Canadian Yearbook of International Law
Annuaire canadien de droit international
(2022), **60**, 292–338 doi:10.1017/cyl.2023.15

CAMBRIDGE UNIVERSITY PRESS

CANADIAN PRACTICE IN INTERNATIONAL LAW / PRATIQUE CANADIENNE EN MATIÈRE DE DROIT INTERNATIONAL

At Global Affairs Canada in 2022

Aux Affaires mondiales Canada en 2022

compiled by / préparé par

Alan H. Kessel

Assistant Deputy Minister Legal Affairs and Legal Adviser, Global Affairs Canada, Ottawa, Canada
Email: jfm@international.gc.ca

1. Law of treaties

A. Provisional application of treaties

The provisional application of treaties is being used in an increasing number of contexts in Canadian practice.

1. Introduction

Provisional application of treaties is being used in an increasing number of contexts. In recognition of this trend and the evolving practice of States, the General Assembly adopted resolution 76/113 of 9 December 2021, entitled "Provisional Application of Treaties," in which the Assembly requested "…the Secretary-General to prepare a volume of the *United Nations Legislative Series* compiling the practice of States and international organizations in the provisional application of treaties, as furnished by the latter over the years, together with other materials relevant to the topic."

The below delineates the scope of Canada's evolving practice on the provisional application of treaties.

2. Provisional application and Canada's treaty adoption process

Canada most recently put forward its position on the role of provisional application in its treaty adoption process at the General Assembly debate on the 2021 Report of the International Law Commission (ILC):

The extracts from official correspondence contained in this survey have been made available by courtesy of Global Affairs Canada. Some of the correspondence from which extracts are given was provided for the general guidance of the enquirer in relation to specific facts that are often not described in full in the extracts within this compilation. The statements of law and practice should not necessarily be regarded as definitive.

> Provisional application is an integral part of Canada's treaty adoption process, though we generally prefer to rely on entry-into-force provisions as a straightforward mechanism. *Canada's current practice is that provisional application may only take effect following the signing of a treaty, and if no domestic implementing legislation is required.* If implementing legislation is required, provisional application is delayed until the required legislation enters into force [emphasis added].[1]

A similar position was articulated by Canada in a study published in 2001 by the Council of Europe (CoE) and the British Institute of International and Comparative Law (BIICL):

> Provisional application is possible, for example, when such a provision is included in the legislation (e.g. the Department of Transport Act). If, however, changes in Canadian laws or regulations are necessary in order to enable the government of Canada to commit itself to provisional application of a treaty, appropriate legislative or regulatory action must be taken.[2]

The approach taken in relation to the *Canada-European Union Comprehensive Economic and Trade Agreement* (*CETA*) illustrates this practice. Article 30.7.3 of *CETA* allows Canada or the European Union (EU) to provisionally apply the treaty granted "that their respective internal requirements and procedures necessary for the provisional application of this Agreement have been completed."[3] Canada therefore enacted the *Canada–European Union Comprehensive Economic and Trade Agreement Implementation Act* and completed other necessary procedures to domestically implement *CETA* (e.g., administrative and regulatory changes) prior to the initiation of *CETA*'s provisional application pursuant to Article 30.7.3.[4]

In addition to enacting any necessary legislative, regulatory or other changes, Canada also typically provides confirmation to the other State of the completion of Canada's relevant domestic procedures to provisionally apply a given treaty and, if applicable, identifies the relevant provisions subject to provisional application (if the intent is to limit provisional application to certain provisions of the treaty).[5]

---

[1]United Nations General Assembly (UNGA) Sixth Committee, *International Law Commission Report*, Canada Statement – Cluster 1, 28 October 2021, at 3, (https://www.un.org/en/ga/sixth/76/pdfs/statements/ilc/19mtg_canada_1e.pdf).

[2]Council of Europe (CoE) and the British Institute of International and Comparative Law (BIICL), eds, *Treaty Making – Expression of Consent by States to be Bound by a Treaty* (The Hague: Kluwer Law, 2001) at 301.

[3]"Text of the Comprehensive Economic and Trade Agreement – Chapter thirty: Final provisions" Government of Canada (http://www.international.gc.ca/trade-commerce/trade-agreements-accords-commerciaux/agr-acc/ceta-aecg/text-texte/30.aspx?lang=eng).

[4]*Canada–European Union Comprehensive Economic and Trade Agreement Implementation Act* S.C. 2017, c. 6; see also "Order Fixing September 21, 2017 as the Day on which the Act Comes into Force, other than Certain Provisions" Canada Gazette <https://gazette.gc.ca/rp-pr/p2/2017/2017-09-07-x1/html/si-tr47-eng.html>.

[5]See, for example, Note no. JLI – 0133 regarding *General Coordination Agreement between the United States of America and Canada on the Use of the Radio Frequency Spectrum by Terrestrial Radiocommunication Stations and Earth Stations* (2021).

https://doi.org/10.1017/cyl.2023.15 Published online by Cambridge University Press

Canada maintains that the ultimate objective is for States to take the necessary domestic steps to ensure that a treaty formally enters into force. Thus, provisional application should be seen as a "transitional stage" or measure that can facilitate the coming into force of a treaty.[6]

3. Canada's practice regarding the forms for prescribing or exercising provisional application

Article 25 of the *Vienna Convention on the Law of Treaties* (*VCLT*) specifies that provisional application may result from the provisions of the treaty in question (Article 25(a)). Provisional application may also occur "in some other manner" (Article 25(b)) as agreed by the negotiating States, including in the form of a separate treaty or, exceptionally, a decision or resolution adopted at an international organization or conference, or by a declaration of a State accepted by another State or international organization.[7]

Canada's practice is generally to prescribe provisional application in the treaty in question or alternatively as a separate treaty (typically through an exchange of notes or a protocol).

In the treaty in question (examples)

A series of bilateral treaties between Canada and Latin American States concluded between the mid-1940s and the mid-1950s include express provisions on their provisional application in the final clauses. These provisions stipulate that the treaty in question would apply provisionally upon signature or on a certain date, pending the treaty's definitive entry into force.[8]

The plurilateral *Free Trade Agreement between Canada and the States of the European Free Trade Association (Iceland, Liechtenstein, Norway and Switzerland)* allows for the provisional application of the treaty and associated bilateral agreements, on condition that the domestic requirements of each State permit this provisional application.[9]

[6]See Juan Manuel Gómez-Robledo, *Second Report on the Provisional Application of Treaties*, UN Doc A/CN.4/675 (2014) at para 84.

[7]Sean D. Murphy explains that "[w]hile the draft guideline [on provisional application] identifies these other forms, virtually all agreements on provisional application may be found in the treaty itself that is being provisionally applied or in a separate treaty; very few (if any) examples may be found of provisional application in the form of a resolution adopted at an international organization or by a declaration of a state accepted by others." See Sean D. Murphy, "Provisional Application of Treaties and Other Topics: The Seventy Second Session of the International Law Commission" (2021) 115:4 AJIL 671, at 673; see also ILC, *Guide to the Provisional Application of Treaties, with commentaries thereto*, UNGAOR, 76th Sess, Supp No 10, UN Doc A/76/10 (2021) at 62, Guidelines 3 and 4.

[8]See *Trade Agreement between Canada and Spain*, E100588 – CTS 1955/12, art X(c); *Agreement between the Government of Canada and the Government of Peru for Air Services between and beyond their respective territories*, E103280 – CTS 1955/1, art XIV; *Trade Agreement between Canada and Mexico*, E100538 – CTS 1946/4, art VIII(2); *Trade Agreement between Canada and Brazil*, E102985 – CTS 1941/18, art X(2); *Trade Agreement between Canada and Chile*, E102997 – CTS 1941/16, art IX(2).

[9]See *Free Trade Agreement between Canada and the States of the European Free Trade Association* (Iceland, Liechtenstein, Norway and Switzerland), CTS 2009/3, art 41.

https://doi.org/10.1017/cyl.2023.15 Published online by Cambridge University Press

In some other manner (examples)

An exchange of notes has been used to prescribe provisional application[10] or to extend provisional application that was prescribed by the initial treaty.[11] Canada has also prescribed provisional application in the form of a protocol with an international organization.[12]

Canada has not prescribed or exercised provisional application through forms other than the treaty itself or by a separate agreement. Canada has expressed the need for greater clarity regarding the exercise of provisional application "in some other manner" as foreseen by Article 25(b) of the *VCLT*, particularly to clarify whether and, if so under what circumstances, consent for provisional application could be tacit or implied and produce legal effects.[13]

4. Conclusion

Overall, provisional application is a voluntary and flexible mechanism that allows States to accommodate differences in their respective domestic treaty adoption requirements while not unduly delaying treaty implementation.[14] Canada's views and practice on provisional application will continue to evolve based on our experience and that of other States.

2. Droit des traités

A. Application à titre provisoire des traités

L'application provisoire des traités est utilisée dans un nombre croissant de situations dans la pratique canadienne.

1. Introduction

L'application provisoire des traités est utilisée dans un nombre croissant de situations.

Au vu de cette tendance et de la pratique en évolution des États, le 9 décembre 2021, l'Assemblée générale a adopté la résolution 76/113, intitulée «

[10]See, for example, *Exchange of Notes between Canada and Sweden providing for the Provisional Application between the two countries of the Provisions of the International Air Services Transit Agreement done at Chicago, December 7, 1944* (now terminated).

[11]See, as an example, *Exchange of Notes (September 23 and October 9 and 12, 1942) Between Canada and Chile Extending the Provisional Application of the Trade Agreement of September 10, 1941*, E104697 – CTS 1942/15; cf *Trade Agreement between Canada and Chile* (E102997 – CTS 1941/16), art IX (2).

[12]See *Protocol Additional to the Agreement between Canada and the International Atomic Energy Agency for the Application of Safeguards in Connection with the Treaty on the Non-Proliferation of Nuclear Weapons*, art 17(b).

[13]See Statement by Canada, UNGA, 70th Session, Sixth Committee, 25th Meeting, UN Doc A/C.6/70/SR.25 (2015) at para 60.

[14]See Memorandum by the ILC Secretariat on Provisional Application of Treaties, UNGA, ILC, 69th session, UN Doc A/CN.4/707, at para 103.

https://doi.org/10.1017/cyl.2023.15 Published online by Cambridge University Press

Application à titre provisoire des traités », dans laquelle elle a prié « […] le Secrétaire général d'établir un volume de la *Série législative des Nations Unies* compilant la pratique des États et des organisations internationales en matière d'application à titre provisoire des traités, telle qu'elle s'est constituée au fil des ans, ainsi que d'autres documents relatifs au sujet ».

Ce qui suit esquisse la portée de la pratique en matière d'application à titre provisoire des traités telle qu'elle a évolué au Canada.

2. Application à titre provisoire et processus d'adoption des traités du Canada

Le Canada a récemment fait connaître sa position concernant le rôle de l'application à titre provisoire dans son processus d'adoption des traités dans le cadre du débat de l'Assemblée générale sur le Rapport de 2021 de la Commission du droit international (CDI):

L'application provisoire fait partie intégrante du processus d'adoption des traités au Canada, bien que nous préférions généralement nous appuyer sur des dispositions d'entrée en vigueur, puisqu'il s'agit d'un mécanisme plus simple. *Au Canada, selon la pratique actuelle, l'application provisoire ne peut prendre effet qu'après la signature d'un traité, pour autant qu'aucune mesure législative de mise en œuvre nationale ne soit requise.* Si une mesure législative de mise en œuvre est nécessaire, l'application provisoire est retardée jusqu'à l'entrée en vigueur de la mesure législative[1] (*italiques ajoutées*).

Le Canada a exprimé une position semblable dans une étude publiée en 2001 par le Conseil de l'Europe (CE) et l'Institut britannique de droit international et de droit comparé (BIICL):

L'application à titre provisoire est par exemple possible lorsque cette disposition est prévue dans la législation (comme dans le cas de la loi relative au [ministère] des transports). Si, toutefois, il s'avère nécessaire de modifier des lois ou règlements pour permettre au Gouvernement canadien de s'engager à appliquer provisoirement un traité, des mesures législatives ou réglementaires ad hoc devront être prises[2].

L'approche qui a été suivie à l'égard de l'*Accord économique et commercial global entre le Canada et l'Union européenne* (*AECG*) illustre cette pratique. L'article 30.7.3 de l'*AECG* permet au Canada ou à l'Union européenne (UE) d'appliquer à titre provisoire ce traité sous réserve de « l'accomplissement de leurs obligations et procédures internes respectives nécessaires à

[1]Sixième Commission de l'Assemblée générale des Nations Unies (AGNU), *Rapport de la Commission du droit international*, Déclaration du Canada – Groupe 1, 27 octobre 2021, p 3 (https://www.un.org/en/ga/sixth/76/pdfs/statements/ilc/19mtg_canada_1.pdf).

[2]Conseil de l'Europe et Institut britannique de droit international et de droit comparé (BIICL), *Conclusion des traités – Expression par les États du consentement à être liés par un traité*, La Haye, Kluwer Law, 2001, à la p 301.

https://doi.org/10.1017/cyl.2023.15 Published online by Cambridge University Press

l'application provisoire du présent accord[3] ». Le Canada a donc promulgué la *Loi de mise en œuvre de l'Accord économique et commercial global entre le Canada et l'Union européenne* et accompli les autres procédures nécessaires à la mise en œuvre au niveau national de l'*AECG* (en procédant notamment à des modifications d'ordre administratif et réglementaire) avant d'amorcer l'application à titre provisoire de l'*AECG* conformément au paragraphe 30.7.3[4].

