

Droit international applicable dans le cyberspace

 international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberspace_droit.aspx

Note de bas de page 1

Bien qu'il n'existe pas de définition unique universellement acceptée de la notion de cyberspace, celui-ci se compose de réseaux interdépendants de structures de technologie de l'information – comprenant l'Internet, les réseaux de télécommunications, les systèmes informatiques et les processeurs et contrôleurs intégrés – ainsi que des logiciels et des données qui y sont contenus. Canada, Conseil de normalisation de la terminologie de la défense, 2016.

[Retour à la référence de la note de bas de page 1](#)

Note de bas de page 2

Ce cadre repose sur l'applicabilité du droit international aux activités des États, sur des normes facultatives et non contraignantes, ainsi que sur l'élaboration et la mise en œuvre de mesures de confiance concrètes pour contribuer à la réduction du risque de conflit découlant des cyberactivités.

[Retour à la référence de la note de bas de page 2](#)

Note de bas de page 3

Assemblée générale des Nations Unies (AGNU), *Rapport du Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale*, documents officiels de l'AGNU, 68e session, Doc NU [A/68/98*](#) (2013) (ci-après *Rapport du GEG 2013*) (adopté ultérieurement par la résolution [A/RES/68/243](#) de l'AGNU); AGNU, *Rapport du Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale*, documents officiels de l'AGNU, 70e session, Nations Unies, Doc NU [A/70/174](#) (2015) (ci-après *Rapport du GEG 2015*) (adopté ultérieurement par la [résolution A/RES/70/237](#) de l'AGNU); AGNU, *Rapport du Groupe de travail à composition non limitée chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale*, Doc NU [A/75/816](#) (2021) (ci-après *Rapport du GTCNL 2021*); et AGNU, *Rapport du Groupe d'experts gouvernementaux chargé d'examiner les moyens de favoriser le comportement responsable des États dans le cyberspace dans le contexte de la sécurité internationale*, 76e session, Doc NU [A/76/135](#) (2021) (ci-après *Rapport du GEG 2021*) (les deux ont été adoptés ultérieurement par la résolution [A/RES/76/19](#) de l'AGNU).

[Retour à la référence de la note de bas de page 3](#)

Note de bas de page 4

Déclarations du Canada lors de la réunion consultative informelle du Groupe d'experts gouvernementaux chargé d'examiner les moyens de favoriser le comportement responsable des États dans le cyberspace dans le contexte de la sécurité internationale (2019) [en anglais seulement], accessible à l'adresse : <https://www.un.org/disarmament/wp-content/uploads/2020/01/statements-canada-informal-consultative-meeting-gge-5-6-december.pdf>.

[Retour à la référence de la note de bas de page 4](#)

Note de bas de page 5

Rapport du GEG 2021, supra, note 3; Recueil officiel des contributions nationales volontaires sur la question de savoir comment le droit international s'applique à l'utilisation des technologies de l'information et des communications par les États, soumises par les experts gouvernementaux participants, paragr. 73; Centre d'excellence pour la cyberdéfense de l'OTAN, *Droit international du cyberspace : trousse d'outils interactifs*(2022) [en anglais seulement], accessible à l'adresse : https://cyberlaw.ccdcoe.org/wiki/Category:National_position.

[Retour à la référence de la note de bas de page 5](#)

Note de bas de page 6

Rapport du GTCNL 2021, supra, note 3, paragr. 36-37, 39-40.

[Retour à la référence de la note de bas de page 6](#)

Note de bas de page 7

Charte des Nations Unies, 26 juin 1945 R.T. Can. TS 1945 no 7, accessible à l'adresse : <https://www.un.org/fr/about-us/un-charter/full-text>.

[Retour à la référence de la note de bas de page 7](#)

Note de bas de page 8

Rapport du GEG 2015, supra, note 3, dans lequel le GEG des Nations Unies a établi pour la première fois onze (11) normes facultatives et non contraignantes de comportement responsable des États ; Rapport du GEG 2021, supra, note 3; Rapport du GTCNL 2021, supra, note 3.

[Retour à la référence de la note de bas de page 8](#)

Note de bas de page 9

Résumé du président, GTCNL, troisième session de fond, annexe, Doc NU [A/AC.290/2021/CRP.3](#) (2021), paragr. 10-15 [en anglais seulement].*

[Retour à la référence de la note de bas de page 9](#)

Note de bas de page 10

Rapport du GTCNL 2021, supra, note 3, paragr. 25.

