'une précédente cyberguerre menée par les organes étatiques dolais[152]. Sans l'intervention des services léoniens, il ne s'agirait plus seulement d'un risque évité de justesse, mais de dommages concrets dont les répercussions auraient été tellement graves qu'ils auraient été comparables à une bombe, arme utilisée traditionnellement en cas d'agression armée. Par conséquent, les effets de l'implantation du logiciel « Crépuscule » sur le Leoni sont directs et mesurables et ont failli causer au Leoni des dommages sévères.

**46.** L'implantation du logiciel Crépuscule est donc une cyberattaque constitutive d'un recours à la force armée.

**47.** Le Leoni prie donc la Cour de dire et juger que le Dole engage sa responsabilité internationale du fait de la violation de l'interdiction de non recours à la force.

## CHAPITRE 2. LA CYBERATTAQUE MENÉE PAR LE DOLE EST UNE VIOLATION DU PRINCIPE DE NON-INTERVENTION

**48.** Le principe de non-intervention découle des principes de souveraineté et d'égalité des États[153]. Ce principe de nature conventionnelle et coutumière interdit toute intervention « *dans des affaires qui relèvent essentiellement de la compétence nationale d'un État* »[154], comme l'a également admis la Cour[155]. L'intervention résidant « *dans le fait pour un État de chercher à "subordonner" la souveraineté d'un autre État mais aussi* [...] *d'essayer de porter atteinte aux droits souverains de cet État* »[156], toute forme d'intervention dans les affaires intérieures d'un État sont interdites[157], Le principe de non-intervention s'applique dans le cyberespace dans la mesure où celui-ci relève de la souveraineté des États[158], et toute cyber opération « *menée par un État contre une cyber infrastructure localisée dans un autre État peut être de nature à violer*

---

[151] *Ibid.*
[152] *Réponses aux questions d'éclaircissement,* n°2.
[153] SA du 4 avril 1928*, Affaire de l'Île de Palmas (États-Unis c. Pays-Bas)*, RSA, vol II, p. 829 ; CIJ, arrêt du 9 avril 1949, *Détroit de* Corfou, *op. cit.*, p. 35 ; CS, S/RES/242, « La situation au Moyen-Orient », 22 novembre 1967 ; DAILLIER (P.), FORTEAU (M.), PELLET (A.), *op. cit.*, pp. 486-487.
[154] *Charte des Nations Unies*, *op. cit.*, article 2§7.
[155] CIJ*,* arrêt du 27 juin 1986, *Affaire des activités militaires et paramilitaires au Nicaragua et contre celui-ci, op. cit.*, pp. 37-38 ; arrêt du 19 décembre 2005, *Activités armées sur le territoire du Congo (République démocratique du Congo c. Ouganda)*, *Rec.* 2005, p. 227, §164.
[156] DAVID (E.), « Portée et limite du principe de non-intervention », *RBDI,* 1990/2, p. 354.
[157] AGNU, Rés. 36/103, *op. cit.*, Annexe, article I (a); CONFORTI (B.), *op. cit.*, pp. 491.
[158] V. *supra* § 28 ; SCHMITT (M. N.) (GE), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, *op. cit.*, p. 11.

*la souveraineté de ce dernier* »[159].

**49.** L'implantation du logiciel malveillant « Crépuscule » par le Dole dans une infrastructure léonienne, à son insu, s'apparente à une intervention dans son système politique et économique. Le logiciel malveillant Crépuscule, arme par destination utilisée par le Dole, porte atteinte au réseau informatique du port de Vaneti, port principal du Leoni. Ce programme pouvait occasionner des dommages militaires, économiques et sociaux. Le programme Crépuscule a donc été installé par le Dole afin d'intervenir dans les affaires internes léoniennes, ce qui porte atteinte à la souveraineté du Leoni. La Cour ne peut que constater que l'installation du programme Crépuscule constitue une intervention dans les affaires internes du Leoni et que le Dole a méconnu le principe de non intervention.

**50.** La République du Leoni prie la Cour de dire et juger qu'en installant le programme malveillant « Crépuscule » dans le système informatique du port de Vaneti, à des fins d'espionnage et de sabotage de l'infrastructure critique, le Dole viole ses obligations internationales et engage sa responsabilité.

## PARTIE 3. LES SANCTIONS DIPLOMATIQUES ET ÉCONOMIQUES PRISES PAR LE DOLE SONT ILLICITES AU REGARD DU DROIT INTERNATIONAL ET ENGAGENT SA RESPONSABILITÉ INTERNATIONALE

**51.** Le droit international permet à un État victime d'un acte international illicite commis par un autre État de prendre des mesures, licites ou illicites, en réaction à cet acte afin de le pousser à se conformer à ses obligations internationales[160]. Encore faut-il qu'il puisse établir la violation préalable d'une obligation internationale.

**52.** Le Dole a pris des sanctions d'ordre diplomatique et économique en réaction au détournement BGP estimant que ce détournement constituait un acte illicite[161]. La République du Leoni démontrera que ces sanctions n'ont aucun fondement en droit international, puisque le détournement BGP n'est pas un acte illicite (Chapitre 1). Si toutefois la Cour venait à considérer que le détournement BGP constitue un acte illicite, les sanctions prises par le Dole demeurent illicites en droit international (Chapitre 2).

[159] SCHMITT (M. N.) (GE), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, *op. cit*., p. 16
[160] AGNU, Rés. 56/83, *op. cit.*, article 21 à 22.
[161] *Exposé des faits*, § 25.

## CHAPITRE 1. LE DÉTOURNEMENT BGP N'EST PAS UN ACTE ILLICITE EN DROIT INTERNATIONAL

**53.** Plusieurs critères permettent de déterminer si la dimension et les effets d'une cyber opération constituent un acte international illicite[162]. Il convient de distinguer les cyber opérations qui se situent en dessous du seuil d'usage de la force, celles qui sont équivalentes à un usage de la force et, enfin, celles qui dépassent ce seuil et sont assimilables à une attaque armée[163]. Les premières constituent un simple désagrément et ne sont donc pas illicites en droit international[164]. Seules les cyber opérations qui causent ou peuvent causer de sérieux dommages aux États sont expressément interdites[165]. Lorsque les effets de la cyber opération sont comparables à un usage de la force au sens de l'article 2 § 4 de la *Charte des Nations Unies*, celle-ci constitue ainsi une cyberattaque[166]. La cyber opération doit toutefois être intentionnelle[167], c'est même un des critères envisagés par les États lorsqu'ils ont cherché à élaborer une politique pénale dans le cyberespace[168].En effet, un acte, même militaire, ne constitue ni agression ni un usage de la force s'il est commis par erreur : l'intention spécifique des dirigeants politiques ou militaires de causer un dommage est déterminante pour qualifier l'agression[169]. Ainsi, il convient de prendre en compte « *l'intention spécifique des dirigeants militaires ou politiques de l'État auteur, de violer la souveraineté de l'autre État* »[170]. En

[162] V. *supra*, Partie 2, Chapitre 1.
[163] TALBOT JENSEN (E.), « Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense », *op. cit.*, p. 222.
[164] *Ibid.* ; SCHMITT (M. N.) (GE), *Manuel de Tallinn sur le droit international applicable à la cyberguerre*, *op. cit.*, p. 48.
[165] SCHMITT (M. N.) (GE), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, *op. cit.*, p. 43.
[166] BANNELIER-CHRISTAKIS (K.), *op. cit.*, p. 436 ; SCHMITT (M. N.) (GE), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, *op. cit.*, p. 106
[167] TALBOT JENSEN (E.), « Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense », *op. cit.*, pp. 222-223 ; SHARP (W. G.), *op. cit.*, p. 133 ; WOLTAG (J.-C.), *Cyber Warfare : computer network operations outside of armed conflict*, *op. cit.*, p. 138 ; AKOTO (E.), « Les cyberattaques étatiques constituent-elles des actes d'agressions en vertu du droit international public ? : Première Partie », *Revue de droit d'Ottawa*, 2015, 46 (1), p. 11
[168] *Convention de Budapest sur la cybercriminalité, op. cit.*, articles 5 et 6.
[169] CIJ, arrêt du 6 novembre 2003, *Plateformes pétrolières (République islamique d'Iran c. États-Unis d'Amérique)*, *Rec.* 2003, p. 161, §§ 61-64 et § 89 ; CDI, « "Force majeure" et "cas fortuit" en tant que circonstances excluant l'illicéité : pratique des Etats, jurisprudence internationale et doctrine », *Ann. CDI*, A/CN.4/315, vol. II, 1ère partie, 1978, pp. 58-77 ; RUYS (T.), « The Meaning of Force and the Boundaries of Jus ad bellum : Are minimal uses of force excluded from UN Charter 2(4) ? », *The American Journal of International Law,* vol. 108, n°2, 2014, p. 173 ; CORTEN (O.), *Le droit de la guerre - L'interdiction du recours à la force en droit international contemporain*, *op. cit.*, p. 146 ; ROSCINI (M.), « World Wide Warfare—Jus ad bellum and the Use of Cyber Force », *in* BOGDANDY (A.), WOLFRUM (R.), *Max Planck Yearbook of United Nations Law*, vol. 14, 2010, p. 116 ; AKOTO (E.), « Les cyberattaques étatiques constituent-elles des actes d'agressions en vertu du droit international public ? Deuxième Partie », *Revue de droit d'Ottawa,* 2015, 46 (2), pp. 214-215
[170] MELZER (N.), *op. cit.*, p. 16.