En plus de procéder aux modifications nécessaires de nature législative, réglementaire ou autre, le Canada fournit généralement à l'autre État une notification confirmant qu'il a accompli ses procédures internes requises pour l'application à titre provisoire du traité, en indiquant, le cas échéant, les dispositions visées par cette application (si les parties souhaitent limiter l'application à titre provisoire à certaines dispositions du traité)[5].

Le Canada est d'avis que l'objectif premier des États consiste à prendre les mesures nécessaires au plan interne pour que le traité puisse entrer officiellement en vigueur. Par conséquent, l'application à titre provisoire devrait être considérée comme une « étape transitoire » ou une mesure qui peut faciliter l'entrée en vigueur d'un traité[6].

3. Pratique du Canada concernant les instruments pouvant être utilisés pour prévoir ou déclencher l'application à titre provisoire d'un traité

L'article 25 de la *Convention de Vienne sur le droit des traités* (*CVDT*) énonce qu'un traité peut s'appliquer à titre provisoire si le traité lui-même en dispose ainsi (article 25 a)). Un traité peut également être appliqué provisoirement si les États ayant participé à la négociation en conviennent ainsi « d'une autre manière » (article 25 b)), y compris sous la forme d'un traité distinct ou, exceptionnellement, d'une décision ou d'une résolution adoptée par une organisation ou une conférence internationale, ou encore d'une déclaration d'un État acceptée par un autre État ou une organisation internationale[7].

[3]Gouvernement du Canada, *Texte de l'Accord économique et commercial global – Chapitre trente : Dispositions finales* (https://www.international.gc.ca/trade-commerce/trade-agreements-accords-commerciaux/agr-acc/ceta-aecg/text-texte/30.aspx?lang=fra).

[4]*Loi de mise en œuvre de l'Accord économique et commercial global entre le Canada et l'Union européenne*, L.C. 2017, ch. 6; voir aussi le Décret fixant au 21 septembre 2017 la date d'entrée en vigueur de la loi, à l'exception de certaines dispositions, *Gazette du Canada,* (https://gazette.gc.ca/rp-pr/p2/2017/2017-09-07-x1/html/si-tr47-fra.html).

[5]Voir, par exemple, la Note n° JLI – 0133 sur l'*Accord général de coordination entre le Canada et les États-Unis d'Amérique concernant l'utilisation du spectre des fréquences radioélectriques par les stations de radiocommunication de Terre et les stations terriennes*, 2021.

[6]Voir Juan Manuel Gómez-Robledo, *Deuxième rapport du Rapporteur spécial sur l'application provisoire des traités*, Doc NU A/CN.4/675 (2014) au para 84.

[7]Sean D. Murphy explique que [*Traduction*] « […] même si le projet de directive [sur l'application à titre provisoire] mentionne ces autres formes, la quasi-totalité des dispositions prévoyant que les parties conviennent d'appliquer provisoirement un traité se trouvent dans le traité devant faire l'objet de cette application, ou encore dans un traité distinct; il n'existe que peu ou pas d'exemples d'une application à titre provisoire résultant d'une résolution adoptée par une organisation internationale ou d'une déclaration d'un État acceptée par un autre État ». Voir Sean D. Murphy, «Provisional Application of Treaties and Other

https://doi.org/10.1017/cyl.2023.15 Published online by Cambridge University Press

Dans la pratique, le Canada prévoit de façon générale qu'un traité fera l'objet de l'application à titre provisoire dans les dispositions du traité concerné, ou dans un traité distinct (prenant habituellement la forme d'un échange de notes ou d'un protocole).

Application à titre provisoire prévue dans les dispositions du traité concerné (exemples)

Plusieurs traités bilatéraux conclus entre le Canada et des États d'Amérique latine dans les années 1940-1950 comportent des dispositions expresses concernant leur application à titre provisoire dans les clauses finales. Ces dispositions prévoient que le traité s'appliquera provisoirement dès sa signature ou à partir d'une date particulière, en attendant son entrée en vigueur définitive[8].

L'*Accord de libre-échange entre le Canada et les États de l'Association européenne de libre-échange (Islande, Liechtenstein, Norvège et Suisse)* autorise l'application à titre provisoire de ce traité plurilatéral et des accords bilatéraux connexes à condition que les formalités internes de chaque État le permettent[9].

Application à titre provisoire dont les parties conviennent d'une autre manière (exemples)

Des échanges de notes ont été utilisés pour permettre l'application à titre provisoire d'un traité[10] ou pour prolonger la période d'application à titre provisoire prévue par le traité initial[11]. Le Canada a également conclu un protocole avec une organisation internationale à cette fin[12].

Topics: The Seventy Second Session of the International Law Commission» (2021) 115:4 AJIL 671, 673 [en anglais seulement]; voir aussi CDI, *Guide de l'application à titre provisoire des traités et commentaires y relatifs*, directives 3 et 4.

[8]Voir l'article X(3) de l'*Accord de commerce entre le Canada et l'Espagne*, F100588 – RTC 1955/12; voir aussi l'article XIV de l'*Accord entre le Gouvernement du Canada et le Gouvernement du Pérou relatif aux services aériens entre leurs territoires respectifs et au-delà de ces territoires*, F103280 – RTC 1955/1; l'article VIII(2) de l'*Accord commercial entre le Canada et le Mexique*, F100538 – RTC 1946/4; l'article X(2) de l'*Accord commercial entre le Canada et le Brésil*, F102985 – RTC 1941/18; et, enfin, l'article IX(2) de l'*Accord commercial entre le Canada et le Chili*, F102997 – RTC 1941/16.

[9]Voir l'article 41 de l'*Accord de libre-échange entre le Canada et les États de l'Association européenne de libre-échange (Islande, Liechtenstein, Norvège et Suisse)*, RTC 2009/3.

[10]Voir, par exemple, l'*Échange de notes entre le Canada et la Suède concernant l'application provisoire entre les deux pays de l'Accord relatif au transit des services aériens internationaux fait à Chicago le 7 décembre 1944* (cet accord n'est plus en vigueur).

[11]Voir, par exemple, l'*Échange de notes (23 septembre, 9 et 12 octobre 1942) entre le Canada et le Chili comportant un Accord portant prorogation de l'application provisoire de l'Accord commercial du 10 septembre 1941*, F104697 – RTC 1942/15; cf. article IX(2) de l'*Accord commercial entre le Canada et le Chili*, F102997 – RTC 1941/16.

[12]Voir l'article 17b) du *Protocole additionnel à l'Accord entre le Canada et l'Agence internationale de l'énergie atomique relatif à l'application de garanties dans le cadre du Traité sur la non-prolifération des armes nucléaires.*

https://doi.org/10.1017/cyl.2023.15 Published online by Cambridge University Press

> Les seuls instruments que le Canada a utilisés jusque-là pour prévoir ou déclencher l'application à titre provisoire d'un traité sont le traité lui-même, ou un traité distinct. Le Canada a souligné la nécessité de clarifier les modalités de l'application à titre provisoire dans les cas où les États en conviennent ainsi « d'une autre manière », comme le prévoit l'article 25 b) de la *CVDT*, et en particulier de préciser si et, le cas échéant, dans quelles circonstances, un consentement à l'application à titre provisoire pourrait être tacite ou implicite et produire des effets juridiques[13].

4. Conclusion

> D'une manière générale, l'application à titre provisoire des traités est un mécanisme à caractère facultatif qui offre aux États la souplesse nécessaire pour s'adapter aux différences pouvant exister entre leurs exigences nationales respectives en matière d'adoption des traités, sans retarder indûment la mise en œuvre de ces derniers[14]. Le point de vue et la pratique du Canada en matière d'application à titre provisoire continueront d'évoluer à la lumière de notre expérience et de celle d'autres États.

B. Subsequent agreements

Subsequent agreements under Article 31 of the Vienna Convention on the Law of Treaties — Canada's treaty adoption process — Legal status and effect of Conference of the Parties (COP) decisions

Concerning a question on the legal status and effect of COP decisions under the *Basel Convention on the Control of Transboundary Movements of Hazardous Wastes and Their Disposal* (*Basel Convention*), the Legal Affairs Bureau of Global Affairs Canada responded as follows:

> A decision made by a Conference of Parties (COP) or other governing body of a convention is binding at international law if the underlying convention grants the governing body the authority to make such a decision binding on State Parties.[1] This is confirmed by Conclusion 11(2) of the ILC's *Draft conclusions on subsequent agreements and subsequent practice in relation to the interpretation of treaties* (*Draft Conclusions*): "The legal effect of a decision adopted within the framework of a Conference of States Parties depends primarily on the treaty and any applicable rules of procedure."[2]

[13]Voir la Déclaration du Canada, Assemblée générale des Nations Unies,70e session, Sixième Commission, 25e séance, Doc NU A/C.6/70/SR.25, paragr. 60.

[14]Voir l'Étude du secrétariat de la CDI sur l'application provisoire des traités, Assemblée générale des Nations Unies, Commission du droit international, 69e session, Doc NU A/CN.4/707, paragr. 103.

[1]For a broader discussion on legally binding and non-legally binding instruments at international law, see Daniel Bodansky, "Legally binding versus non-legally binding instruments", Geneva Reports on the World Economy, 2015-November, 155-165, available online: <https://asu.pure.elsevier.com/en/publications/legally-binding-versus-non-legally-binding-instruments>.

[2]See Draft conclusions on subsequent agreements and subsequent practice in relation to the interpretation of treaties (2018), Draft Conclusion 11(2), available online: <https://legal.un.org/ilc/texts/instruments/english/draft_articles/1_11_2018.pdf>.

https://doi.org/10.1017/cyl.2023.15 Published online by Cambridge University Press

Article 15 of the *Basel Convention*, which establishes the COP and its mandate, grants it the power to adopt rules of procedures, rules governing the financial contributions of Parties under the Convention, and amendments to the Convention or its annexes as agreed by the Parties to the Convention. Article 15 appears to limit the COP's mandate to such functions related to the effective administration of the treaty. It does not appear to grant the COP authority to issue a binding decision that would alter the obligations of the Parties to the Convention. Amendments to the Convention must be proposed by a Party to the Convention, adopted by consensus (ideally), and follow the formal treaty process.[3]

However, a COP decision may advance a position on the interpretation of a Convention; for example, a COP decision may interpret or clarify a provision of the Convention in light of the particulars of a case at issue. Commentary on the above-referred Conclusion 11 of the *Draft Conclusions* clarifies that COP decisions may take the form of "subsequent agreements" or "understandings" under Article 31, paragraph 3(a) of the *Vienna Convention on the Law of Treaties* (*VCLT*), which "interpret the provisions of the Convention by defining, specifying or otherwise elaborating on the meaning and scope of the provisions, as well as through the adoption of guidelines on their implementation."[4]

It is crucial to distinguish the interpretative or clarificatory function of "subsequent agreements" under Article 31, paragraph 3 of the *VCLT* from subsequent amending agreements, which would engage the treaty amendment procedures under Articles 39-41 of the *VCLT*. From the domestic side, the amendment of a treaty would trigger Canada's treaty adoption process. Indeed, Draft Conclusions 4 and 7 confirm that these "subsequent agreements" or "understandings" intend to build consensus around a particular interpretation of a treaty, not to amend the treaty.[5]

Finally, despite the use of the word "agreement," a "subsequent agreement" is not necessarily legally binding unless it takes the form of a treaty. Draft Conclusion 10(1) endorses this understanding: "An agreement under article 31, paragraph 3 (a) and (b) [of the *VCLT*], requires a common understanding regarding the interpretation of a treaty which the parties are aware of and accept. *Such an agreement may, but need not, be legally binding for it to be taken into account*" [emphasis added].

[3]See *Basel Convention on the Control of Transboundary Movements of Hazardous Wastes and Their Disposal*, arts 15(5)(c) and 17.

[4]See International Law Commission, *Draft conclusions on subsequent agreements and subsequent practice in relation to the interpretation of treaties, with commentaries*, Commentary to Draft Conclusion 11(2) para 11, page 85, available online: <https://legal.un.org/ilc/texts/instruments/english/commentaries/1_11_2018.pdf>.