[Retour à la référence de la note de bas de page 10](#)

Note de bas de page 11

Cour permanente d'arbitrage, Affaire de l'île de Palmas (ou Miangas), Les États-Unis c. Les Pays-Bas, sentence arbitrale, II RIAA 829, ICGJ 392, 4 avril 1928 [en anglais seulement], accessible à l'adresse : https://legal.un.org/riaa/cases/vol_II/829-871.pdf.

[Retour à la référence de la note de bas de page 11](#)

Note de bas de page 12

R. c. Hape, 2007 CSC 26 (CanLII), accessible à l'adresse : <https://canlii.ca/t/1rq5p>.

[Retour à la référence de la note de bas de page 12](#)

Note de bas de page 13

Ibid., paragr. 43.

[Retour à la référence de la note de bas de page 13](#)

Note de bas de page 14

Le droit international prévoit des exceptions à la règle de souveraineté territoriale telles que les actions i) autorisées par le Conseil de sécurité des Nations Unies, ii) prises en état de légitime défense face à une attaque armée, iii) auxquelles l'État touché a consenti, ou iv) qui constituent des contre-mesures. Ces exceptions s'appliquent dans le cyberspace.

[Retour à la référence de la note de bas de page 14](#)

Note de bas de page 15

Schmitt, Michael N., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2e éd., Cambridge, Cambridge University Press, 2017, p. 20, paragr. 10 [en anglais seulement] (ci-après *Tallinn Manual 2.0*).

[Retour à la référence de la note de bas de page 15](#)

Note de bas de page 16

Il convient de signaler que l'espionnage, bien qu'il ne soit pas en soi illicite au regard du droit international, peut être réalisé d'une manière susceptible de violer le droit international. Voir, de manière générale, *Tallinn Manual 2.0, supra*, note 15, règle 4 et passage sur le cyberespionnage à la p. 19, paragr. 7-9.

[Retour à la référence de la note de bas de page 16](#)

Note de bas de page 17

Par exemple, au Canada, l'espionnage économique constitue une violation de l'article 19 de la *Loi sur la protection de l'information* (L.R.C. 1985, c. O-5), et toute personne qui commet une infraction visée au paragraphe 19(1) est coupable d'un acte criminel passible d'un emprisonnement maximal de 10 ans.

[Retour à la référence de la note de bas de page 17](#)

Note de bas de page 18

Les fonctions intrinsèquement souveraines (aussi appelées « domaine réservé ») comprennent les matières à propos desquelles l'État peut se décider librement, comme les systèmes politiques, économiques, sociaux et culturels, ainsi que la formulation de la politique étrangère.

[Retour à la référence de la note de bas de page 18](#)

Note de bas de page 19

Tallinn Manual 2.0, *supra*, note 15, règle 66 et commentaire connexe à la p. 318, paragr. 19, selon lequel [traduction] « la contrainte à elle seule ne suffit pas pour établir que l'interdiction d'intervenir a été violée [...] elle doit aussi viser à influencer sur l'issue d'une question relevant exclusivement de l'État touché ou sur la conduite de celui-ci à cet égard ».

[Retour à la référence de la note de bas de page 19](#)

Note de bas de page 20

Voir les commentaires sur les normes facultatives et non contraignantes du GEG des Nations Unies dans le *Rapport du GEG 2021*, *supra*, note 3, paragr. 29-30 et 42-46. Le Canada ne considère pas que le consensus qui s'est dégagé au sein du GEG des Nations Unies en 2015, et depuis lors, sur des normes facultatives et non contraignantes en la matière empêche la reconnaissance d'une règle juridique contraignante de diligence raisonnable en droit international coutumier. Le Canada continue d'étudier cette question.

[Retour à la référence de la note de bas de page 20](#)

Note de bas de page 21

Un État peut également engager sa responsabilité internationale s'il contraint un autre État à commettre un fait internationalement illicite, ou donne des directives et exerce un contrôle dans la commission d'un fait internationalement illicite par un autre État : Commission du droit international, *Projet d'articles sur la responsabilité de l'État pour fait internationalement illicite et commentaires y relatifs 2001*, art. 17 et 18, accessible à l'adresse : https://legal.un.org/ilc/texts/instruments/french/commentaries/9_6_2001.pdf .