l'absence d'intention, un acte ne peut donc être qualifié de recours à la force, quand bien même les effets de l'acte seraient violents.

**54.** Le Leoni ne conteste pas que le détournement BGP a barré temporairement l'accès aux plateformes de l'écosystème numérique dolais PERK, de 7h à 12h13, soit pour une durée totale de 5 heures et 13 minutes. Toutefois, cet événement n'était pas intentionnel et provient d'une erreur humaine[171]. En effet, ce détournement d'internet ne visait pas le Dole et les conséquences que cet acte a eu n'étaient pas recherchés par les services leoniens. La dimension et les effets de ce détournement ne sont par ailleurs pas assimilables à ce qu'auraient eu une attaque armée traditionnelle : les effets de ce détournement involontaire de BGP sont en effet la privation des internautes des services de PERK et des pertes économiques d'entreprises privées dolaises. Aucun bien n'a été détruit, aucun dommage aux personnes n'a eu lieu[172]. Et le Dole ne démontre pas l'atteinte à une infrastructure critique. Le Leoni n'avait aucune intention hostile et malveillante à égard du Dole.

**55.** En l'absence d'une telle intention, le détournement de BGP ne peut être qualifié d'agression armée ni constitué un usage de la force. Le détournement de BGP ne constitue donc pas un acte internationale illicite et les sanctions prises par le Dole en réaction à cet acte ne sont pas fondées en droit.

## CHAPITRE 2. LES SANCTIONS PRISES SONT ILLICITES AU REGARD DU DROIT INTERNATIONAL

**56.** Le Dole prétend avoir pris des sanctions en réaction au détournement BGP. Si un État considère avoir subi une attaque ou une agression armée, l'État attaqué peut se défendre selon en usant de son droit de légitime défense individuelle ou collective conformément à l'article 51 de la *Charte*. Il peut aussi se défendre en prenant des actes qui n'impliquent pas l'emploi de la force[173] comme les contre-mesures[174]. L'État peut donc prendre des sanctions qui constituent des mesures coercitives destinées à mettre une certaine pression sur l'État agresseur afin que celui-ci mette fin à un acte illicite en cours, le mettre au ban de la communauté internationale ou le décourager de commettre à nouveau un tel acte[175]. Ces mesures ont donc une finalité

[171] *Exposé des faits*, §§ 22- 23.
[172] *Ibid.*, § 24.
[173] AGNU, Rés. 56/83, *op. cit.*, art 21.
[174] *Ibid.*, article 22.
[175] HOFER (A.), « The proportionality of unilateral "targeted" sanctions: whose interests should count », *Nordic Journal of International Law*, *vol*. 89, 2020, p. 400 ; AHMAD (Z.), *WTO Law and Trade Policy Reform for Low-Carbon Diffusion Technology Diffusion*, Brill, Nijhoff, vol. 5, 2021, pp. 241-242

politique, l'État se devant de protéger sa population et les intérêts de ses ressortissants[176]. Bien que l'État puisse agir de manière unilatérale pour se défendre, le système de défense consacré par la *Charte* implique une réponse collective à toute « *menace contre la paix, d'une rupture de la paix ou d'un acte d'agression* »[177].

**57.** Le Leoni démontrera premièrement que le Dole, estimant faussement avoir été attaqué par le Leoni, n'a pas recouru au Conseil de Sécurité et a agi de manière unilatérale contrevenant ainsi à la *Charte* (Section 1) et deuxièmement, a pris des mesures qui sont *per se* illicites (Section 2).

## Section 1. La réaction du Dole n'est pas conforme aux dispositions de la *Charte*

**58.** Tout en reconnaissant le droit des États à se défendre individuellement, la *Charte* instaure un système de défense collective et limite l'action individuelle des États afin d'assurer le respect de l'interdiction de recours à la force dans les relations internationales et le maintien de la paix et sécurité internationale[178]. Ainsi, le Conseil de Sécurité (ci-après « CS ») « *fait des recommandations ou décide quelles mesures seront prises*» lorsqu'il constaté « *l'existence d'une menace contre la paix, d'une rupture de la paix ou d'un acte d'agression* »[179]. La Cour a ainsi reconnu que

> « *C'est* […] *Conseil de Sécurité qu'est dévolu le pouvoir d'imposer l'obligation explicite de se conformer aux ordres qu'il peut émettre au titre du chapitre VII, par exemple contre un agresseur. Seul le Conseil de Sécurité peut prescrire des mesures d'exécution par une action coercitive contre un agresseur*. »[180]

En effet, l'article 41 de la *Charte* permet au CS de « *décider quelles mesures prendre* », mesures qui n'impliquent pas l'emploi de la force armée, en cas de menace ou rupture de la paix ou d'agression. Ces mesures peuvent prendre la forme de « *l'interruption complète ou partielle des relations économiques et des communications ferroviaires, maritimes, aériennes, postales, télégraphiques, radioélectriques et des autres moyens de communication, ainsi que la rupture des relations diplomatiques* »[181] voire de cybermesures, à savoir des mesures prises dans le cyberespace[182].

---

[176] THOUVENIN (J.-M.) « Sanctions économiques en droit international », *Droits*, 2013, n°57, p. 162
[177] *Charte des Nations Unies*, *op. cit.*, article 39.
[178] KOLB (R.), « Considérations générales sur la violence et le droit international », *AFRI*, 2005, vol. VI, p. 39.
[179] *Charte des Nations Unies*, *op. cit.*, article 39.
[180] CIJ, avis consultatif du 20 juillet 1962, *Certaines dépenses des Nations Unies (article 17, paragraphe 2, de la Charte)*, *Rec.* p. 151, p. 163.
[181] *Charte des Nations Unies, op. cit.*, article 41.
[182] MELZER (N.), *op. cit.*, p. 19 ; SCHMITT (M. N.) (GE), *Tallinn Manual 2.0 on the International Law applicable to cyber operations, op. cit.*, p. 144.

**59.** En ce sens, c'est au CS qu'il revient de prendre les sanctions contre l'État agresseur afin d'obliger ce dernier à se conformer au droit international[183]. En effet, les sanctions sont « *des moyens de pression par voie d'astreinte tendant à obtenir de l'État récalcitrant un comportement volontaire conforme à l'injonction de l'ONU*»[184] et sont des mesures coercitives prises contre un État pour l'obliger à se conformer à ses obligations internationales[185]. Ces sanctions doivent, entre autres, doivent faire suite à la constatation d'un manquement à une obligation juridique préexistante et clairement précisée, être ciblées et ne viser que l'État auteur de la violation, et correspondre à une échelle de mesures préétablies et proportionnées à la gravité du manquement au droit, et provisoires[186]. Et bien qu'un certain nombre d'États a tendance à prendre des sanctions unilatérales, c'est-à-dire de leur propre chef et sans l'autorisation du CS comme l'affirme le défenseur, cette pratique n'en demeure pas moins contraire aux dispositions de la *Charte*[187] et à l'esprit de ce texte dont les dispositions servent à encourager et renforcer la coopération des États et l'action collective[188].