[5]See International Law Commission, *Draft conclusions on subsequent agreements and subsequent practice in relation to the interpretation of treaties* (2018), Draft Conclusions 4 and 7, available online: <https://legal.un.org/ilc/texts/instruments/english/draft_articles/1_11_2018.pdf>.

https://doi.org/10.1017/cyl.2023.15 Published online by Cambridge University Press

3. Immunities

A. Privileges and immunities of delegates attending the COP

The fifteenth Conference of the Parties (COP-15) to the *United Nations Convention on Biological Diversity* took place in Montreal on 7–19 December 2022:

> At the request of the United Nations and China, Canada agreed to host the 15th Conference of the Parties (COP15) to the *United Nations Convention on Biological Diversity* in Montreal from December 7 to 19, 2022. Canada succeeded in planning and delivering this conference, which welcomed over 12,000 delegates from all over the world.
>
> A key element of hosting such a conference is to clearly define the responsibilities of all partners, including the host country and the United Nations or the multilateral organization partner. This is accomplished through the negotiation of an instrument between Canada and the relevant organization. In the case of COP15, Canada and the United Nations concluded a non-binding Memorandum of Understanding.
>
> Hosting this type of international conference also involves a review of the rules on the privileges and immunities applicable to various delegates. The purpose of such privileges and immunities is not to benefit these individuals, but rather to ensure the efficient performance of their public functions while in Canada for the conference.
>
> The *Convention on Biological Diversity* Secretariat is headquartered in Montreal. Canada had therefore already concluded a Host Country Agreement relating to the Secretariat and adopted the *Privileges and Immunities of the Secretariat of the Convention on Biological Diversity Order* under Canada's *Foreign Missions and International Organizations Act* (*FMIOA*). These instruments provided the privileges and immunities necessary for various delegates participating in COP15.
>
> Furthermore, representatives from United Nations Member States which are not party to the *Convention on Biological Diversity* were granted privileges and immunities during COP15 in accordance with the *Privileges and Immunities Accession Order (United Nations)*, also adopted under the *FMIOA*.
>
> To ensure Canada respected its obligations as the host of COP15, federal-provincial-municipal coordination was essential for awareness of the privileges and immunities afforded to certain delegates and the inviolability of the COP15 conference venue.
>
> These contributions provided the "machinery" necessary for a positive outcome. COP15 saw the adoption of a historic deal to protect nature and biodiversity. Governments in attendance agreed to a set of international targets and goals for biodiversity called the Kunming-Montreal Global Biodiversity Framework.

https://doi.org/10.1017/cyl.2023.15 Published online by Cambridge University Press

4. Inter-state dispute settlement

A. International Court of Justice

Allegations of Genocide under the Convention on the Prevention and Punishment of the Crime of Genocide (Ukraine v Russian Federation) — Intervention — Joint Intervention of Canada and the Netherlands

On 7 December 2022, Canada and the Netherlands, relying on Article 63 of the *Statute of the Court*, filed in the Registry of the Court a joint declaration of intervention in the case concerning *Allegations of Genocide under the Convention on the Prevention and Punishment of the Crime of Genocide (Ukraine v. Russian Federation)*. The full text of the declaration is available at <www.icj-cij.org/public/files/case-related/182/182-20221207-WRI-02-00-EN.pdf>.

5. Cyberspace

A. Law applicable to cyberspace

Canada published a national statement on the application of international in cyberspace in April 2022.

Statement on the Application of International Law in Cyberspace
[French version follows the English one]

Abstract
Canada published a national statement on the application of international law in cyberspace in April 2022. This is part of our ongoing efforts, in particular through United Nations processes, to promote a free, open, stable and secure cyberspace. This statement sets out Canada's current view on key aspects of international law applicable in cyberspace and explains how these apply. Canada's views were consolidated through extensive interdepartmental consultations, in particular with the Department of National Defense, the Canadian Armed Forces and the Communications Security Establishment, and are well aligned with those of our closest allies and like-minded. Canada believes that the articulation of national positions on how international law applies to State action in cyberspace will increase international dialogue and the development of common understandings and consensus on lawful and acceptable State behaviour. These statements can help reduce the risk of misunderstandings and escalation between States arising from cyber activities. Recognizing the ongoing nature of technological change, Canada will continue to develop and publicise its views, including through dialogue with other States and stakeholders. This information is available in French and English at *International Law applicable in cyberspace*, <https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=eng>.

***

https://doi.org/10.1017/cyl.2023.15 Published online by Cambridge University Press

Introduction

1. The recent rise in malicious online activities and rapid developments in cyber capabilities have led States to consider questions on how international law applies to State activity in cyberspace.
2. Canada supports the rules-based international order (RBIO), grounded in respect for international law. Canada considers that the RBIO extends to moderating State behaviour in cyberspace.[1] To this end, Canada has been active in multilateral efforts to create the framework for responsible State behaviour in cyberspace.[2]
3. Canada is committed to reinforcing the application of international law in cyberspace and building on the international *acquis* on responsible State behaviour affirmed again last year by the United Nations (UN) Group of Governmental Experts (GGE) and Open-Ended Working Group (OEWG).[3] In plain terms, Canada believes that international law provides essential parameters for States' behaviour in cyberspace[4] and will continue to help ensure global stability and security.
4. Canada supports calls for States to develop and publish their national views on *how* international law applies in cyberspace. States have started stepping forward to issue statements on their national views. Canada is now in a position to do this ourselves. This follows several years of intensive consultations, reflection on the views of a range of States, and participation in formal and informal processes with States and other key stakeholders.[5]

[1]Although cyberspace has no single agreed upon definition, it consists of interdependent networks of information technology structures—including the Internet, telecommunications networks, computer systems, embedded processors and controllers—as well as the software and data that reside within them: Canada Defence Terminology Standardization Board (DTSB) (2016).

[2]This framework is based on the applicability of international law to State activities; voluntary, non-binding norms; and the development and implementation of practical confidence building measures to help reduce the risk of conflict stemming from cyber activities.

[3]United Nations General Assembly (UNGA), Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UNGAOR, 68th Sess, UN Doc A/68/98*(2013) (2013 GGE Report) (later adopted by the UNGA Resolution A/RES/68/243); UNGA, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UNGAOR, 70th Sess, UN Doc A/70/174 (2015) (2015 GGE Report) (later adopted by the UNGA Resolution A/RES/70/237); UNGA, Report of the Open-ended working group on developments in the field of information and telecommunications in the context of international security, UN Doc A/75/816 (2021) (2021 OEWG Report); UNGA, Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, 76th Sess, UN Doc A/76/135 (2021) (2021 GGE Report) (both later adopted by UNGA Resolution A/RES/76/19).

[4]Statements by Canada during the informal consultative meeting of the Group of Governmental Experts on Advancing Responsible State behaviour in Cyberspace in the context of international security (2019), online: <www.un.org/disarmament/wp-content/uploads/2020/01/statements-canada-informal-consultative-meeting-gge-5-6-december.pdf>.

[5]2021 GGE Report, supra note 3; Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts, at 73; The NATO Cooperative Cyber Defence Centre of Excellence, International cyber law: interactive toolkit (2022), online: <https://cyberlaw.ccdcoe.org/wiki/Category:National_position>.

https://doi.org/10.1017/cyl.2023.15 Published online by Cambridge University Press

5. Canada believes that the articulation of national positions on *how* international law applies to State action in cyberspace will increase international dialogue and the development of common understandings and consensus on lawful and acceptable State behaviour. [6]These statements can help reduce the risk of misunderstandings and escalation between States arising from cyber activities.
6. Canada continues to strongly advocate for capacity-building on the application of international law in cyberspace. We are committed to ensuring that the broadest possible group of States participates effectively in addressing these important questions, which increasingly affect all States.
7. This statement sets out Canada's current view on key aspects of international law applicable in cyberspace and explains how these apply. Where possible we have included examples to better illustrate our position on a given aspect. Cyber-related challenges are magnified by rapid technological developments and the ever-increasing activities of malicious actors. Recognizing the ongoing nature of technological change, Canada will continue to develop and publicise its views, including through dialogue with other States and stakeholders.

General application of international law

8. Canada affirms that international law applies to the activities of every State in cyberspace. This includes the *United Nations Charter* (*UN Charter*) in its entirety and customary international law.[7] Canada recognizes the obligations of every State flowing from the principle of sovereignty to: refrain from the threat or use of force; settle disputes peacefully; and refrain from intervention in the internal affairs of other States. Canada further recognizes the obligations arising, in a non-exhaustive manner, from international human rights law (IHRL), international humanitarian law (IHL) and in relation to the law of State responsibility.
9. Canada supports agreed voluntary, non-binding norms for responsible State behaviour in cyberspace,[8] as a complement to international law, and continues to promote their implementation by all States.[9] Such voluntary norms do not replace or alter States' binding obligations or rights under international law: they provide additional specific guidance on what constitutes responsible State behaviour.[10]

Sovereignty

10. Sovereignty is a fundamental element of international law and international relations. It is axiomatic that the principle of sovereignty applies in cyberspace, just as it does elsewhere. It animates a number of obligations for all States.

[6]2021 OEWG Report, *supra* note 3 at 36-37, 39-40.

[7]Charter of the United Nations (UN Charter), 26 June 1945 Can TS 1945 No.7, online: <https://www.un.org/en/about-us/un-charter/full-text>.

[8]2015 GGE Report, *supra* note 3, which first established the eleven (11) non-binding, voluntary norms of responsible State behaviour; 2021 GGE Report, supra note 3; 2021 OEWG Report, supra note 3.

[9]Chair's Summary, OEWG, 3rd substantive session, Annex, UN Doc A/AC.290/2021/CRP.3* (2021) 10-15.

[10]2021 OEWG Report, supra note 3 at 25.

https://doi.org/10.1017/cyl.2023.15 Published online by Cambridge University Press

11. In the relations between States, sovereignty signifies independence. It confers to each State the exclusive right to exercise the functions of a State within its territory.[11]
12. This concept is also reflected in Canadian jurisprudence where Canada's highest court found that "sovereignty" referred to "the various powers, rights and duties that accompany statehood under international law…"[12] and "…one of the organizing principles of the relationships between independent states".[13]
13. Territorial sovereignty is a rule under international law.[14] Every State must respect the territorial sovereignty of every other State. States enjoy sovereignty over their territory, including in particular infrastructure located within their territory and activities associated with that infrastructure. An infringement upon the affected State's territorial integrity, or an interference with or usurpation of inherently governmental functions of the affected State, would be a violation of territorial sovereignty.[15]
14. In assessing the possible infringement of a State's territorial sovereignty, several key factors must be considered. The scope, scale, impact or severity of disruption caused, including the disruption of economic and societal activities, essential services, inherently governmental functions, public order or public safety must be assessed to determine whether a violation of the territorial sovereignty of the affected State has taken place.
15. In general, the impact or severity of cyber effects will be evaluated in the same manner and according to the same criteria as for physical activities. Cyber activities that rise above a level of negligible or *de minimis* effects, causing significant harmful effects within the territory of another State without that State's consent, could amount to a violation of the rule of territorial sovereignty with respect to the affected State. It is also important to note that cyber activities with effects in another State do not constitute physical presence in the territory of that State. As such, territorial sovereignty is not violated by virtue merely of remote activities having been carried out on or through the cyber infrastructure located within the territory of another State. Furthermore, cyber activities carried out remotely from within Canada with negligible effects in a foreign State do not involve an extraterritorial exercise of enforcement jurisdiction by Canada.
16. Cyber activities that cause a loss of functionality with respect to cyber infrastructure located within the territory of the affected State may also constitute a violation of territorial sovereignty if the resulting loss of functionality causes significant harmful effects similar to those caused by physical

[11]Island of Palmas (or Miangas) Case: United States v Netherlands, Award, (1928) 2 RIAA 829, ICGJ 392 (PCA 1928), 4th April 1928, Permanent Court of Arbitration [PCA], online: <https://legal.un.org/riaa/cases/vol_II/829-871.pdf>.

[12]R. v. Hape, 2007 SCC 26 (CanLII), [2007] 2 SCR 292, online: <https://canlii.ca/t/1rq5n>.

[13]*Ibid* at 43.

[14]International law provides for exceptions to the rule on territorial sovereignty such as those actions (i) authorised by the United Nations Security Council; (ii) taken in self-defence in relation to an armed attack; (iii) consented to by the affected State; or (iv) that constitute countermeasures. These exceptions apply in cyberspace.

[15]Schmitt, Michael N., Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, 2d ed (Cambridge: Cambridge University Press, 2017) at 20 para. 10 [hereinafter Tallinn Manual 2.0].

https://doi.org/10.1017/cyl.2023.15 Published online by Cambridge University Press

damage to persons or property. For example, a violation of the territorial sovereignty will occur when the cyber activity creates a significant harmful effect that necessitates the repair or replacement of physical components of cyber infrastructure in the affected State. The loss of functionality of physical equipment that relies on the affected infrastructure in order to operate could also form part of the violation. The assessment of the effects includes both intended and unintended consequences that reach the threshold required to trigger a violation.

17. The rule of territorial sovereignty does not require consent for every cyber activity that has effects, including some loss of functionality, in another State. Activities causing negligible or *de minimis* effects would not constitute a violation of territorial sovereignty regardless of whether they are conducted in the cyber or non-cyber context. Nor are States precluded by the rule of territorial sovereignty from taking measures that have negligible or *de minimis* effects to defend against the harmful activity of malicious cyber actors or to protect their national security interests. For example, Canada considers that a cyber activity that requires rebooting or the reinstallation of an operating system is likely not a violation of territorial sovereignty.
18. The other key basis for assessing a violation of territorial sovereignty is whether a cyber activity interferes with or usurps the inherently governmental functions of another State. Cyber activities that have significant harmful effects on the exercise of inherently governmental functions would constitute an internationally wrongful act. For Canada, this would include government activities in areas such as health care services, law enforcement, administration of elections, tax collection, national defence and the conduct of international relations, and the services on which these depend. There can be a violation of territorial sovereignty by way of effects on governmental functions regardless of whether there is physical damage, injury, or loss of functionality. An example would be a cyber activity that interrupts health care delivery by blocking access to patient health records or emergency room services, resulting in risk to the health or life of patients.
19. Importantly, some cyber activities, such as cyber espionage, do not amount to a breach of territorial sovereignty, and hence to a violation of international law.[16] They may however be prohibited under the national laws of a State.[17]
20. It is possible that a series of cyber activities could lead to significant harmful effects that violate the rule of territorial sovereignty. This is the case even if the individual cyber activity on its own would not reach this threshold.
21. Canada will assess whether a violation of territorial sovereignty has occurred on a case-by-case basis. As noted below, Canada believes further State practice and *opinio juris* will help clarify the scope of customary law in this area over time. In any event, Canada considers that the existence of varied approaches to assessing the legality of cyber activities should not prevent States from

[16]Of note, espionage, while not *per se* wrongful under international law, could be carried out in a way that might violate international law. See generally *Tallinn Manual 2.0*, *supra* note 15, Rule 4 and its discussion of cyber espionage at 19 paras 7-9.