[Retour à la référence de la note de bas de page 21](#)

Note de bas de page 22

Ibid., art. 8.

[Retour à la référence de la note de bas de page 22](#)

Note de bas de page 23

Ibid., art. 22.

[Retour à la référence de la note de bas de page 23](#)

Note de bas de page 24

À cet égard, le droit de la responsabilité des États prévoit des cas où la notification peut ne pas être requise : *ibid.*, art. 52 b).

[Retour à la référence de la note de bas de page 24](#)

Note de bas de page 25

Gouvernement du Canada, *Droits de la personne et inclusion dans les contextes en ligne et numériques* (2022), accessible à l'adresse : https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/human_rights-droits_homme/internet_freedom-liberte_internet.aspx?lang=fra.

[Retour à la référence de la note de bas de page 25](#)

Note de bas de page 26

Pacte international relatif aux droits civils et politiques (PIDCP), 16 décembre 1966, 999 UNTS 171, accessible à l'adresse : <https://www.ohchr.org/fr/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights>.

[Retour à la référence de la note de bas de page 26](#)

Note de bas de page 27

Charte des Nations Unies, *supra*, note 7, art. 2(3) et 33(1) ; *Tallinn Manual 2.0*, *supra*, note 15, règle 65, p. 303.

[Retour à la référence de la note de bas de page 27](#)

Note de bas de page 28

Charte des Nations Unies, *supra*, note 7, art. 2(4).

[Retour à la référence de la note de bas de page 28](#)

Note de bas de page 29

Charte des Nations Unies, *supra*, note 7, art. 51.

[Retour à la référence de la note de bas de page 29](#)

Note de bas de page 30

Tallinn Manual 2.0, *supra*, note 15, règle 80, p. 375.

[Retour à la référence de la note de bas de page 30](#)

Note de bas de page 31

Tallinn Manual 2.0, *supra*, note 15, règle 92, p. 415. Voir aussi, de manière générale, l'article 49(1) du *Protocole additionnel aux Conventions de Genève du 12 août 1949 relatif à la protection des victimes des conflits armés internationaux (Protocole I)*, 8 juin

1977, 1125 UNTS 3, accessible à l'adresse : <https://www.ohchr.org/fr/instruments-mechanisms/instruments/protocol-additional-geneva-conventions-12-august-1949-and>.

[Retour à la référence de la note de bas de page 31](#)

Note de bas de page 32

Protocole I, supra, note 31, art. 36. Voir aussi, de manière générale, *Tallinn Manual 2.0, supra*, note 15, règle 110 et commentaire connexe à la p. 464.

[Retour à la référence de la note de bas de page 32](#)

Note de bas de page 33

Les avis du Comité international de la Croix-Rouge (CICR) jettent un éclairage précieux sur ce point. Selon le CICR, [traduction] « Les cyberactivités menées lors d'un conflit armé ne se produisent pas dans un "vide juridique" ou une "zone grise" - elles sont assujetties aux règles et principes établis du droit international humanitaire » : CICR, *Déclaration du Comité international de la Croix-Rouge dans le cadre du débat ouvert du Conseil de sécurité des Nations Unies sur la cybersécurité et le maintien de la paix et de la sécurité internationales dans le cyberspace*(2021) [en anglais seulement], accessible à l'adresse : <https://www.icrc.org/en/document/cyber-operations-during-armed-conflict-are-not-happening-legal-void-or-grey-zone-they-are>. De plus, le CICR [traduction] « appelle tous les États à affirmer que le DIH s'applique, et impose donc des limites, aux cyberactivités menées durant les conflits armés » : CICR, *Déclaration adressée au Groupe d'experts gouvernementaux chargé d'examiner les moyens de favoriser le comportement responsable des États dans le cyberspace dans le contexte de la sécurité internationale, Réunion consultative informelle (2021)* [en anglais seulement], accessible à l'adresse : <https://www.icrc.org/en/document/icrc-calls-all-states-affirm-ihl-applies-and-therefore-restricts-cyber-operations-during>.

[Retour à la référence de la note de bas de page 33](#)