**60.** En l'espèce, le Dole a estimé avoir subi une cyberattaque dont les effets sont équivalents à un recours à la force armée et en réaction, a annoncé par le biais d'une conférence de presse la prise de sanctions unilatérales contre le Leoni[189]. Le Dole, qui dénonce pourtant une *« attaque intolérable contre les intérêts économiques dolais, l'Internet mondial et la liberté*

---

[183] *Ibid.* ; CS, S/RES/232, « Rhodésie du Sud », 16 décembre 1966, Préambule, §4 ; S/RES/1718, « Non-prolifération/République populaire démocratique de Corée », 13 décembre 2006, Préambule, §10 ; D'ARGENT (P.), D'ASPREMONT (L.), DOPAGNE (F.), VAN STEENBERGHE (R.) , « Action en cas de menace contre la paix, de rupture de la paix et d'acte d'agression : Article 39 » *in* COT (J.P.), FORTEAU (M.), PELLET (A.), *La Charte des Nations Unies, Commentaire article par article*, Economica, vol. 2, 3ème édition, 2005, p. 1141 ; AKOTO (E.), « Les cyberattaques étatiques constituent-elles des actes d'agressions en vertu du droit international public ? Deuxième Partie », *op. cit.*, p. 208.

[184] COMBACAU (J.), *Le Pouvoir de sanction de l'O.N.U. : étude théorique de la coercition non militaire*, Paris, Pedone, 1974, p. 16 ; LAGRANGE (E.), EISEMANN (P. M.), « Article 41 » *in* COT (J.P.), FORTEAU (M.), PELLET (A.), *op. cit.*, p. 1200.

[185] AGNU, Rés. 51/242, *Supplément à l'Agenda pour la paix*, 26 septembre 1997, Annexe II, article 5; LAW (J.), MARTIN (E. A.), *A Dictionary of Law*, Oxford University Press, 2014, p. 479 ; RUYS (T.), « Sanctions, retortions and countermeasures: concepts and international legal framework », *in* VAN DEN HERIK (L.), *Research Handbook on UN Sanctions and International Law,* Cheltenham, Edward Elgar, 2017, p.19 ; FARRALL (J. M.), *United Nations Sanctions and the Rule of Law*, Cambridge, Cambridge University Press, 2007, p. 110 ; VERHOEVEN (J.), *op. cit.*, p. 809 ; AHMAD (Z.), *op. cit.*, p. 242.

[186] AGNU, Rés. 51/242, *op. cit.*, Annexe II ; KELSEN (H.), *The Law of the United Nations: A critical Analysis of its fundamental problems*, Stevens & Sons Limited, 1951, pp. 735-737 ; COMBACAU (J.), SUR (S.)*, op. cit.*, p. 697 ; SUBEDI (S.P.), « Conclusions: The Current Law on Unilateral Sanctions, Remedies against Unlawful Use of such Sanctions and Recommendations » *in* SUBEDI (S.P.), *Unilateral Sanctions in International Law*, Hart, 2021, pp. 327.

[187] KHALALEH (Y.), « The Blocke of Qatar : Where Coercive Diplomacy Fails, Principles of Law Should Prevail », *International Law Review*, 2018, p. 50 ; SUBEDI (S.P.), « Introduction » *in* SUBEDI (S. P.), *op. cit.*, p. 1.

[188] *Charte des Nations Unies*, *op. cit.*, Préambule et article 1 ; KOLB (R.), *op. cit.*, p. 39 ; DUPUY (P.-M.), « The Place and Role of Unilateralism in Contemporary International Law », *EJIL*, 2000, vol. 11, pp. 23-24.

[189] *Exposé des faits,* § 25.

*d'expression* »[190], n'a pas sollicité le CS, ni antérieurement ni postérieurement à l'adoption des mesures prises contre le Leoni alors mêmes qu'elles ont été prises le lendemain du détournement de BGP[191] et que l'acte reproché au Dole avait cessé[192], procédure qui contrevient donc à la *Charte.*

**61.** Le Dole, en prenant ainsi des mesures unilatérales, et en l'absence de toute mesure illicite comme démontré *supra,* viole les dispositions de la *Charte des Nations Unies.*

Section 2 : Les mesures prises par le Dole sont illicites et ne sont pas des mesures de rétorsions

**62.** Le Dole qualifie les mesures prises contre le Leoni de mesures de rétorsions. Ce sont des mesures prises par un État ou un groupe d'États qui sont par nature licites[193] mais en réaction à un acte illicite[194]. Le droit des États de recourir à ce type de sanctions unilatérales est limité par les règles conventionnelles et coutumières: toute sanction doit être proportionnée au dommage subi, ne doit pas contrevenir aux règles de *jus cogens* ou à la *Charte des Nations Unies* ou principes généraux du droit international[195]. La licéité des mesures de rétorsion est donc appréciée au cas par cas et la liberté des États d'édicter de telles mesures n'est pas absolue.

**63.** Ces mesures doivent être proportionnelles à l'acte illicite préalablement commis[196], c'est-à-dire être qu'il doit y avoir une équivalence entre l'acte illicite et la réponse qui s'ensuit. Cela implique d'une part, que la réponse n'excède pas le niveau normatif de la violation et d'autre part, que la réaction entraîne des dommages équivalents à ladite violation[197]. Il s'agit de

---

[190] *Ibid.*, § 24.
[191] *Ibid.*, § 25.
[192] *Ibid.*, § 22.
[193] CDI, « Rapport de la Commission du droit international sur les documents de sa quarante-troisième session, " Responsabilité des États " », *Ann. CDI*, document A/CN.4/440 et Add.1, vol. II, 1ère partie, 1991, pp. 10-11 ; EHLERMANN (C. D.), « Communautés Européennes et sanctions Internationales - Une réponse à J. Verhoeven », *RBDI*, 1984-1985, p. 98 ; RUYS (T.), « Sanctions, retortions and countermeasures: concepts and international legal framework », *op. cit.*, p. 24.
[194] CDI, « Rapport de la Commission du droit international sur les documents de sa quarante-troisième session, " Responsabilité des États " », *op. cit.*, p.10 ; THIERRY (H.), COMBACAU (J.), SUR (S.), VALLEE (CH.) *Droit international public*, Paris, Montchrestien, 1975, p. 192 ; DECAUX (E.)*, La réciprocité en droit international*, LGDJ, 1980, p. 224 et p. 229 ; AKEHURST (M.), *A Modern Introduction to International Law*, Harper Collins Publishers Ltd, 5ème édition, 1987, p. 6 ; ZEMANEK (K.) « Responsibility of States : General principles », *in* BERNHARD (R.), *Encyclopedia of public International Law*, Elsevier Science Publishers B.V, 1987, p. 370 ; LEBEN (C.), « Les contre-mesures inter-étatiques et les réactions à l'illicite dans la société internationale », *AFDI*, vol. 28, 1982, p. 14 ; SUBEDI (S.P.), « Conclusions: The Current Law on Unilateral Sanctions, Remedies against Unlawful Use of such Sanctions and Recommendations », *op. cit.*, p. 1.
[195] *Ibid.*, pp. 328-329 ; CANNIZZARO (E.), « The role of proportionality in the law of international countermeasures », *Eur. J. Int'l L.*, vol. 12, n°5, p. 905 ; RYNGAERT (C.), *Jurisdiction in International Law*, Oxford – New-York, Oxford University Press, 2ème édition, 2015, pp. 158-160.
[196] *Ibid.* ; RUYS (T.), « Sanctions, retortions and countermeasures: concepts and international legal framework », *op. cit.*, p. 24.
[197] CANNIZZARO (E.), *op. cit.*, p. 905.

confronter ce que gagne l'auteur de la mesure, face à la charge que cette dernière va imposer à l'autre État[198]. Ainsi, toute mesure qui n'est pas proportionnelle à l'acte illicite à l'origine de la mesure serait illicite[199], d'autant plus que ces mesures sont coercitives et punitives en ce qu'elles ont pour objet de contraindre l'État auteur de l'acte illicite allégué de cesser celui-ci[200].