[17]For example, in Canada economic espionage is a violation of section 19 of the *Security of Information Act* (R.S.C. 1985, c.O-5), and every person who commits an offence under subsection 19(1) is guilty of an indictable offence and is liable to imprisonment for a term of not more than 10 years.

https://doi.org/10.1017/cyl.2023.15 Published online by Cambridge University Press

agreeing that particular malicious cyber activities are internationally wrongful acts.

Non-Intervention

22. State cyber activities may breach the foundational international law prohibition of intervention in the internal or external affairs of another State. This would be the case where both of the following conditions are met:

    - the activities aim to interfere with the internal or external affairs of the affected State involving its inherently sovereign functions, known as *domaine réservé*[18]; and
    - the activities would cause coercive effects that deprive, compel, or impose an outcome on the affected State on matters in which it has free choice.[19]

23. In its most serious form, coercion may arise through the threat or use of force but could also arise where a cyber activity is designed to deprive the affected State of its freedom of choice. Coercion must be distinguished from other conduct such as public diplomacy, criticism, persuasion, and propaganda.
24. An example of a prohibited intervention would be a malicious cyber activity that hacks and disables a State's election commission days before an election, preventing a significant number of citizens from voting, and ultimately influencing the election outcome. Another example would be a malicious cyber activity that disrupts the functioning of a major gas pipeline, compelling the affected State to change its position in bilateral negotiations surrounding an international energy accord.
25. Whether or not a cyber activity meets the threshold for a violation of the rule on territorial sovereignty or rises to the level of a violation of the rule against intervention will be determined on a case-by-case basis. As with the thresholds for violations of territorial sovereignty, Canada believes that further State practice and *opinio juris* will help clarify the thresholds for the rule of non-intervention, and the scope of customary law in this area over time.

Due Diligence

26. No State should knowingly allow its territory to be used for acts contrary to the rights of other States.[20] This also applies in cyberspace. A State that has knowledge of a malicious cyber activity is expected to take all appropriate and reasonably available and feasible steps to stop ongoing or temporally imminent cyber activities that result or would result in significant harmful effects that impact the legal rights of another State.

[18]Inherently sovereign functions (also known as *domaine réservé*) include those matters in which a State may decide freely, such as political, economic, social, and cultural systems, as well as the formation of foreign policy.

[19]*Tallinn Manual* 2.0 *supra* note 15, Rule 66 and accompanying commentary at 318 para 19, provides that "mere coercion does not suffice to establish a breach of the prohibition of intervention…[it] must be designed to influence outcomes in, or conduct with respect to, a matter reserved to a target State."

[20]See the discussion of the voluntary, non-binding UN GGE norms in the 2021 UN GGE Report, *supra* note 3 at 29-30, 42-46. Canada does not consider that the UN GGE consensus in 2015, and subsequently, on voluntary, non-binding norms touching on this matter precludes the recognition of a binding legal rule of due diligence under customary international law. Canada continues to study this matter.

https://doi.org/10.1017/cyl.2023.15 Published online by Cambridge University Press

27. The precise threshold that triggers this expectation will depend on the totality of the circumstances in that situation. This would include whether the State has knowledge of the wrongful acts, its technical and other capacities to detect and stop these acts, and what is reasonable in that case. For example, a State with limited technical capabilities would not likely be expected to respond if it failed to detect a malicious cyber activity emanating from or through cyber infrastructure on its territory. However, once aware, the State would be expected to respond.

State Responsibility

28. The international law of State responsibility applies across the whole spectrum of substantive areas of international law, including in cyberspace. It governs such issues as the attribution of internationally wrongful acts to States. It also addresses circumstances precluding wrongfulness, including countermeasures, and possible remedies. The law of State responsibility is not concerned with the legality of the use of force, including in self-defence, which is a separate area of international law.
29. In Canada's view, this well-established body of international law is not only applicable, but highly relevant in relation to contemporary cyber activities. To date, all publicly known malicious cyber activities have been widely interpreted by States as falling below the threshold (or thresholds) of the threat or use of force or armed attacks.

Internationally Wrongful Acts

30. An internationally wrongful act in the cyber context is a cyber-related action or omission that:
    - constitutes a breach of an international legal obligation, whether to another State or the entire international community; and
    - is attributable to a State under international law.
31. International law recognises exceptions to what would otherwise be internationally wrongful acts. Examples include cases of self-defence and countermeasures.

Attribution

32. Canada applies the customary international law on State responsibility to attribute wrongful conduct in cyberspace. Under the law of State responsibility, an important element is that of attribution, which involves the identification of a State as legally responsible for an internationally wrongful act. A State can be responsible directly, or indirectly where a non-State actor has acted on the instructions of, or under the direction or control of, that State.[21] In this

[21] A State may also engage international responsibility if it coerces another state or directs and controls it in the commission of an internationally wrongful act: International Law Commission, *Draft Articles on Responsibility of States for Internationally Wrongful Acts (Articles on State Responsibility), with commentaries, (2001)* Arts. 17, 18, online: <https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf>.

https://doi.org/10.1017/cyl.2023.15 Published online by Cambridge University Press

respect, States cannot escape legal responsibility for internationally wrongful cyber acts by perpetrating them through non-state actors who act on a State's instruction or under its direction or control.[22]

33. Attribution in its legal sense is of course distinct from the technical identification (or technical attribution) of the actor responsible for malicious cyber activity, whether State or non-State, as well as from the public denunciation of the responsible actor (political attribution). Further, Canada believes that the public attribution of internationally wrongful acts engages various political considerations beyond technical and legal attribution. To this end, States bear no obligation to publicly provide the basis upon which an attribution is made.

Countermeasures

34. Canada considers that States are entitled to use countermeasures in response to internationally wrongful acts including in cyberspace. The customary international law of State responsibility defines limits in the exercise of the right to take countermeasures, being actions that would otherwise be unlawful.[23] Countermeasures may not be taken in retaliation, but only to induce compliance, and directed at the State responsible for the internationally wrongful act. They may not constitute the threat or use of force, must be consistent with other peremptory norms of international law, and they must be proportional.
35. Lawful countermeasures in response to internationally wrongful cyber acts can be non-cyber in nature, and can include cyber operations in response to non-cyber internationally wrongful acts.
36. A State taking countermeasures is not obliged to provide detailed information equivalent to the level of evidence required in a judicial process to justify its cyber countermeasures; however, the State should have reasonable grounds to believe that the State that is alleged to have committed the internationally wrongful act was responsible for it. The precise scope of certain procedural aspects of countermeasures, such as notification, needs to be further defined through State practice given the unique nature of cyberspace.[24]
37. Assistance can be provided on request of an injured State, for example where the injured State does not possess all the technical or legal expertise to respond to internationally wrongful cyber acts. However, decisions as to possible responses remain solely with the injured State. Canada has considered the concept of "collective cyber countermeasures" but does not, to date, see sufficient State practice or *opinio juris* to conclude that these are permitted under international law. Canada distinguishes "collective cyber countermeasures" from actions taken in "collective self-defence" including measures taken in cyberspace.

International human rights law (IHRL)

38. It is beyond dispute that international human rights law applies to activities in cyberspace. For many years, Canada has consistently advanced that all

[22]Articles on State Responsibility, supra note 21,Art. 8.

[23]Articles on State Responsibility, supra note 21, Art. 22.

[24]In this regard the law of state responsibility foresees cases where notification may not be required – Articles on State Responsibility, supra note 21, Art. 52(b).

https://doi.org/10.1017/cyl.2023.15 Published online by Cambridge University Press

individuals enjoy the same human rights, and States are bound by the same human rights obligations, online just as offline.[25] States' activities in cyberspace must be in accordance with their international human rights obligations as expressed in the international human rights treaties to which they are a party, and in customary international law.

39. Canada notes that according to Article 2(1) of the *International Covenant on Civil and Political Rights,* each State Party is required to respect and to ensure to all individuals within its territory and subject to its jurisdiction the rights recognized in that instrument, without distinction.[26]
40. The internationally recognized human rights that are of particular concern in relation to cyberspace include the right to freedom of expression and to hold opinions without unlawful interference, freedom of association and of peaceful assembly, freedom from discrimination, and the right not to be subjected to arbitrary or unlawful interference with one's privacy or correspondence.

Peaceful Settlement of disputes

41. A central, and at times overlooked, rule of international law is the obligation of every State, under the *UN Charter*, to seek the settlement of disputes by peaceful means.[27] This is closely related to the prohibition of the threat or use of force.[28] Like that prohibition, it applies in cyberspace just as it does elsewhere. Thus, Canada considers that in line with the *UN Charter*, in case of disputes States may seek solutions through negotiation, enquiry, mediation, conciliation, arbitration, judicial settlement, and resort to regional agencies or arrangements, or other peaceful means of their own choice.
42. The obligation to seek the settlement of disputes by peaceful means is not unlimited, nor does it diminish other international legal obligations or rights, such as the inherent right of self-defence.
43. Canada considers that a State may always respond to an unfriendly act or an internationally wrongful act with unfriendly acts provided they are not contrary to international law.

Threat or use of Force

44. Article 2(4) of the *UN Charter* requires that States refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any State, or in any other manner inconsistent with the purposes of the UN. This also applies in cyberspace. In general, cyber activities that amount to such a threat or use of force are unlawful, with recognised exceptions under international law.
45. In Canada's view, cyber activities may amount to such a threat or use of force where the scale and effects are comparable to those from other operations that

[25]Government of Canada, *Human rights and inclusion in online and digital contexts* (2022), online: <https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/human_rights-droits_homme/internet_freedom-liberte_internet.aspx?lang=eng>.

[26]International Covenant on Civil and Political Rights (ICCPR), 16 December 1966, 999 UNTS 171, online: <https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights>.

[27]UN Charter, supra note 7, Art. 2(3), Art. 33(1); Tallinn Manual 2.0, supra note 15, Rule 65 at 303.

[28]UN Charter, supra note 7, Art. 2(4).

https://doi.org/10.1017/cyl.2023.15 Published online by Cambridge University Press

constitute the use of force at international law. Canada will assess cyber activities that may amount to a threat or use of force on a case-by-case basis.

Self-Defence against Armed Attack

46. Canada considers that the inherent right of self-defence if an armed attack occurs against a State also applies in cyberspace.[29]
47. Canada will respond to cyber activities that amount to an armed attack in a manner that is consistent with international law. Canada's response may include cyber operations. The right to self-defence is both an individual and collective right of States.

International Humanitarian Law (IHL)

48. IHL applies to cyber activities conducted in the context of both international and non-international armed conflict and regulates the conduct of hostilities and protects the victims of armed conflict.[30] In any armed conflict, the right of parties to choose means and methods of warfare is not unlimited.
49. Cyber activities are an attack under IHL, whether in offence or defence, where their effects are reasonably expected to cause injury or death to persons or damage or destruction to objects.[31]This could include harmful effects above a *de minimis* threshold on cyber infrastructure, or the systems that rely on it. Such cyber activities must respect relevant treaty and customary IHL rules applicable to attacks including those relating to distinction, proportionality, and the requirement to take precautions in attack.
50. States that are Parties to *Additional Protocol I* to the *Geneva Conventions* are required to review new weapons, means or methods of warfare to ensure compliance with IHL.[32] This obligation applies in the context of cyber capabilities and activities, although not all cyber capabilities and activities will constitute a weapon or means or method of warfare.
51. Canada emphasises that acknowledging the application of IHL to cyber activities in armed conflict neither contributes to militarising cyberspace nor legitimises cyber activities that are unlawful.[33]

[29]UN Charter, supra note 7, Art. 51.

[30]Tallinn Manual 2.0, supra note 15, Rule 80 at 375.

[31]Tallinn Manual 2.0, supra note 15, Rule 92 at 415; see also generally Article 49(1) of the Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protections of Victims of International Armed Conflicts (Protocol I), 8 June 1977, 1125 UNTS 3, online: <https://www.ohchr.org/en/instruments-mechanisms/instruments/protocol-additional-geneva-conventions-12-august-1949>.

[32]Protocol I, supra note 31, Art. 36; see also generally Tallinn Manual 2.0 supra note 15, Rule 110 and accompanying commentary at 464.