**64.** Les mesures de rétorsion peuvent prendre la forme de mesures économiques coercitives[201] afin de « *limiter ou priver purement et simplement la liberté financière de l'État visé au moyen de divers instruments économiques ou financiers* »[202] et sont généralement de « *de grande intensité* »[203]. Dans la sphère économique, cela aboutit à retirer un avantage octroyé à l'État visé par la sanction[204]. L'État étant souverain sur son territoire, il exerce cette souveraineté à l'encontre des opérateurs économiques privés ayant la nationalité de l'État visé par les sanctions se trouvant sur son territoire mais doit veiller à respecter les normes conventionnelles coutumières et commerciales[205]. Elles peuvent également consister en des sanctions diplomatiques puisque qu'un État dispose toujours du pouvoir discrétionnaire que lui reconnaît le droit des relations diplomatiques, d'informer à tout moment l'État accréditant que le chef de la mission est *persona non grata*[206]. La Cour considère toutefois qu'il s'agit en réalité d'un moyen de « *remédier aux abus de la fonction diplomatique que peuvent commettre les membres d'une mission à titre individuel* »[207].

**65.** Les mesures prises par le Dole ne sont pas des mesures rétorsions. Ces mesures ne répondent pas à un acte illicite : comme démontré *supra*[208], le détournement de BGP n'est pas un acte illicite voire inamicale. Ce malheureux incident qui a débordé les frontières du Leoni ne visait pas le Dole, le détournement de BGP ne devant initialement avoir lieu que sur le territoire leonien[209]. Les mesures économiques et diplomatiques ne sont pas donc pas proportionnelles

---

[198] RUYS (T.), « Sanctions, retortions and countermeasures: concepts and international legal framework », *op. cit.*, p. 28 ; RYNGAERT (C.), *op. cit.*, p. 160.
[199] SUBEDI (S.P.), « Conclusions: The Current Law on Unilateral Sanctions, Remedies against Unlawful Use of such Sanctions and Recommendations », *op. cit.*, pp. 328-329.
[200] AHMAD (Z.), *op. cit.*, p. 241.
[201] LOWENFELD (A. F.)*, International Economic Law*, Oxford, Oxford University Press, 1ère édition, 2002, p. 69.
[202] SUBEDI (S.P.), « Introduction », *op. cit.*, p. 1.
[203] *Ibid.*
[204] BOTHE (M.), « Compatibility and Legitimacy of Sanctions Regimes », *in* RONZITTI (N.), *Coercive Diplomacy, Sanctions and International Law*, Brill, Nijhoff, 2016, p. 33.
[205] PICCHIO FORLATI (L.), « The Legal Core of International Economic Sanctions » *in* PICCHIO FORLATI (L.), SICILIANOS (L.-A.), *Les sanctions économiques en droit international,* Académie de droit internationale La Haye, Brill, Nijhoff, 2004, pp. 101 - 104 ; AHMAD (Z.), *op. cit.*, pp. 241-243.
[206] *Convention de Vienne sur les relations diplomatiques*, adoptée à Vienne le 18 avril 1961, entrée en vigueur le 24 avril 1964, article 9 ; COLLIARD (C.-A.) « La Convention de Vienne sur les relations diplomatiques », *AFDI*, vol. 7, 1961, p. 16.
[207] CIJ, arrêt du 24 mai 1980, *Personnel diplomatique et consulaire des Etats-Unis à Téhéran (États-Unis c. Iran), Rec*. 1980, p. 3, §85.
[208] V. *supra*, §§ 50-52
[209] *Exposé des faits*, § 23.

au détournement de BGP. L'expulsion des diplomates léoniens se trouvant au Dole n'avaient commis aucun acte illicite et la motivation du Dole de les expulser n'est pas liée à leur mission diplomatique[210]. De même, le fait de restreindre les exportations de services de LeoWeb au Dole ne vise pas spécifiquement l'État léonien mais une entreprise privée léonienne, ce qui constitue un acte contraire aux obligations conventionnelles du Dole, celui-ci étant membre de l'Organisation mondiale du commerce qui interdit de telles restrictions arbitraires. Enfin, la dénonciation de l'entente conclue entre le Dole et le Leoni contrevient au droit des traités, la procédure de dénonciation prévue par la *Convention de Vienne sur le droit des traités* de 1969 n'étant pas respectée. Toutes ces mesures ont été prises le lendemain du détournement du BGP alors même que celui-ci n'avait plus lieu. Elles n'ont donc pas pour objet de faire cesser un acte prétendument illicite mais de punir le Leoni d'une erreur humaine commise.

**66**. Par conséquent, les mesures prises par le Dole ne sont pas des mesures de rétorsions et sont illicites.

**67.** Au regard de tout ce qui précède, le Leoni prie la Cour de dire et juger que le Dole a pris des mesures qui sont illicites au regard du droit international, les mesures prises le défendeur n'étant pas des sanctions en ce qu'elles ne répondent pas à aucun acte illicite ni des mesures de rétorsions en ce qu'elles sont illicites en elles-mêmes, ce qui ce qui engage sa responsabilité.

[210] *Ibid.*, § 25.

## CONCLUSIONS

---

**64.** Le Leoni demande à la Cour de dire et de juger que :

- la responsabilité internationale du Dole est engagée du fait des activités menées par le collectif NoVox afin d'interférer dans le cours de la campagne électorale leonienne de 2020.
- la responsabilité internationale du Dole est engagée du fait de l'installation du programme malveillant « Crépuscule » dans le système informatique du port de Vaneti, à des fins d'espionnage et de sabotage d'une infrastructure critique ;
- les sanctions diplomatiques et économiques prises par le Dole le 2 octobre 2020 à l'encontre du Leoni sont illicites au regard du droit international et engagent sa responsabilité internationale.

## BIBLIOGRAPHIE ET TABLE DES JURISPRUDENCES

---

# I. LÉGISLATIONS : SOURCES INTERNATIONALES - INSTRUMENTS CONVENTIONNELS ET DÉRIVÉS

## A. Conventions internationales


- *Charte des Nations-Unies*, adoptée le 26 juin 1945 à San Francisco, entrée en vigueur le 24 octobre 1945.
- *Statut de la Cour internationale de Justice*, annexe à la *Charte des Nations Unies* adoptée le 26 juin 1945 à San Francisco, entrée en vigueur le 24 octobre 1945.
- *Convention de Vienne sur les relations diplomatiques*, adoptée à Vienne le 18 avril 1961, entrée en vigueur le 24 avril 1964.
- *Convention de Budapest sur la cybercriminalité*, adoptée à Budapest le 23 novembre 2001, entrée en vigueur le 1er juillet 2004.


## B. ACTES ET RÉSOLUTIOONS D'ORGANISATIONS INTERNATIONALES

1) Organisation des Nations Unies (ONU)

a) Conseil de Sécurité des Nations Unies


- S/RES/232, « Rhodésie du Sud », 16 décembre 1966.
- S/RES/242, « La situation au Moyen-Orient », 22 novembre 1967.
- S/RES/2341, « Protection des infrastructures essentielles contre les attaques terroristes », 13 février 2017.


b) Assemblée générale des Nations Unies


- A/RES/2131 (XX), *Déclaration sur l'inadmissibilité de l'intervention dans les affaires intérieures des États et la protection de leur indépendance et de leur souveraineté*, 21 décembre 1965.

- A/RES/2625 (XXV), *Les principes du droit international touchant aux relations amicales entre Etats*, 24 octobre 1970.
- A/RES/3314 (XXIX), *Définition de l'agression*, 14 décembre 1974.
- A/RES/36/103, *Déclaration sur l'inadmissibilité de l'intervention et de l'ingérence dans les affaires intérieures de l'Etat*, 9 décembre 1981.
- A/RES/51/242, *Supplément à l'Agenda pour la paix*, 26 septembre 1997.
- A/RES/56/83, *Responsabilité de l'État pour fait internationalement illicite*, 12 décembre 2001.
- A/RES/58/199, *Création d'une culture mondiale de la cybersécurité et protection des infrastructures essentielles de l'information*, 30 janvier 2004.
- A/68/98, *Rapport du Groupe d'experts gouvernementaux chargé d'examiner les progrès de la téléinformatique dans le contexte de la sécurité internationale*, 24 juin 2013.
- A/70/174, *Rapport du Groupe d'experts gouvernementaux chargé d'examiner les progrès de la téléinformatique dans le contexte de la sécurité internationale,* 22 juillet 2015.
- A/R/73/27, *Progrès de l'informatique et des télécommunications et sécurité internationale*, 5 décembre 2018.

c) Commission du Droit International

- CDI, « Rapport de la Commission du droit international sur les travaux de sa dixième session », *Ann. CDI*, A/3859, *vol. II*, 1958, pp. 81-145.
- AGO (R.), « Quatrième rapport sur la responsabilité des États », *Ann. CDI*, vol. II, 1972, 174 p.
- CDI, « "Force majeure" et "cas fortuit" en tant que circonstances excluant l'illicéité: pratique des Etats, jurisprudence internationale et doctrine », *Ann. CDI,* document A/CN.4/315, vol. II, 1ère partie, 1978.
- CDI, « Rapport de la Commission du droit international sur les documents de sa quarante-troisième session, "Responsabilité des États" », *Ann. CDI*, document A/CN.4/440 et Add.1, vol II, 1ère partie, 1991, pp. 7-37.
- CDI, « Projets d'articles sur la responsabilité de l'État pour fait internationalement illicite et commentaires y relatif », *Ann. CDI*, vol. II(2), 2001, pp. 61-393.

- CDI, « Principes directeurs applicables aux déclarations unilatérales des États susceptibles de créer des obligations juridiques et commentaires y relatifs », *Ann. CDI*, 2006, vol. II (2), pp. 387-400.
- CDI, *La commission du droit international et son œuvre - septième édition*, New-York, Nations Unies, vol. I, 2009, 466 p.

d) Institut des Nations Unies pour la recherche sur le désarmement (UNIDIR)

- MELZER (N.), *Cyberwarfare and International Law*, Institut des Nations Unies pour la recherche sur le désarmement (UNIDIR), Genève, coll. Resources, 2011, 38 p.

2) Union Européenne

- Commission européenne, COM(2005) 576 final, *Livre Vert sur un Programme Européen de Protection des Infrastructures Critiques*, 17 novembre 2005.
- Commission Européenne, *Plan d'action contre la désinformation, Communication conjointe au Parlement européen, au Conseil européen, au Conseil, au Comité économique et social européen, et au Comité des régions*, Bruxelles, 5 décembre 2018, 20 p.

3) Organisation de Shanghai pour la coopération

- *Agreement between the governments of state members of the Shanghai Cooperation Organization on cooperation in the field of ensuring international information security*, Shanghai Cooperation Organization, 16 juin 2009.

4) Organisation du Traité de l'Atlantique Nord

- O.T.A.N., *Trends in international law for cyberspace*, CCDCOE Nato Cooperative Cyber defence centre of excellence, mai 2019, 8 p.

## II. INDEX DE JURISPRUDENCE

### A. Cour Permanente de Justice Internationale

Avis consultatifs

- CPJI, avis consultatif du 7 février 1923, *Décrets de nationalité promulgués en Tunisie et au Maroc,* Série B, n°4, p. 7

Arrêts

- CPJI, arrêt du 7 septembre 1927, *Affaire du Lotus (France c. Turquie)*, *Rec.* série A, n°10, p. 4.
- CPJI, arrêt du 13 septembre 1928, *Usine de Chorzów,* série A, n°13, p. 4.

### B. Cour Internationale de Justice

Avis consultatifs

- CIJ, avis consultatif du 11 avril 1949, *Réparation des dommages subis au service des Nations Unies, Rec.* 1949, p. 174
- CIJ, avis consultatif du 20 juillet 1962, *Certaines dépenses des Nations Unies (article 17, paragraphe 2, de la Charte)*, *Rec.* p. 151.
- CIJ*,* avis consultatif du 8 juillet 1996, *Licéité de la menace ou de l'emploi des armes nucléaires*, *Rec.* 1996, p. 226.
- CIJ, avis consultatif du 25 février 2019, *Effets juridiques de la séparation de l'archipel des Chagos de Maurice en 1965*, *Rec.* 2019, p. 95.

Ordonnances

- CIJ, ordonnance du 22 novembre 2013*, Certaines activités menées par le Nicaragua dans la région frontalière (Costa Rica c. Nicaragua)*, *Rec.* 2013, p. 354

Arrêts

- CIJ, arrêt du 9 avril 1949, *Affaire du détroit de Corfou (Royaume-Uni de Grande-Bretagne c. Albanie)*, *Rec.* 1949, p. 4.
- CIJ, arrêt du 26 mai 1961, *Affaire du Temple de Préah Vihéar (Cambodge c. Thaïlande),* exceptions préliminaires, *Rec.* 1961, p. 17.
- CIJ, arrêt du 20 février 1969, *Affaire du Plateau continental de la mer du Nord*, *Rec.* 1969, p. 7
- CIJ, arrêt du 24 mai 1980, *Affaire relative au personnel diplomatique et consulaire des Etats-Unis à Téhéran, (Etats-Unis d'Amérique c. Iran), Rec.* 1980, p. 3.
- CIJ, arrêt du 27 juin 1986, *Affaire des activités militaires et paramilitaires au Nicaragua et contre celui-ci (Nicaragua c. Etats-Unis d'Amérique)*, fond, *Rec.* 1986, p. 14.
- CIJ, arrêt du 22 décembre 1986, *Affaire du différend frontalier (Burkina Faso c. République du Mali), Rec.* 1986, p. 573
- CIJ, arrêt du 25 septembre 1997, *Affaire relative au projet Gabčíkovo-Nagymaros (Hongrie c. Slovaquie), Rec.* 1997, p. 7.
- CIJ, arrêt du 6 novembre 2003, *Affaire des Plateformes pétrolières (République islamique d'Iran c. États-Unis d'Amérique*), *Rec*. 2003, p. 161.
- CIJ, arrêt du 19 décembre 2005, *Activités armées sur le territoire du Congo (République démocratique du Congo c. Ouganda)*, *Rec.* 2005, p. 168.
- CIJ, arrêt du 3 février 2006, *Activité*s *armées sur le territoire du Congo (nouvelle requête :2002) (République démocratique du Congo c. Rwanda),* compétence et recevabilité *Rec.* 2006, p. 6.
- CIJ, arrêt du 26 février 2007, *Application de la convention pour la prévention et la répression du crime de génocide (Bosnie-Herzégovine c. Serbie-et-Monténégro), Rec.* 2007, p. 43.
- CIJ, arrêt du 20 avril 2010, *Affaire relative aux Usines de pâte à papier sur le fleuve Uruguay (Argentine c. Uruguay)*, *Rec.* 2010, p. 14.
- CIJ, arrêt du 30 novembre 2010, *Ahmadou Sadio Diallo (République de Guinée c. République démocratique du Congo), Rec*. 2010, p. 639.
- CIJ, arrêt du 20 juillet 2012, *Questions concernant l'obligation de poursuivre ou d'extrader (Belgique c. Sénégal), Rec.* 2012, p. 422.
- CIJ, arrêt du 9 février 2022, *Affaire Activités armées sur le territoire du Congo (République démocratique du Congo c. Ouganda).*

Opinions dissidentes

- CIJ, arrêt du 26 février 2007, *Application de la convention pour la prévention et la répression du crime de génocide (Bosnie- Herzégovine c. Serbie et Monténégro)*, *op.cit*., opinion dissidente du juge AL-KHASAWNEH, p. 241.
- CIJ, arrêt du 26 février 2007, *Application de la Convention pour la prévention et la répression du crime de génocide (Bosnie-Herzégovine c. Serbie-et-Monténégro)*, *Rec.* 2007, p. 43, Opinion dissidente du juge MAHIOU, p. 381.

## C. Sentences arbitrales

- SA du 11 mars 1941, *Affaire de la Fonderie du Trail (Canada c. États-Unis), RSA,* vol. III, p. 1905.
- SA du 1er mai 1925, *Affaire des Réclamations britanniques dans la zone espagnole du Maroc, (Grande Bretagne c. Espagne)*, *RSA*, vol. II, p. 649.
- SA du 4 avril 1928, *Affaire de l'Île de Palmas (Pays-Bas c. Etats-Unis d'Amérique)*, *RSA*, vol. II, pp. 829-871.
- SA du 24/27 juillet 1956, *Affaire relative à la concession des phares de l'Empire ottoman (Grèce c. France), RSA*, vol. II, pp. 155-269.
- SA du 16 novembre 1957, *Affaire du lac Lanoux* (*Espagne c. France*), *RSA*, vol. XII, pp. 281 – 317.
- SA du 30 avril 1990, *Rainbow Warrior (Nouvelle-Zélande c. France), RSA*, vol. XX, 1990, pp. 215-284.