[33]The views of the International Committee of the Red Cross (ICRC) are a valuable reference on this point: ICRC, *Cyber operations during armed conflict are not happening in the a 'legal void' or 'grey zone'-they are subject to the established principles and rules of international humanitarian law*: Statement by the International Committee of the Red Cross to the UN Security Council Open Debate on Cyber Security, maintaining international peace and security in cyberspace (2021), online: <https://www.icrc.org/en/document/cyber-operations-during-armed-conflict-are-not-happening-legal-void-or-grey-zone-they-are>; ICRC, *The ICRC calls on all States to affirm that IHL applies to, and therefore restricts, cyber operations during armed conflicts:* Statement to the Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security, Informal Consultative meeting (2021), online: <https://www.icrc.org/en/document/icrc-calls-all-states-affirm-ihl-applies-and-therefore-restricts-cyber-operations-during>.

https://doi.org/10.1017/cyl.2023.15 Published online by Cambridge University Press

Conclusion

52. With this statement, Canada joins the many other States which have publicised their views on how international law applies in cyberspace. We hope that States which have not yet done so will consider publishing their own statements as well and thus contribute to the emergence of common understandings.
53. To that end, Canada will continue to actively support capacity building on international law and cyberspace. Canada has found the process of consultations that led to this statement to be very beneficial in developing a deeper understanding of *how* international law applies to cyberspace.
54. Canada believes it is crucial for all States to move beyond discussions of general concepts and build common understandings of what constitutes unlawful conduct in cyberspace. Canada will continue to develop and publicise its positions, including through dialogue with other States and stakeholders, in its ongoing efforts to contribute to security and stability in cyberspace.

***

Déclaration canadienne sur le droit international applicable dans le cyberespace

Résumé

Dans le cadre de nos efforts continues pour promouvoir un cyberespace ouvert, libre et sûr, notamment à travers les processus des Nations Unies, le Canada a publié une déclaration sur l'application du droit international dans le cyberespace, en avril 2022. Cette déclaration donne le point de vue actuel du Canada sur les aspects clés du droit international qui s'appliquent dans le cyberespace et explique comment ils s'appliquent. Les opinions du Canada ont été soutenus par de nombreuses consultations interdépartementales, notamment avec les Forces armées canadiennes, le ministère de la Défense et le Centre de la sécurité des télécommunications et sont en alignement à celles de nos alliés les plus proches et celles des autres pays aux points de vues similaires. Le Canada croit qu'exprimer publiquement le positionnement national sur la question de savoir comment le droit international s'applique aux actions que les états portent en cyberespace, va permettre à ce que le dialogue sur le plan international ait lieu et qu'il y ait un développement de la compréhension commune sur la conduite acceptable et légale d'un état. Ces déclarations pourraient aussi aider à réduire les risques d'incompréhensions et des escalades vers un conflit entre États suite à des cyberactivités. Le Canada reconnaît que la technologie est de nature à évoluer rapidement et constamment. Ainsi, le Canada continue à développer et publier ses opinions, entre autres en échangeant avec d'autres États et les autres parties prenantes. Cette information est disponible en français et en anglais: *Droit international applicable dans le cyberespace* <https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=fra>.

https://doi.org/10.1017/cyl.2023.15 Published online by Cambridge University Press

Introduction

1. L'augmentation récente des activités malveillantes en ligne et l'évolution rapide des capacités cybernétiques ont conduit les États à s'interroger sur la manière dont le droit international s'applique aux activités des États dans le cyberespace.
2. Le Canada appuie l'ordre international fondé sur des règles (OIFR), ancré dans le respect du droit international. Le Canada considère que l'OIFR devrait encadrer le comportement des États dans le cyberespace[1]. C'est pourquoi le Canada a participé activement aux efforts multilatéraux visant à créer un cadre destiné à guider le comportement responsable des États dans le cyberespace[2].
3. Le Canada est déterminé à renforcer l'application du droit international dans le cyberespace et à s'appuyer sur l'acquis international en matière de comportement responsable des États réitéré l'année passée par le Groupe d'experts gouvernementaux (GEG) et le Groupe de travail à composition non limitée (GTCNL) des Nations Unies[3]. Le Canada estime que le droit international établit les paramètres essentiels du comportement des États dans le cyberespace[4]et qu'il continuera de contribuer à assurer la stabilité et la sécurité dans le monde.
4. Le Canada appuie les appels lancés aux États pour qu'ils élaborent et publient leurs points de vue nationaux sur **la manière** dont le droit international s'applique dans le cyberespace. Les États ont commencé à répondre à ces appels et à formuler des déclarations sur leurs points de vue nationaux. Le Canada est maintenant en mesure de le faire lui-même, et ce, à l'issue de plusieurs années de consultations intensives, de réflexion sur les points de vue exprimés par divers

[1]Bien qu'il n'existe pas de définition unique universellement acceptée de la notion de cyberespace, 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.

[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.

[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 cyberespace 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).

[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 cyberespace 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>.

https://doi.org/10.1017/cyl.2023.15 Published online by Cambridge University Press

États, et de participation à des processus officiels et informels avec d'autres États et interlocuteurs clés[5].

5. Le Canada estime que la formulation de positions nationales sur **la manière** dont le droit international s'applique à l'activité de l'État dans le cyberespace permettra d'intensifier le dialogue international et de développer une compréhension commune et un consensus sur ce qui constitue un comportement acceptable et licite de l'État[6]. Des déclarations de cette nature peuvent contribuer à réduire les risques de malentendus et d'escalade entre les États occasionnés par les cyberactivités.
6. Le Canada continue de préconiser avec force le renforcement des capacités en matière d'application du droit international dans le cyberespace. Nous sommes résolus à faire en sorte que le plus grand nombre possible d'États participent effectivement à l'examen de ces importantes questions, qui touchent de plus en plus l'ensemble des États.
7. La présente déclaration présente le point de vue actuel du Canada concernant les principaux aspects du droit international applicables dans le cyberespace, et explique la manière dont ils s'appliquent. Dans la mesure du possible, nous avons inclus des exemples pour mieux illustrer notre position sur les aspects abordés. Les défis liés au cyberespace sont accentués par les avancées technologiques rapides et la multiplication incessante des activités d'acteurs malveillants. Conscient de l'évolution constante des technologies, le Canada continuera de préciser et de communiquer ses points de vue, y compris dans le cadre de dialogues avec d'autres États et interlocuteurs.

Application générale du droit international

8. Le Canada affirme que le droit international s'applique aux activités de chaque État dans le cyberespace. Cela comprend la *Charte des Nations Unies*[7] dans son intégralité et le droit international coutumier Le Canada reconnaît les obligations qui incombent à chacun des États du fait du principe de souveraineté, à savoir : s'abstenir de recourir à la menace ou à l'emploi de la force ; régler les différends par des moyens pacifiques; et s'abstenir de toute intervention dans les affaires intérieures d'un autre État. Le Canada reconnaît en outre les obligations découlant, entre autres, du droit international en matière de droits de la personne (DIDP), du droit international humanitaire (DIH) et du droit de la responsabilité des États.
9. Le Canada soutient des normes non contraignantes convenues sur une base facultative en matière de comportement responsable des États dans le

[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>.

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

[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>.

https://doi.org/10.1017/cyl.2023.15 Published online by Cambridge University Press

cyberespace[8], en complément du droit international, et continue d'en promouvoir la mise en œuvre par tous les États[9]. Ces normes facultatives ne viennent ni remplacer ni modifier les obligations contraignantes ou les droits des États au titre du droit international : elles apportent des orientations plus précises sur ce qui constitue un comportement responsable des États[10].

Souveraineté

10. La souveraineté est un élément fondamental du droit international et des relations internationales. Il va de soi que le principe de souveraineté s'applique dans le cyberespace, au même titre qu'ailleurs. Ce principe sous-tend plusieurs obligations qui incombent à tous les États.
11. Dans les relations entre États, la souveraineté signifie l'indépendance. Elle confère à chaque État le droit exclusif d'exercer les fonctions de l'État sur son territoire[11].
12. Ce concept trouve aussi son expression dans la jurisprudence canadienne, le plus haut tribunal du Canada ayant conclu que la « souveraineté » s'entend des « différents pouvoirs, droits et obligations que confère la qualité d'État en droit international[12]» et qu'elle est « l'un des principes fondateurs des relations entre les États indépendants[13] ».
13. La souveraineté territoriale est une règle du droit international[14]. Chaque État doit respecter la souveraineté territoriale de chacun des autres États. Les États jouissent d'une souveraineté sur leur territoire, y compris sur les infrastructures qui s'y trouvent et les activités connexes. Une atteinte à l'intégrité territoriale de l'État touché, une ingérence dans les fonctions intrinsèquement gouvernementales de l'État touché, ou encore une usurpation de ces fonctions, constituerait une violation de la souveraineté territoriale[15].
14. Pour évaluer une éventuelle atteinte à la souveraineté territoriale d'un État, plusieurs facteurs clés doivent être pris en compte. La portée, l'ampleur, les répercussions ou la gravité de la perturbation causée, y compris la perturbation des activités économiques et sociétales, des services essentiels, des fonctions intrinsèquement gouvernementales, de l'ordre public ou de la sécurité

[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.

[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].

[10]*Rapport du GTCNL 2021*, *supra,* note 3, paragr. 25.

[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>.

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

[13]*Ibid*., paragr. 43.

[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 cyberespace.

[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*).

https://doi.org/10.1017/cyl.2023.15 Published online by Cambridge University Press

publique, doivent être évaluées pour déterminer si une violation de la souveraineté territoriale de l'État touché a eu lieu.

15. En général, les répercussions ou la gravité des cybereffets seront évaluées de la même façon et selon les mêmes critères que pour les activités tangibles. Les cyberactivités dont les effets dépassent le seuil du négligeable ou *de minimis*, qui entraînent des effets dommageables importants sur le territoire d'un autre État sans le consentement de ce dernier, pourraient constituer une violation de la règle de souveraineté territoriale à l'égard de l'État touché. Il importe également de noter que les cyberactivités ayant des effets dans un autre État ne constituent pas une présence physique sur le territoire de cet État. Par conséquent, la souveraineté territoriale n'est pas violée du seul fait que des activités à distance ont été menées à partir de ou via la cyberinfrastructure située sur le territoire d'un autre État. De plus, les cyberactivités menées à distance à partir du Canada qui ont des effets négligeables dans un État étranger ne donnent pas lieu à un exercice extraterritorial de la compétence d'exécution par le Canada.
16. Les cyberactivités qui entraînent une perte de fonctionnalité en lien avec une cyberinfrastructure située sur le territoire de l'État touché peuvent également constituer une violation de la souveraineté territoriale si la perte de fonctionnalité qui en résulte entraîne des effets dommageables importants similaires à ceux causés par des dommages physiques à des personnes ou à des biens. À titre d'exemple, il y aura violation de la souveraineté territoriale lorsque la cyberactivité crée un effet dommageable important qui nécessite la réparation ou le remplacement de composantes physiques de la cyberinfrastructure dans l'État touché. La perte de fonctionnalité des équipements physiques qui dépendent de l'infrastructure touchée pour fonctionner pourrait également faire partie de la violation. L'évaluation des effets porte à la fois sur les conséquences intentionnelles et les conséquences non intentionnelles qui atteignent le seuil requis pour constituer une violation.
17. La règle de souveraineté territoriale n'exige pas le consentement pour chaque cyberactivité qui entraîne des effets, y compris une certaine perte de fonctionnalité, dans un autre État. Les activités ayant des effets négligeables/*de minimis* ne constitueraient pas une violation de la souveraineté territoriale, qu'elles soient menées dans un contexte cybernétique ou non. La règle de souveraineté territoriale n'empêche pas non plus les États de prendre des mesures ayant des effets négligeables/*de minimis* pour se défendre contre l'activité nuisible de cyberacteurs malveillants ou pour protéger leurs intérêts en matière de sécurité nationale. À titre d'exemple, le Canada considère qu'une cyberactivité qui nécessite le redémarrage ou la réinstallation d'un système d'exploitation ne constitue probablement pas une violation de la souveraineté territoriale.
18. L'autre critère essentiel pour évaluer une violation de la souveraineté territoriale est de savoir si une cyberactivité constitue une ingérence dans les fonctions intrinsèquement gouvernementales d'un autre État ou une usurpation de ces dernières. Les cyberactivités qui ont des effets dommageables importants sur l'exercice de fonctions intrinsèquement gouvernementales constitueraient un fait internationalement illicite. Pour le Canada, cela comprendrait les activités gouvernementales dans des domaines tels que les services de santé, l'application de la loi, l'administration des élections, la perception des impôts, la défense nationale et la conduite des relations internationales, ainsi que les

https://doi.org/10.1017/cyl.2023.15 Published online by Cambridge University Press

services dont ces activités dépendent. Il peut y avoir une violation de la souveraineté territoriale en raison des effets produits sur les fonctions gouvernementales, qu'il y ait ou non des dommages physiques, un préjudice ou une dégradation fonctionnelle. Il pourrait s'agir, par exemple, d'une cyberactivité qui interrompt la prestation de soins de santé en bloquant l'accès aux dossiers médicaux des patients ou aux services d'urgence, entraînant ainsi un risque pour la santé ou la vie des patients.

19. Il importe de souligner que certaines cyberactivités, comme le cyberespionnage, ne constituent pas une atteinte à la souveraineté territoriale, et ne donnent donc pas lieu à une violation du droit international[16]. Elles peuvent toutefois être interdites par la législation nationale d'un État[17].
20. Il est possible qu'une série de cyberactivités entraîne des effets dommageables importants qui constituent une violation de la règle de souveraineté territoriale, et ce, même si la cyberactivité prise isolément n'atteint pas ce seuil.
21. Le Canada évaluera au cas par cas si une violation de la souveraineté territoriale s'est produite. Comme il est indiqué ci-après, le Canada estime que la portée du droit coutumier dans ce domaine sera précisée au fil du temps tant par la pratique des États que par l'*opinio juris*. En tout état de cause, le Canada considère que les différentes approches en voie d'élaboration ne devraient pas empêcher les États de convenir que certaines cyberactivités malveillantes constituent des faits internationalement illicites.