## D. Cour Européenne des Droits de l'Homme

- CEDH, arrêt du 18 décembre 1996, *Affaire Loizidou c. Turquie*, req. n° 15318/89.
- CEDH, arrêt du 10 mai 2001, *Affaire Chypre c. Turquie*, req. n° 25781/94.

## E. Cour Interaméricaine des droits de l'Homme

- Cour IADH, 27 juin 2012, *Affaire du Peuple autochtone Kichwa de Sarayaku c. Equateur, mérites et réparations*, série C, N° 245.

**F. <u>Cour Pénale Internationale</u>**

- CPI, arrêt du 29 janvier 2007, *Le Procureur c/ Thomas Lubanga Dyilo*, n° ICC-01/04-01/06.

**G. <u>Tribunal pénal international pour l'ex-Yougoslavie</u>**

- TPI-Y, arrêt du 15 juillet 1999, *Le Procureur c. Dusko Tadic*, n°IT-94-1-A.

**H. <u>Tribunal des réclamations de l'Iran et des Etats-Unis</u>**

- IUSCT,18 et 19 février 1987, *Affaire Kenneth P. Yeager c/ La République islamique d'Iran*, n° 10199.

## III. DOCTRINE

### A. OUVRAGES GÉNÉRAUX


- AKEHURST (M.), *A Modern Introduction to International Law*, Harper Collins Publishers Ltd, 5ème édition, 1987, 310 p.
- ALEDO (L.-A.), *Le droit international public*, Dalloz, 4ème édition, 2021, 176 p.
- ALLAND (D.), *Manuel de droit international public*, Paris, P.U.F., 8ème édition, 2021, 336 p.
- BLIN (O.), *Droit international public général*, Bruylant, 2ème édition, 2019, 320 p.
- CANAL-FORGUES (E.), RAMBAUD (P.), *Droit international public*, Barcelone, Champs université, 3ème édition, 2016, 502 p.
- CARREAU (D.), MARRELLA (F.), *Droit international public*, Paris, Pedone, 12ème édition, 2018, 767 p.
- COMBACAU (J.), SUR (S.), *Droit international public*, Paris, Précis Domat, 13ème édition, 2019, 882 p.
- DAILLIER (P.), FORTEAU (M.), PELLET (A.), *Droit international public*, Paris, LGDJ, 8ème édition, 2009, 1709 p.
- DECAUX (E.), DE FROUVILLE (O.), *Droit International Public*, Paris, Dalloz, 12ème édition, 2020, 643 p.
- DUPUY (P.-M.), KERBRAT (Y.), *Droit international public*, Paris, Dalloz, 15ème édition, 2020, 960 p.
- FLEURY GRAFF (T.), *Manuel de droit international public*, Paris, PUF, vol. II, 1ère édition, 2016, 272 p.
- GRANT (J. P.), BARKER (J. C.), PARRY (C.), *Parry and Grant Encyclopaedic dictionary of International Law,* Oxford, New-York, Oxford University Press, 3ème édition, 2009, 691 p.
- LAW (J.), MARTIN (E.), *A Dictionary of Law*, Oxford University Press, 7ème édition, 2014, 602 p.
- MORELLI (G.), *Notions de droit international public*, Paris, Pedone, 7ème édition, 2013, 295 p.
- NDIOR (V.), *Dictionnaire de l'actualité internationale*, Paris, Pedone, 2021, 569 p.
- RIVIER (R.), *Droit international public,* Paris, PUF, 3ème édition, 2017, 841 p.
- SALMON (J.) (dir.), *Dictionnaire de droit international public*, Bruxelles, Bruylant,

2001, 1198 p.
- SHAW (M.N.), *International Law*, Cambridge, New-York, Cambridge University Press, 7ème édition, 2014, 981 p.
- TOURME-JOUANNET (E.), *Le droit international,* Paris, P.U.F.*,* 2013, 126 p.
- THIERRY (H .), COMBACAU (J.), SUR (S.), VALLEE (CH.), *Droit international public*, Paris, Montchrestien, 1975, 770 p.
- SINKONDO (M.), *Droit international public*, Paris, Ellipses, 1999, 508 p.
- VERHOEVEN (J.), *Droit international public*, Bruxelles, Larcier, 2000, 856 p.

## B. MONOGRAPHIES

- AHMAD (Z.), *WTO Law and Trade Policy Reform for Low-Carbon Diffusion Technology Diffusion*, Brill, Nijhoff, vol. 5, 2021, 308 p.
- BANNELIER (K.), CHRISTAKIS (T.), *Cyberattaques - Prévention-réactions : rôle des États et des acteurs privés,* Paris, Les Cahiers de la Revue Défense Nationale, , 2017, 90 p.
- BAUDIN (L.), *Les cyberattaques dans les conflits armés : qualification juridique, imputabilité et moyens envisagés en droit humanitaire*, Paris, L'Harmattan, 2014, 246 p.
- BESSON (S.), *La due diligence en droit international,* La Haye, Brill, Nijhoff, vol.46, 2021, 363 p.
- COMBACAU (J.), *Le Pouvoir de sanction de l'O.N.U. : étude théorique de la coercition non militaire*, Paris, Pedone, 1974, 394 p.
- CORTEN (O.), *Le droit de la guerre - L'interdiction du recours à la force en droit international contemporain*, Paris, Pedone, 3ème édition, 2020, 903 p.
- CRAWFORD (J.), *Les articles de la CDI sur la responsabilité de l'État*, Paris, Pedone, 2003, 462 p.
- CRAWFORD (J.), KOSKENNIEMI (M.), *The Cambridge companion to International Law*, Cambdridge, Cambridge University Press, 2012, 471 p.
- DECAUX (E.)*, La réciprocité en droit international*, LGDJ, 1980, 374 p.
- DINSTEIN (Y.), *The Conduct of Hostilities under the Law of International Armed Conflict*, Cambridge, Cambdridge University Press, 2004, 275 p.
- FARRALL (J. M.), *United Nations Sanctions and the Rule of Law*, Cambdridge, Cambridge University Press, 2007, 542 p.

- Program on Humanitarian Policy and Conflict Research at Harvard University, H. P. C. R. *Manual on International Law Applicable to Air and Missile Warfare*, Cambridge, Cambridge University Press, 2013, 504 p.
- KELSEN (H.), *The Law of the United Nations: A critical Analysis of its fundamental problems*, Stevens & Sons Limited, 1951, 994 p.
- LOWENFELD (A. F.), *International Economic Law*, Oxford, Oxford University Press, ère édition, 2002, 776 p.
- POLEMI (N.), *Port Cybersecurity: Securing Critical Information Infrastructures and Supply Chains*, Elsevier, 1ère edition, 2017, 214 p.
- ROSCINI (M.), *Cyber operations and the Use of Force in International Law*, Oxford, Oxford University Press, 1ère edition, 2014, 308 p.
- RYNGAERT (C.), *Jurisdiction in International Law*, Oxford – New-York, Oxford University Press, 2ème édition, 2015, 262 p.
- SCHMITT (M. N) (GE), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge, Cambridge University Press, 1st edition, 2013, 300 p.
- SCHMITT (M. N.) (GE), *Tallinn Manual 2.0 on the International Law applicable to cyber operations,* Cambridge, Cambridge University Press, 2017, 598 p.
- SHARP (W. G.), *Cyberspace and the Use of Force*, Ageis Research Corp, 1999, 234 p.
- TURK (P.), VALLAR (C.) (dir.), *La souveraineté numérique, le concept, les enjeux*, Mare & Martin, 2017, 239 p.
- WOLTAG (J.-C.), *Cyber Warfare : computer network operations outside of armed conflict*, Intersentia, 1ère édition, 2014, 313 p.