Non-intervention

22. Les cyberactivités menées par un État peuvent enfreindre le principe fondamental du droit international interdisant toute intervention dans les affaires intérieures ou extérieures d'un autre État. Cela se produit lorsque les deux conditions suivantes sont réunies:
    - les activités sont menées dans le but de s'ingérer dans les affaires intérieures ou extérieures de l'État touché relevant de ses fonctions intrinsèquement souveraines, c.-à-d. de son domaine réservé[18];
    - les activités ont des effets coercitifs qui privent l'État touché d'un résultat ou visent à obtenir ou à imposer un résultat à l'État touché sur des questions dont il devrait pouvoir décider librement[19].
23. Dans sa forme la plus grave, la contrainte peut se traduire par un recours à la menace ou à l'emploi de la force, mais il peut aussi s'agir d'une cyberactivité qui vise à priver l'État touché de sa liberté de choix. La contrainte ne doit pas

[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.

[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.

[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.

[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 influer sur l'issue d'une question relevant exclusivement de l'État touché ou sur la conduite de celui-ci à cet égard ».

https://doi.org/10.1017/cyl.2023.15 Published online by Cambridge University Press

être confondue avec d'autres pratiques telles que la diplomatie publique, la critique, la persuasion et la propagande.

24. À titre d'exemple, une intervention interdite pourrait prendre la forme d'une cyberactivité malveillante de piratage qui paralyse les systèmes de la commission électorale d'un État quelques jours avant un scrutin, empêchant un grand nombre de citoyens d'aller voter, et influençant ainsi le résultat des élections. Un autre exemple serait celui d'une cyberactivité malveillante qui perturberait le fonctionnement d'un important gazoduc, obligeant ainsi l'État touché à modifier sa position dans des négociations bilatérales sur un accord énergétique international.
25. La question de savoir si une cyberactivité donnée répond aux critères requis pour constituer une violation de la règle relative à la souveraineté territoriale, ou si elle donne plutôt lieu à une violation de la règle de non-intervention, sera examinée au cas par cas. Le Canada estime que, tout comme les critères applicables aux violations de la souveraineté territoriale, les critères relatifs à la règle de non-intervention et la portée du droit coutumier dans ce domaine seront précisés au fil du temps par la pratique des États et par l'*opinio juris*.

Diligence raisonnable

26. Aucun État ne devrait permettre sciemment que son territoire soit utilisé aux fins d'actes contraires aux droits d'autres États[20]. Cette obligation s'applique aussi dans le cyberespace. On s'attend à ce qu'un État qui a connaissance d'une cyberactivité malveillante prenne toutes les mesures adéquates, possibles et raisonnables dans une situation donnée pour arrêter des cyberactivités en cours ou imminentes qui entraînent ou entraîneraient des effets dommageables importants ayant une incidence sur les droits d'un autre État.
27. Le seuil précis déclenchant cette attente dépendra de l'ensemble des circonstances dans une situation donnée. Il s'agira notamment de savoir si l'État a connaissance des faits illicites, de quelles capacités techniques et autres il dispose pour détecter ces faits et les arrêter, et de ce qui est raisonnable dans ce cas. Par exemple, on ne s'attendrait vraisemblablement pas à ce qu'un État disposant de capacités techniques limitées réagisse s'il n'a pas détecté une cyberactivité malveillante menée à partir d'une infrastructure informatique située sur son territoire ou via celle-ci. Toutefois, dès que l'État en aura connaissance, il devra agir.

Responsabilité de l'État

28. Le droit international de la responsabilité des États s'applique à l'ensemble des domaines de fond du droit international, y compris au cyberespace. Il régit des questions telles que l'attribution de faits internationalement illicites à des États. Il traite également des circonstances excluant l'illicéité, y compris les contre-mesures, et des recours possibles. Le droit de la responsabilité des États

[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.

https://doi.org/10.1017/cyl.2023.15 Published online by Cambridge University Press

n'aborde pas la question de la légalité de l'emploi de la force, y compris en cas de légitime défense, qui est un domaine distinct du droit international.

29. Le Canada est d'avis que cet ensemble de règles bien établies en droit international est non seulement applicable, mais aussi très pertinent au regard des cyberactivités contemporaines. Jusqu'à maintenant, les États ont largement considéré qu'aucune des cyberactivités malveillantes connues publiquement n'a atteint le seuil (ou les seuils) requis pour constituer un recours à la menace ou à l'emploi de la force, ou une attaque armée.

Faits internationalement illicites

30. Dans le contexte du cyberespace, un fait internationalement illicite désigne une action ou une omission liées à une activité de nature cybernétique qui:

    - d'une part, enfreint une obligation juridique internationale, que ce soit envers un autre État ou la communauté internationale dans son ensemble;
    - d'autre part, est attribuable à un État en vertu du droit international.

31. Le droit international reconnaît des exceptions à ce qui constituerait par ailleurs un fait internationalement illicite, par exemple les cas de légitime défense et la prise de contre-mesures.

Attribution

32. Le Canada applique le droit international coutumier sur la responsabilité des États pour attribuer des actes illicites commis dans le cyberespace. L'attribution, qui constitue un élément important du droit sur la responsabilité des États, implique la désignation de l'État légalement responsable d'un fait internationalement illicite. Un État peut être responsable directement ou indirectement lorsqu'un acteur non étatique a agi sur les instructions ou les directives ou sous le contrôle de cet État[21]. Ainsi, un État ne peut échapper à sa responsabilité en droit à l'égard d'un fait internationalement illicite commis dans le cyberespace en le perpétrant par l'intermédiaire d'acteurs non étatiques agissant sur ses instructions ou ses directives ou sous son contrôle[22].
33. L'attribution au sens juridique est bien entendu distincte de l'identification technique (attribution technique) du responsable d'une activité malveillante dans le cyberespace, qu'il s'agisse d'un État ou d'un acteur non étatique, ainsi que de la dénonciation publique du responsable (attribution politique). De plus, le Canada est d'avis que l'attribution dans la sphère publique de faits internationalement illicites comporte d'autres considérations d'ordre politique allant au-delà de l'attribution technique. À cette fin, les États ne sont pas tenus de communiquer publiquement les éléments sur lesquels ils se fondent pour attribuer un acte donné.

Contre-mesures

34. Le Canada considère que les États ont le droit de recourir à des contre-mesures en réponse à des faits internationalement illicites, y compris dans le

[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>.

[22]*Ibid.*, art. 8.

https://doi.org/10.1017/cyl.2023.15 Published online by Cambridge University Press

cyberespace. Le droit international coutumier sur la responsabilité des États fixe des limites à l'exercice du droit de prendre des contre-mesures, puisqu'il s'agit d'actions qui seraient par ailleurs illicites[23] Les contre-mesures ne peuvent pas être prises à titre de représailles, mais seulement pour obtenir l'exécution des obligations, et elles doivent être dirigées contre l'État responsable du fait internationalement illicite. Les contre-mesures ne peuvent pas constituer un recours à la menace ou à l'emploi de la force, et elles doivent être proportionnelles et conformes aux autres normes impératives du droit international.

35. Les contre-mesures licites prises en réponse à des faits internationalement illicites commis dans le cyberespace ne doivent pas nécessairement être de nature cybernétique, et peuvent comprendre des cyberopérations menées en réponse à des faits internationalement illicites qui n'ont pas été commis dans le cyberespace.
36. L'État qui impose des contre-mesures n'est pas tenu de fournir des renseignements détaillés répondant à des normes de preuve équivalentes à celles applicables à une procédure judiciaire pour justifier les contre-mesures qu'il prend dans le cyberespace ; toutefois, cet État devrait avoir des motifs raisonnables de croire que l'État auquel on reproche d'avoir commis le fait internationalement illicite est responsable de celui-ci. La portée précise de certains aspects procéduraux des contre-mesures, comme la notification, devra être définie de manière plus approfondie par la pratique des États, compte tenu de la nature unique du cyberespace[24].
37. Une assistance peut être fournie à la demande d'un État lésé, par exemple lorsque ce dernier ne dispose pas de toute l'expertise technique ou juridique requise pour réagir à un fait internationalement illicite commis dans le cyberespace. Toutefois, les décisions concernant les réactions possibles relèvent exclusivement de l'État lésé. Le Canada s'est penché sur le concept de « contre-mesures collectives dans le cyberespace », mais estime que la pratique des États et l'*opinio juris* ne permettent pas, à l'heure actuelle, de conclure que de telles mesures sont permises en vertu du droit international. Le Canada établit une distinction entre les « contre-mesures collectives dans le cyberespace » et les mesures prises pour assurer la « légitime défense collective », y compris celles prises dans le cyberespace.

Droit international en matière de droits de la personne (DIDP)

38. Il est incontestable que le droit international en matière de droits de la personne s'applique aux activités dans le cyberespace. Depuis de nombreuses années, le Canada soutient invariablement le principe selon lequel tous les individus jouissent des mêmes droits de la personne, et les États sont liés par les mêmes obligations en matière de droits de la personne, et ce, en ligne et hors ligne[25]. Les activités des États dans le cyberespace doivent être conformes à leurs obligations internationales en matière de droits de la personne, telles

[23] *Ibid.*, art. 22.

[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).

[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>.

https://doi.org/10.1017/cyl.2023.15 Published online by Cambridge University Press

qu'elles sont exprimées dans les traités internationaux relatifs aux droits de la personne auxquels ils sont parties et dans le droit international coutumier.

39. Le Canada note que, en vertu de l'article 2(1) du *Pacte international relatif aux droits civils et politiques*[26], chaque État partie est tenu de respecter et de garantir à tous les individus se trouvant sur son territoire et relevant de sa compétence les droits reconnus dans cet instrument, sans distinction aucune.
40. Les droits de la personne internationalement reconnus qui suscitent des préoccupations particulières en ce qui concerne le cyberespace comprennent le droit à la liberté d'expression sans crainte d'être inquiété pour ses opinions, la liberté d'association et de réunion pacifique, le droit d'être libre de discrimination et le droit de ne pas faire l'objet d'interférence arbitraire ou illégale dans sa vie privée ou sa correspondance.

Règlement pacifique des différends

41. L'obligation de chercher à régler les différends par des moyens pacifiques qui incombe à chacun des États en vertu de la *Charte des Nations Unies* constitue une règle centrale, et parfois oubliée, du droit international[27]. Cette obligation est étroitement liée à l'interdiction de recourir à la menace ou à l'emploi de la force[28]. À l'instar de cette dernière, elle s'applique dans le cyberespace comme partout ailleurs. Ainsi, le Canada estime que, comme le prévoit la *Charte des Nations Unies*, les États peuvent rechercher la solution de leurs différends par voie de négociation, d'enquête, de médiation, de conciliation, d'arbitrage, de règlement judiciaire, de recours aux organismes ou accords régionaux, ou par d'autres moyens pacifiques de leur choix.
42. L'obligation de chercher à régler les différends par des moyens pacifiques n'est cependant pas illimitée, et elle ne restreint pas les autres droits ou obligations juridiques internationaux, comme le droit naturel de légitime défense.
43. Le Canada considère qu'un État peut toujours répondre à un acte inamical ou à un fait internationalement illicite par des actes inamicaux à condition que ceux-ci ne soient pas contraires au droit international.

Menace ou emploi de la force

44. L'article 2(4) de la *Charte des Nations Unies* requiert que les États s'abstiennent, dans leurs relations internationales, de recourir à la menace ou à l'emploi de la force, soit contre l'intégrité territoriale ou l'indépendance politique de tout État, soit de toute autre manière incompatible avec les buts des Nations Unies. Cette obligation s'applique aussi dans le cyberespace. En règle générale, une cyberactivité est illicite si elle constitue un recours à la menace ou à l'emploi de la force.
45. Le Canada estime qu'une cyberactivité peut constituer un recours à la menace ou à l'emploi de la force lorsque son ampleur et ses effets sont comparables à ceux d'autres opérations qui constituent un emploi de la force en droit

[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>.

[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.

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

https://doi.org/10.1017/cyl.2023.15 Published online by Cambridge University Press

international. Le Canada évaluera au cas par cas les cyberactivités qui pourraient constituer un recours à la menace ou à l'emploi de la force.

Légitime défense face à une agression armée

46. Le Canada considère que le droit naturel de légitime défense d'un État face à une agression armée s'applique également dans le cyberespace[29].
47. Le Canada réagira aux cyberactivités qui constituent une agression armée d'une manière conforme au droit international, y compris en recourant à des cyberopérations s'il y a lieu. Le droit de légitime défense des États est à la fois individuel et collectif.

Droit international humanitaire (DIH)

48. Le DIH s'applique aux cyberactivités menées dans le contexte des conflits armés internationaux et des conflits armés non internationaux, il régit la conduite des hostilités, et protège les victimes des conflits armés[30]. Dans un conflit armé, le droit des parties de choisir les moyens et méthodes de guerre n'est pas illimité.
49. Les cyberactivités constituent une attaque au sens du DIH, qu'elles soient menées à titre offensif ou défensif, lorsque leurs effets sont raisonnablement susceptibles de causer la mort ou des blessures à des personnes ou la dégradation ou la destruction d'objets[31]. Cela pourrait comprendre des effets nocifs dommageables supérieurs à un seuil *de minimis* lorsqu'il s'agit de la cyberinfrastructure ou des systèmes qui en dépendent. Les cyberactivités de ce type doivent respecter les règles du DIH conventionnel et coutumier applicables aux attaques, y compris celles relatives au principe de distinction, à la proportionnalité et à l'obligation de prendre des précautions lors d'une attaque.
50. Les États parties au *Protocole additionnel I* aux *Conventions de Genève* sont tenus d'examiner les nouvelles armes et les nouveaux moyens ou méthodes de guerre pour s'assurer de leur conformité au DIH[32]. Cette obligation s'applique dans le contexte des capacités et activités cybernétiques, même si toutes les capacités et activités de ce type ne constituent pas une arme ou un moyen ou une méthode de guerre.
51. Le Canada tient à souligner que la reconnaissance du fait que le DIH s'applique aux cyberactivités lors des conflits armés ne contribue pas à la militarisation du cyberespace et ne vient pas légitimer les cyberactivités illicites[33].

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

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

[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>.

[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.

[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*

https://doi.org/10.1017/cyl.2023.15 Published online by Cambridge University Press

Conclusion

52. En publiant la présente déclaration, le Canada se joint aux nombreux États qui ont fait connaître publiquement leurs points de vue concernant la manière dont le droit international s'applique dans le cyberespace. Nous espérons que les États qui ne l'ont pas encore fait envisageront de publier eux aussi leurs propres déclarations et contribueront ainsi à l'émergence d'une compréhension commune.
53. À cette fin, le Canada continuera de soutenir activement le renforcement des capacités en matière de droit international et de cyberespace. Le processus de consultations qui a abouti à la présente déclaration nous a permis de beaucoup mieux comprendre la *manière* dont le droit international s'applique dans le cyberespace.
54. Le Canada estime qu'il est essentiel pour tous les États de dépasser les discussions sur les concepts généraux, et de développer une interprétation commune de vues sur ce qui constitue un comportement illicite dans le cyberespace. Le Canada continuera de développer et de communiquer ses positions, y compris au moyen d'un dialogue avec d'autres États et interlocuteurs, dans le cadre des efforts constants qu'il déploie pour contribuer à la sécurité et à la stabilité dans le cyberespace.

6. Law of the sea

A. Continental shelf

Canada made a revised submission to the Commission on the Limits of the Continental Shelf (CLCS) on 19 December 2021.

Canada's Continental Shelf in the Arctic Ocean

On 19 December 2022, Canada submitted to the Commission on the Limits of the Continental Shelf (CLCS), an addendum to the Executive Summary (Addendum) of its 2019 submission in respect of areas in the Arctic Ocean pursuant to article 76(8) and Annex II, article 4 of the *United Nations Convention on the Law of the Sea* (*UNCLOS*). [1] The filing of the Addendum was the first step in revising Canada's 2019 Arctic Ocean submission to extend the outer limits of Canada's continental shelf along the full lengths of the Lomonosov Ridge and the Alpha-Mendeleev Ridge complex. The revision of Canada's 2019 submission is a necessary response to the addendum filed by

dans le cyberespace(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 cyberespace 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>.

[1] *United Nations Convention on the Law of the Sea*, 10 December 1982, 1833 UNTS 397, (entered into force 16 November 1994).

https://doi.org/10.1017/cyl.2023.15 Published online by Cambridge University Press

the Russian Federation to its revised 2015 Arctic Ocean submission on 31 March 2021. The Russian Federation's addendum expanded the outer limits of its continental shelf to include the full lengths of the Lomonosov and Alpha-Mendeleev ridges, more than tripling the area of overlap with Canada's extended continental shelf in the Arctic Ocean (as set out in the 2019 submission) and reaching Canada's 200 nautical mile (M) EEZ.[2]

Delineation of the continental shelf

1. The rules-based order established for the world's oceans, including the Arctic Ocean, is supported by a system of international laws and institutions. Canada signed the *1982 United Nations Convention on the Law of the Sea* (*UNCLOS*) on the day it was opened for signature and ratified it on 7 November 2003. *UNCLOS* entered into force for Canada on 7 December 2003. *UNCLOS* governs a wide range of maritime activities in the world's oceans, including the definition of maritime zones over which states have sovereign rights or jurisdiction, as well as legal obligations. One of these maritime zones is the continental shelf (i.e., the natural prolongation of the coastal state's land territory). The area of the continental shelf that extends beyond the state's 200 nautical miles (M) limit is colloquially referred to as the "extended continental shelf" or ECS.
2. Under article 77 of *UNCLOS* coastal states exercise sovereign rights over the seabed and subsoil of the continental shelf and the natural resources thereof, as well as jurisdiction over certain activities such as marine scientific research. These rights and jurisdiction apply to the continental shelf inside and beyond the 200 M limit and "do not depend on occupation, effective or notional, or on any express proclamation"[3] as they exist *ipso facto* and *ab initio*.[4] In the *Bangladesh* v *Myanmar* case, the International Tribunal for the Law of the Sea (ITLOS) ruled that, although only the coastal state can establish the outer limits of its continental shelf beyond 200 M pursuant to article 76(8) of *UNCLOS*, the opposability of those limits against other states requires that coastal states comply with the process detailed in article 76.[5] More precisely, within ten years of entry into force of the Convention for the coastal state, it must submit to the CLCS information on the limits of its continental shelf in accordance with article 4 of Annex II of *UNCLOS* and rule 45 of the *Rules of Procedure of the Commission on the Limits of the Continental Shelf* (*RoP*).[6] In order to satisfy the 10-year time period, a coastal state may fulfill its obligation by filing preliminary information indicating the limits of its continental shelf beyond 200 M.[7] (See also decision SPLOS/183 regarding the filing of preliminary information to satisfy the 10 year time period.)

[2]<https://www.un.org/depts/los/clcs_new/submissions_files/rus01_rev15/20210802UsNvUN.pdf>.

[3]*United Nations Convention on the Law of the Sea*, art. 77(3).

[4]*Cases concerning the delimitation of the continental shelf of the North Sea (Federal Republic of Germany v Denmark and Federal Republic of Germany v Netherlands)*, [1969] ICJ Rep 3 at 19.

[5]*Case concerning the delimitation of the maritime boundary in the Bay of Bengal (Bangladesh v Myanmar)*, [2012] ITLOS Rep 4 at 407.

[6]CLCS, 21st Sess, 58th Mtg, CLCS/40/Rev.1 (2008) (Rules of Procedure).

[7]*Decision regarding the workload of the Commission on the Limits of the Continental Shelf and the ability of States, particularly developing States, to fulfil the requirements of article 4 of annex II to the United Nations*

https://doi.org/10.1017/cyl.2023.15 Published online by Cambridge University Press

3. A submission to the CLCS includes an executive summary, a main body consisting of analyses and interpretation, and all the supporting scientific and technical data.[8] A coastal state may file partial submissions, usually used for different geographic regions in which it has an ECS. For example, Canada's 2019 submission in respect of its continental shelf in the Arctic Ocean is a partial submission. For brevity states often just refer to submissions even if partial. Coastal states are also required to inform the CLCS of any dispute pertaining to the delimitation of the continental shelf or unresolved land or maritime matters with adjacent states along with the names of CLCS members who have provided technical or scientific advice.[9] A submission to the CLCS is made through the Secretary-General of the United Nations, who notifies the CLCS and, afterwards, all member states of the United Nations, and makes public the executive summary, which includes coordinates of the outer limits and depictions thereof.[10]

The role of the Commission on the Limits of the Continental Shelf

4. The CLCS consists of twenty-one members, from States Parties to *UNCLOS*, with expertise in geology, geophysics or hydrography. Members are elected for a five-year term, may be re-elected, and serve in their personal capacity.[11] The CLCS reviews submissions made by coastal states and provides recommendations on the location of the outer limits of the continental shelf. Given the CLCS' duty to preserve confidentiality, its meetings and those of its subsidiary bodies are held in private, unless it decides otherwise.[12] A Canadian has served on the CLCS since 2012.
5. During its review and analysis of a coastal state's submission and its scientific and technical information, the CLCS may recommend adjusting portions of the outer limit line landward or seaward. A coastal state that has submitted limits questioned by the CLCS has the opportunity to present additional information or gather more data to support the limits put forward.[13] Through this engagement process, a desirable outcome is that the CLCS and the coastal state arrive at a shared view of the location of the outer limits and their rationale. If a coastal state agrees with recommendations issued by the CLCS it will then proceed to establish the outer limits of its continental shelf under article 76(8) of *UNCLOS*; if a coastal state does not agree with the recommendations issued it will file a revised or new submission within a reasonable time.[14]
6. The CLCS considers submissions solely on scientific criteria and only makes recommendations on the limits of the continental shelf of the coastal state.[15] Although it is not an adjudicatory body and does not establish international

Convention on the Law of the Sea, as well as the decision contained in SPLOS/72, paragraph (a), SPLOS/183, 20 June 2008, [online] <https://www.tandfonline.com/doi/pdf/10.1080/00908320903510084>.

[8]Ibid, art 1(1) of Annex III.

[9]*Ibid*, rule 45(2).

[10]*Ibid*, Annex I; Ibid, rule 50.

[11]*United Nations Convention on the Law of the Sea*, *supra* note 1, art 2(2) and art 2(4) of Annex II.

[12]*CLCS, supra* note 6, rule 23.

[13]*Ibid*, para III(6) of Annex III.

[14]*United Nations Convention on the Law of the Sea*, supra note 1, art 8 of Annex II.

[15]*Ibid*, art 3 of Annex II.

https://doi.org/10.1017/cyl.2023.15 Published online by Cambridge University Press

boundaries, article 76(8) of *UNCLOS* provides that the outer limits established by the coastal state "on the basis" of the recommendations are final and binding on member states to the United Nations. Recommendations of the CLCS are without prejudice to delimitation of the continental shelf between states.[16]

7. If there are overlaps between submissions filed by more than one state, article 83(1) of *UNCLOS* requires states to enter into delimitation agreements on the basis of international law to achieve an "equitable solution". Arctic Ocean coastal states expressed their commitment to the orderly settlement of overlaps in the May 2008 *Ilulissat Declaration.*[17] As the Arctic Ocean is an enclosed area, and coastal states are using many of the same geological and geographic features to delineate their continental shelves, significant overlaps between the submissions of the coastal states had been expected.
8. Since the CLCS will not consider a submission (or parts thereof) relating to land or maritime disputes, the filing state will usually seek a commitment from each neighbouring state where overlaps may occur indicating that the latter does not object to the CLCS's consideration of the submission in question.[18] Such commitments are without prejudice to the delineation of the outer limits of the neighbour's shelf and the delimitation of any future boundary. The neighbouring states communicate this commitment to the CLCS via a diplomatic note ("non-objection note"), which is normally posted on the UN Division for Ocean Affairs and the Law of the Sea (DOALOS) website.
9. Given the commitment of the Arctic Ocean coastal states to cooperate on matters generally, and on continental shelf matters specifically, Canada, the Kingdom of Denmark, the Russian Federation, the Kingdom of Norway and the United States (U.S.), all have agreements to file non-objection notes with respect to each other's Arctic submissions when overlaps occur.

Arctic Ocean Submissions

10. All five Arctic Ocean coastal states are following the procedures set out in *UNCLOS* to delineate their continental shelves in the Arctic Ocean but they are at different stages of the process. Rule 51(4) of the *RoP* provides that the submissions are queued "in the order that they are received", thus the first submitted will be the first to be considered by the CLCS. Although not a Party to *UNCLOS*, the U.S. has engaged since 2003 in the collection and analysis of data in accordance with the provisions of article 76 of *UNCLOS* to determine its outer limits.[19]
11. The Russian Federation ratified *UNCLOS* on 12 March 1997. On 20 December 2001, it submitted to the CLCS information on the limits of its ECS in the Pacific Ocean and in the Arctic Ocean in accordance with article 76(8) of *UNCLOS.*[20] Following consultations with the Russian Federation and deliberations among CLCS members and in accordance with rule 12(6) of the *RoP*,

[16] *Ibid*, art 76(10).

[17] *Ilulissat Declaration*, 28 May 2008, (Canada/Denmark/Norway/Russia/United States), online: <https://arcticportal.org/images/stories/pdf/Ilulissat-declaration.pdf>.

[18] ROP, rule 46 and para 5(a) of Annex I

[19] <https://www.state.gov/u-s-extended-continental-shelf-project/>.