## C. ARTICLES D'OUVRAGES COLLECTIFS

- BANNELIER-CHRISTAKIS (K.), « Is the principle of distinction still relevant in cyberwarfare? From doctrinal discourse to States' practice », *in* TSAGOURIAS (N.), BUCHAN (R.), *Research Handbook on International Law and Cyberspace*, Edward Elgar , 2015, 2ème éd., pp. 427-455.
- BANNELIER (K.), « Le standard de due diligence et la cyber-sécurité », *in* SFDI, *Le standard de due diligence et la responsabilité internationale,* SFDI, Paris, Pedone, 2018, pp. 67-91.
- BESSON (S.), *«* Sovereignty *», in* WOLFRUM (R.), *The Max Planck Encyclopedia of public international law*, vol. VIII, Oxford University Press, 2012, pp. 366-391

- BOTHE (M.), « Compatibility and Legitimacy of Sanctions Regimes », *in* RONZITTI (N.), *Coercive Diplomacy, Sanctions and International Law*, Brill Nijhoff, 2016, pp. 33-42.
- CONFORTI (B.), « Le principe de non-intervention » *in* BEDJAOUI (M.) (dir.), *Droit international : bilan et perspectives*, Paris, Pedone, 1991, pp. 489-505.
- D'ARGENT (P.), D'ASPREMONT (L.), DOPAGNE (F.), VAN STEENBERGHE (R.) , «Action en cas de menace contre la paix, de rupture de la paix et d'acte d'agression : Article 39 » *in* COT (J.P.), FORTEAU (M.), PELLET (A.), *La Charte des Nations Unies, Commentaire article par article*, Economica, Vol. 2, 3ème édition, 2005, pp. 1131 – 1170.
- EHRIEL (C.), « Souveraineté et innovation : trouver l'équilibre », *in* BLANDIN-OBERNESSER (A.) (dir.), *Droits et souveraineté numérique en Europe*, Bruylant, 2016, pp. 91-95.
- GUILLAUME (G.), « Article 2, § 7 » *in* COT (J.P.), FORTEAU (M.), PELLET (A.) (dir.), *La Charte des Nations Unies, Commentaire article par article*, Economica, 3ème édition, vol. I, pp. 485 – 509.
- HOFMANN (R.), « International Law and the Use of Military Force Against Iraq », *in* DELBRÜCK (J.), HOFMANN (R.), ZIMMERMANN (A.), *German Yearbook of International Law - Jahrbuch für Internationales Recht*, Duncker & Humblot GmbH, vol. 45, 2003, pp. 9-34.
- KOIVUROVA (T.), *«* Due diligence *», in* WOLFRUM (R.), *The Max Planck Encyclopedia of public international law*, vol. III, Oxford University Press, 2012, pp. 236-246.
- KEES (A.), *«* Responsibility of States for private actors *», in* WOLFRUM (R.), *The Max Planck Encyclopedia of public international law*, Oxford University Press, vol. VIII, 2012, pp. 959- 965.
- KUNIG (P.), *«* Intervention, Prohibition of *», in* WOLFRUM (R.), *The Max Planck Encyclopedia of public international law*, vol. VI, Oxford University Press, 2012, pp. 289-299.
- LAGRANGE (E.), EISEMANN (P. M.), « Article 41 » *in* COT (J.P.), FORTEAU (M.), PELLET (A.), *La Charte des Nations Unies, Commentaire article par article*, Economica, Vol. 2, 3ème édition, 2005, pp. 1195 – 1242.
- ORAKHELASHVILI (A.), « Changing Jus Cogens through State practice? The case of the Prohibition of the Use of Force and its Exceptions », *in* WELLER (M.), RYLATT

(J.W.), SOLOMOU (A.), *The Oxford Handbook of the Use of Force in International Law*, Oxford, Oxford University Press, 2015, pp. 157-175.

- PICCHIO FORLATI (L.), « The Legal Core of International Economic Sanctions » *in* PICCHIO FORLATI (L.), SICILIANOS (L.-A.), *Les sanctions économiques en droit international,* Académie de droit internationale La Haye, Brill, Nijhoff, 2004, pp. 99 - 207.
- PISILLO MAZZESCHI (R.) « Le standard de due diligence comme extension ou limite de la responsabilité internationale *»*, *in* SFDI, *Le standard de due diligence et la responsabilité internationale*, Paris, Pedone, 2018, pp. 225-239.
- ROSCINI (M.), « World Wide Warfare—Jus ad bellum and the Use of Cyber Force », *in* Armin BOGDANDY (A.), WOLFRUM (R.), *Max Planck Yearbook of United Nations Law*, vol. 14, 2010, pp. 85-130.
- RUYS (T.), « Sanctions, retortions and countermeasures: concepts and international legal framework », *in* VAN DEN HERIK (L.), *Research Handbook on UN Sanctions and International Law*, Cheltenham, Edward Elgar, 2017, pp. 19-51.
- SALMON (J.), « L'intention en matière de responsabilité internationale », *in Le droit international au service de la paix, de la justice et du développement* : *Mélanges Michel Virally* Paris, Pedone, 1991, pp. 413-422.
- SZPUNA (M.), « Territoriality of Union Law in the Era of Globalisation », in PETRLIK (D.), BOBEK (M.), PASSER (J.) et MASSON (A.) (dir.), *Évolution des rapports entre les ordres juridiques de l'Union européenne, international et nationaux*, Liber Amicorum Jiří Malenovský, Bruylant, 2020, 1ère édition, pp. 149- 168.
- SUBEDI (S. P.), « Introduction » *in* SUBEDI (S.P.), *Unilateral Sanctions in International Law*, Hart, 2021, pp. 1 – 17.
- SUBEDI (S. P.), « Conclusions: The Current Law on Unilateral Sanctions, Remedies against Unlawful Use of such Sanctions and Recommendations », *in* SUBEDI (S.P.), *Unilateral Sanctions in International Law*, Hart, 2021, pp. 327 – 342.
- WOLTAG (J.-C.), *«* Internet *», in* WOLFRUM (R.), *The Max Planck Encyclopedia of public international law*, Oxford University Press, vol. VI, 2012, pp. 227-238.
- ZEMANEK (K.), « Armed attacks », *in* LACHENMANN (F.), RÜDIGER (W.), *The law of armed conflict and the use of force*: *The Max Planck Encyclopedia of Public International Law*, Oxford University Press, 1st edition, 2017, pp. 26-31.

- ZEMANEK (K.), « Responsibility of States: General principles », *in* BERNHARD (R.), *Encyclopedia of Public International Law*, Elsevier Science Publishers B.V, 1987, pp. 362-372.

## D. COURS ET CONFÉRENCES

- CONDORELLI (L), « L'imputation à l'Etat d'un fait internationalement illicite: solutions classiques et nouvelles tendances », *RCADI,* 1984, vol. 189, 221 p.
- PREUSS (L.), *«* Article 2, paragraph 7 of the Charter of the United Nations and Matters of domestic juridiction *»*, *RCADI*, vol. I, tome 74, 1949, pp. 553-652.
- ROUSSEAU (C.), « L'indépendance de l'Etat dans l'ordre international », *RCADI*, vol. 73, 1948, , pp. 167-253.

## E. ARTICLES DE PÉRIODIQUES

- AKOTO (E.), « Les cyberattaques étatiques constituent-elles des actes d'agressions en vertu du droit international public ? : Première Partie », *Revue de droit d'Ottawa*, 2015, 46 (1), pp. 1 – 24.
- AKOTO (E.), « Les cyberattaques étatiques constituent-elles des actes d'agressions en vertu du droit international public ? Deuxième Partie », *Revue de droit d'Ottawa,* 2015, 46 (2), pp. 199 – 230.
- ASCENSIO (H.), « La responsabilité selon la Cour internationale de Justice dans l'affaire du génocide bosniaque », *RGDIP*, 2007, n° 2, pp. 285-303.
- BANNELIER (K.), « Cyber Diligence: A Low-Intensity Due Diligence Principle for Low-Intensity Cyber Operations »*, Baltic Yearbook of International Law, (Brill),* 2014, vol. 14, pp. 23-39.
- BANNELIER (K.), « Obligations dans de diligence dans le cyberespace : qui a peur de la cyber-diligence », *RBDI*, 2017/2, pp. 612-665.
- BARAT-GINIES (O.), « Existe-t-il un droit international du cyberespace?», *Hérodote*, 2014, n°152-153, pp. 201-220.
- BOWETT (D.W.), «Economic Coercion and Reprisals by States», T*he Virginia Journal of International Law*, vol.18, n°1, 1972, pp. 1-12.

- BROWN (D.), « A Proposal for an International Convention To Regulate the Use of Information Systems in Armed Conflict », *Harvard International Law Journal*, vol. 47, 2006, pp. 179-221.
- CASSESE (A.), « The Nicaragua and Tadic Tests Revisited in Light of the ICJ Judgment on Genocide in Bosnia », *Eur. J. Int'l L.*, vol. 18, n° 4, 2007, pp. 649-668
- CANNIZZARO (E.), « The role of proportionality in the law of international countermeasures », *Eur. J. Int'l L, vol*. 12, n°5, pp. 889-916.
- COLLIARD (C-A.) « La Convention de Vienne sur les relations diplomatiques », *AFDI,* vol. 7, 1961. pp. 3-42.
- CONDE (P. Y.), « L'Affaire du génocide : Bosnie et Serbie devant la Cour internationale de Justice ou la dénonciation à l'épreuve du droit international », *Droits et cultures*, 2009 - 2, p. 109-140.
- CONDRON (S.M.), « Getting it right: Protecting American critical infrastructure in cyberspace », *Harvard Journal of Law & Technology, vol.* 20, n° 2, 2007, pp. 403-422.
- CORTEN (O.), « L'arrêt rendu par la CIJ dans l'affaire du *Crime de génocide (Bosnie-Herzégovine c/ Serbie)* : vers un assouplissement des conditions permettant d'engager la responsabilité d'un État pour génocide ? », *AFDI*, vol. 53, 2007, pp. 249-279.
- DAVID (E.), « Portée et limite du principe de non-intervention », *RBDI,* 1990/2, pp. 350-367
- DROEGE (C.), «Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians», *International Review of the Red Cross,* vol. 94, n° 886, 2013, pp. 533-578.
- DUPUY (P.-M.), « The Place and Role of Unilateralism in Contemporary International Law », *EJIL*, 2000, vol. 11, pp. 19 – 29.
- EHLERMANN (C. D.), « Communautés Européennes et sanctions Internationales - Une réponse à J. Verhoeven », *RBDI*, 1984-1985, pp. 97-112.
- FERRARO (T.), « La position juridique du CICR sur la qualification des conflits armés incluant une intervention étrangère et sur les règles du DIH applicables à ces situations », *RICR*, vol. 97, Sélection française, 2015, pp. 181-206.
- FLORY (M.), « Souveraineté », *Répertoire de droit international*, décembre 1998 (actualisation : juin 2015), 18 p.
- FORTEAU (M.), « L'Etat selon le droit international : une figure à géométrie variable?», *RDGIP*, 2007-2, pp. 737-768

- FRANZESE (P.W.) « Sovereignty in cyberspace : Can it exist? », *The Air Force Law Review,* vol. 64, 2009, pp. 1-42.
- GEISS (R.), LAHMANN (H.), « Cyber warfare: applying the principle of distinction in an interconnected space », *Israel Law Review, vol*. 45 (3), 2012, pp. 381-399.
- HARRISON DINNISS (H.), « Attacks and Operations: The debate over computer network 'attacks'», *The Minerva Center for Human Rights*, 28-29 November 2011, pp. 1-9.
- HOFER (A.), « The proportionality of unilateral "targeted" sanctions: whose interests should count », *Nordic Journal of International Law*, *vol*. 89, 2020, pp. 399-421.
- KHALALEH (Y.), « The Blocke of Qatar : Where Coercive Diplomacy Fails, Principles of Law Should Prevail », *International Law Review*, 2018, pp. 45-63.
- KOLB (R.), « Considérations générales sur la violence et le droit international », *AFRI*, 2005, vol. VI, pp. 27 – 44.
- TALBOT JENSEN (E.), « Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense », *Stanford Journal of International Law*, vol. 38, 2002, pp. 207-240.
- TALBOT JENSEN (E.T.), « The Tallin Manual 2.0: Highights and insights », *Georgetown Journal of International Law,* 2017*,* vol. 48, pp. 735-778.
- LEBEN (C.), « Les contre-mesures inter-étatiques et les réactions à l'illicite dans la société internationale », *AFDI, vol*. 28, 1982, pp. 9-77.
- RUYS (T.), « The Meaning of Force and the Boundaries of Jus ad bellum : Are minimal uses of force excluded from UN Charter 2(4)? », *The American Journal of International Law*, vol. 108, n° 2, 2014, pp. 159-210.
- SCHAAP (A. J.), « Cyber Warfare Operations: Development and Use Under International Law »*, The Air Force Law Review,* vol. 64, 2009, pp. 121-173.
- SCHMITT (M. N.), « Foreign Cyber Interference in Elections »*, International Law Studies,* 2021, vol. 97, pp 730-764.
- SCHONDORF (R.) « Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations », *International Law Studies*, 2021, vol. 97, pp. 395-406.
- SOREL (J.M.), « Les multiples lectures d'un arrêt : entre sentiment d'impunité et sentiment de cohérence, une décision à relativiser », RGDIP, 2007/2, pp. 259-272.
- THOUVENIN (J.M.) « Sanctions économiques en droit international », *Droits*, 2013, n°57, pp. 161-176.

- TOUGAS (M.L.) « Commentaire de la Partie 1 du Document de Montreux sur les obligations juridiques pertinentes et les bonnes pratiques pour les États en ce qui concerne les opérations des entreprises militaires et de sécurité privées pendant les conflits armés », *RICR*, vol. 96, Sélection française, 2014, pp. 237-292.
- WATTS (S.), RICHARD (T.), « Baseline territorial sovereignty and cyberspace », *Lewis and Clark Law Review*, 2018, pp. 803-872.
- WAXMAN (M.C.), « Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4) », *Yale Journal of International Law*, vol. 36, 2010, pp. 421-459.
- WECKEL (P.), « L'arrêt sur le génocide : le souffle de l'avis de 1951 n'a pas transporté la Cour », *RGDIP*, 2007, pp. 305-331.
- YUYING LIU (I.), « La doctrine de la diligence raisonnable en vertu du Manuel de Tallinn 2.0 », *in Computer Law & Security Review,* vol. 33, avril 2017, pp. 390–395.
- ZIOLKOWSKI (K.), « Computer Network Operations and the Law of Armed Conflict », *Military Law and Law of War Review*, vol. 49, 2010, pp. 47-94.

## F. Rapports et autres études

- Observation électorale et l'appui à la démocratie, *Recueil des normes internationales pour les élections*, Luxembourg, Office des publications de l'Union Européenne, 4ème édition, 2016, 311 p.
- C.E.I.S., « Analyse du Manuel de Tallinn 2.0 sur le droit international applicable aux cyber-opérations », *Étude prospective et stratégique*, 29 novembre 2017, 73 p.
- ILA*, Study Group on Due Diligence International Law - Second Report*, juillet 2016, 48 p. , file:///home/chronos/u-2aec3df9fcae26be235e20b1df6aa72ef32e0805/MyFiles/Downloads/Draft%20Study%20Group%20Report%20Johannesburg%202016.%20(2).pdf
-
- FRANCESCHINI (L.), *Analyse juridique de la proposition de la loi française relative à la lutte contre la manipulation de l'information au regard des principes internationaux régissant la liberté de l'information*, novembre 2018, 24 p.

## G. SITES INTERNET ET PUBLICATIONS EN LIGNE

- CHOUKRI (I.), « Remarques sur les Manuels de Tallinn (1.0 et 2.0) et le droit international applicable aux cyber-opérations. Paix et sécurité européenne et internationale », *PSEI*, 2018, https://halshs.archives-ouvertes.fr/halshs-03156559
- DE FROUVILLE (O.) « L'attribution d'un fait à l'Etat - Les personnes privées », *in* BODEAU (P.), CRAWFORD (J.), PELLET (A.), SZUNEK (S.) (dir.), *Le droit de la responsabilité internationale*, Paris, 2016, https://www.frouville.com/wp-content/uploads/2020/05/FROUVILLE-RESPONSABILITE-1.pdf.
- DÖRMANN (K.), « Applicability of the Additional Protocols to Computer Network Attacks », *in International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law*, 17-19 novembre 2004, https://www.icrc.org/en/doc/resources/documents/misc/68lg92.htm.

**F) AUTRES SOURCES**

- GEBEL (M.), « Misinformation vs. Disinformation: What to Know about Each Form of False Information, and How to Spot Them Online », *Business Insider,* 2021, https://www.businessinsider.com/misinformation-vs-disinformation?r=US&IR=T.
- « Déstabilisation du Venezuela, une opération de piraterie internationale », *Sputnik France*, 22 mars 2019.

## TABLE DES MATIÈRES