[20] <https://www.un.org/depts/los/clcs_new/submissions_files/submission_rus.htm>.

https://doi.org/10.1017/cyl.2023.15 Published online by Cambridge University Press

the CLCS recommended in 2002 that the Russian Federation revise its submission for the Central Arctic Ocean.[21]

12. Pursuant to article 8 of Annex II of *UNCLOS* and rule 53(4) of the *RoP*, the Russian Federation filed its first revised submission for the Arctic Ocean in 2015. Prior to receiving any revised submissions, the CLCS decided at its 26th session that revised submissions should be considered on a priority basis, notwithstanding the queue.[22]
13. On 27 November 2006, the Kingdom of Norway filed with the CLCS its submission for the Northeast Atlantic and the Arctic. The Kingdom of Denmark filed its submission for the northern continental shelf of Greenland on 15 December 2014. Canada filed its Arctic Ocean submission with the CLCS on 23 May 2019 (after having filed preliminary information on 6 December 2013).
14. Canada's Arctic Ocean 2019 continental shelf submission shows entitlement to 1.2 million square kilometres of additional area of the seafloor beyond its 200 M EEZ limit, including the geographic North Pole.[23] It relies on two subsurface geological features, the Lomonosov Ridge and the Alpha-Mendeleev Ridge complex. Both these features span the entire Arctic Ocean and their classification as seafloor elevations has been used in the submissions of Canada, the Kingdom of Denmark and the Russian Federation to extend their ECS beyond 350 M, as interpreted in the CLCS's *Scientific and Technical Guidelines* as natural prolongations and natural components of the continental margin.
15. The Kingdom of Denmark's 2014 outer limits included the full length of the Lomonosov Ridge up to the Russian Federation's 200 M EEZ limit. Although the Kingdom of Denmark did not use the entire length of the Alpha-Mendeleev Ridge complex to show entitlement, their submission overlaps with 9.8% of the Alpha-Mendeleev Ridge complex in Canada's ECS.
16. The outer limits of the Russian Federation in its 2015 revised submission included both the Lomonosov Ridge and the Alpha-Mendeleev Ridge complex but did not extend to either the Danish or the Canadian 200 M EEZ limit. As well, the Russian Federation did not extend its outer limits past the provisional treaty line established in 1990 with the U.S. in the *Agreement between the United States of America and the Union of the Soviet Socialist Republics on the Maritime Boundary* (*1990 USA/USSR Maritime Boundary Agreement*).[24]
17. In its 2019 submission, Canada delineated its outer limits with data acquired during a decade of survey work. The extent of the outer limits, using portions of the Lomonosov Ridge and Alpha-Mendeleev Ridge complex, was demonstrated with fixed points in Canada Basin and Amundsen Basin without extending to the full length of its presumed entitlement along these ridges

[21] *Report of the Secretary-General*, UNGAOR, 57th session, Supp No 49, UN doc A/57/57/Add.1, (2002), 1 at 41.

[22] CLCS/68, paragraph 57

[23] Canada's 2019 ECS Outer Limits, at 16 <https://www.un.org/depts/los/clcs_new/submissions_files/can1_84_2019/CDA_ARC_ES_EN_secured.pdf>.

[24] *Agreement between the United States of America and the Union of the Soviet Socialist Republics on the Maritime Boundary*, United States and Union of Soviet Socialist Republics, June 1, 1990, 106 US Stat 5162, <https://www.state.gov/wp-content/uploads/2020/02/US_Russia_1990.pdf>.

https://doi.org/10.1017/cyl.2023.15 Published online by Cambridge University Press

(i.e. the full length of the ridges to the 200 M EEZ limit of the Russian Federation).[25] The area of overlap with the Russian Federation and the Kingdom of Denmark was extensive, but deemed reasonable by Canada at the time, considering that the Russian Federation had taken a restrained approach in its 2015 submission.

The 2021 Russian Federation Revision

18. In April 2020, the Russian Federation advised Canada that they would be conducting marine scientific research close to the Greenland, Canadian and U.S. 200 M EEZ limits, suggesting that the Russian Federation planned to acquire data to revise its submission. Following this, Canada held several bilateral meetings with Russian Federation, U.S. and Danish program officials.
19. The Russian Federation acquired new data in the summer of 2020 and filed an addendum to its revised submission with the CLCS on 31 March 2021. This addendum contained new outer limits extending along the full lengths of Lomonosov Ridge and the Alpha-Mendeleev Ridge complex, more than tripling the area of overlap with Canada's 2019 submission (from 247,647 to 783,883 sq. km.) and abutting portions of Canada's 200 M EEZ limit.[26] The Russian Federation addendum also increased the overlap area with the Kingdom of Denmark.[27] In terms of the outer limits of its continental shelf, the Russian Federation continued to respect the provisional treaty line with the U.S. but only up to a point where the U.S. is likely to be able to demonstrate entitlement to an extended continental shelf (i.e., within Nautilus Basin).

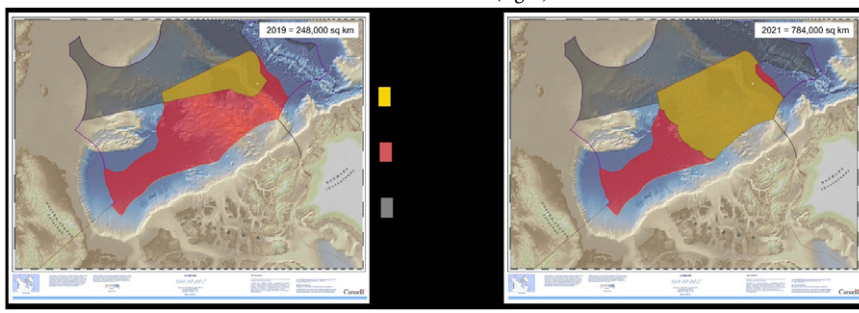
The 2022 Canadian Revision

20. After a thorough review of the implications and its options on the basis of available data, on 19 December 2022, Canada filed an addendum to the executive summary of its 2019 Arctic Ocean submission, extending the outer limits of Canada's Arctic Ocean continental shelf submission along the full lengths of the Lomonosov Ridge and the Alpha-Mendeleev Ridge complex to the outer limits of the Russian Federation's 200 M EEZ limit.

[25] *United Nations Convention on the Law of the Sea*, *supra* note 6, art 76(4).

[26] https://www.un.org/depts/los/clcs_new/submissions_files/submission_rus_rev1.htm.

[27] Overlap between Canada's 2019 ECS and the Russian Federation's 2015 ECS (left); overlap between Canada's 2019 ECS and the Russian Federation's 2021 ESC (right).



https://doi.org/10.1017/cyl.2023.15 Published online by Cambridge University Press

21. Through filing the addendum, Canada informed the international community of its intent to delineate additional outer limits of its continental shelf to its 2019 submission. This addendum rebalances Canada's position in any future boundary delimitation negotiations, and clearly demonstrates that Canada will defend its continental shelf entitlement in the Arctic Ocean, and the sovereign rights and jurisdiction inherent to it.

Next steps

22. Canada's Extended Continental Shelf Program (ECS Program) has begun its review of the CLCS recommendations to the Russian Federation issued in February 2023.
23. Within the next five years, new data collection and analyses will continue with surveys in remote areas to further support Canada's addendum. Canada will file this information for the consideration of the CLCS.
24. Realistically, it may take ten or more years before the CLCS is in a position to begin reviewing Canada's 2019 submission given that the average time of consideration of a submission is three years, that the CLCS deals with nine submissions concurrently, and that there are an estimated 34 submissions ahead of Canada's Arctic submission as of early March 2023. This does not count revised submissions, which take priority. Similarly, this does not include submissions in the queue that are blocked from consideration due to disputes, though it is possible their status could change if the states involved furnish the CLCS with non-objection notes. Also as of early March 2023, there are an estimated 20 submissions ahead of Canada's Atlantic submission for consideration.
25. Canada understands that there is a need to maintain knowledge and data in support of both submissions during this period prior to and during consideration by the CLCS. The ECS Program will continue to augment these submissions with new data and information as they become available, and in light of improved knowledge and technologies.

7. International trade law

A. World Trade Organization (WTO)

Third Party Participation – China – Anti-Dumping and Countervailing Duty Measures on Barley from Australia (DS598)

In a letter to the chairperson in the dispute dated 4 March 2022, Canada outlined its position on the suspension of the Russian Federation's third party rights to the dispute. The representative of the Permanent Mission of Ukraine in Geneva warmly welcomed Canada's position on this issue (footnotes omitted to facilitate reading; citations are as they appear in Canada's original communication, which is available upon request by contacting jlt@international.gc.ca):

> […] We write further to Ukraine's recent communication that requested the suspension of the Russian Federation's third party rights in this dispute. Canada is deeply concerned by the ongoing events in Ukraine, the impact on its people, and its impact on this dispute.

https://doi.org/10.1017/cyl.2023.15 Published online by Cambridge University Press

Canada condemns in the strongest possible terms the Russian Federation's egregious and unprovoked attack. The invasion violates Ukraine's sovereignty and territorial integrity and therefore clearly violates both international law and the Charter of the United Nations. Canada asks that the Panel grant Ukraine's request and exercise its discretion to temporarily suspend the Russian Federation's third party rights in this dispute. In our view, the Dispute Settlement Understanding (DSU) provides the Panel with the discretion to do so.

Article 12.1 of the DSU provides that panels shall follow the Working Procedures in Appendix 3, "unless the panel decides otherwise after consulting with the parties to the dispute". Appendix 3 sets out a proposed timetable for panel work in paragraph 12 that provides that the "above calendar may be changed in the light of unforeseen developments." The Russian Federation's aggression clearly constitutes such an unforeseen development. The Panel should, thus, first consult with Australia and China and then exercise its discretion and modify the proposed timetable for Panel work to suspend the participation of the Russian Federation in the third party session until such time as the conflict is resolved and Ukraine is able to fully exercise its third party rights in this proceeding.

Ukraine has a substantial interest in this matter and duly notified this interest to the Dispute Settlement Body. Pursuant to Article 10.2 of the DSU, Ukraine has the right to have an opportunity to be heard by the Panel. Ukraine's ability to effectively exercise this right has been prejudiced and effectively vitiated by the Russian Federation's aggression. Moreover, Article 3.2 of the DSU states that the dispute settlement system is central to "providing security and predictability to the multilateral trading system." The actions of the Russian Federation have directly impeded the functioning of the dispute settlement system. In the current exceptional circumstances, permitting the Russian Federation to continue to exercise its third party rights while that Member is actively preventing Ukraine from exercising its own rights would undermine the WTO dispute settlement system and, in turn, the security and predictability of the multilateral trading system itself.

The Russian Federation's assault on Ukraine constitutes a serious breach of the peremptory norm of general international law (*jus cogens*) on the prohibition of aggression. The Panel should take into consideration relevant norms of international law, as identified by the International Law Commission (ILC) in the *Draft Articles on Responsibility of States for Internationally Wrongful Acts* (*Articles on State Responsibility*) and the *Draft Conclusions on the Peremptory Norms of General International Law* (*jus cogens*) (*Draft Conclusions*). Canada observes that panels and the Appellate Body have found that the *Articles on State Responsibility* set out recognized principles of customary international law. Article 41 of the *Articles on State Responsibility* provides that "States shall cooperate to bring to an end through lawful means any serious breach" by a State of an obligation arising under a peremptory norm of general international law, such as the prohibition against aggression. A similar provision is found in Conclusion 19 of the *Draft Conclusions*. The ILC Commentary to Conclusion

https://doi.org/10.1017/cyl.2023.15 Published online by Cambridge University Press

> 19 explains that the obligation of States to act collectively has "particular consequences" for cooperation within international organizations (such as the WTO) and that, in the face of serious breaches of jus cogens, international organizations "should act, within their respective mandates and when permitted to do so under international law, to bring to an end such breaches". Moreover, if an international organization has the discretion to act, the obligation to cooperate also "imposes a duty on the members of that international organization to act with a view to the organization exercising that discretion in a manner to bring to an end" to the breach.
>
> This Panel has the discretion under the DSU to act by temporarily suspending the participation of the Russian Federation in the third party session, thereby assisting in bringing to an end Russia's serious breach of the prohibition on aggression. As an adjudicative body of the WTO, the Panel should exercise this discretion in accordance with the duty expressed in the Draft Conclusions. Only this step sends the clear and unequivocal message that lawlessness and violence that impede the functioning of the WTO dispute settlement process will not be tolerated.
>
> If, however, the Panel declines to exercise its discretion in this manner, Canada endorses the positions taken by Australia, the European Union, and the United Kingdom, and will join their delegations in declining to participate in the portion of the third-party session in which the Russian Federation will make its oral statement.
>
> At the time of writing, Ukrainian cities are under relentless attack. The WTO, the WTO Members, and the Panel have a duty to do whatever is in their power and discretion to help bring an end to Russian Federation aggression.

Trade Facilitation Agreement (TFA) — China — Measures Concerning the Importation of Canola Seed from Canada (DS589)

In its first written submission, dated 6 January 2022, Canada made the following arguments on Articles 7.4.2 and 7.4.4 of the *Trade Facilitation Agreement* (*TFA*) (footnotes omitted to facilitate reading):

> 519. The *TFA* aims to expedite the movement, release, and clearance of goods. Article 7 of the *TFA* sets out procedures for the release and clearance of goods for import, export, or transit. The purpose of Article 7.4 is to facilitate trade by requiring Members to concentrate customs control practices and procedures on high-risk consignments while expediting the release of low-risk consignments. More specifically, Article 7.4 regulates the methodology and practices that customs authorities use to determine which import, export, or transit transactions should be subject to control and the type and degree of control to be applied. Article 7.4 focuses on the use of risk assessment and risk management to manage and facilitate customs clearance. […]
>
> 522. The concept of "risk assessment", which is found in Article 7.4.4 of the *TFA*, refers to the assessment of risks arising from consignments. To manage risks, a Member must first establish what risks need to be managed pursuant to

https://doi.org/10.1017/cyl.2023.15 Published online by Cambridge University Press

a risk assessment. Risk management is the stage after the risk assessment where a Member decides what is the most appropriate response to manage the risk that has been identified in the assessment of risk.

523. The *TFA* does not define the term "risk management". In the broader customs context, the World Customs Organization ("WCO") defines "risk management" as "the systematic application of management procedures and practices which provide customs with the necessary information to address movements or consignments which present a risk". When risk management involves SPS control and more specifically, pest risk management, the ISPMs applicable to pest risk analysis provide relevant context for the purposes of understanding the concept of "risk management" under Article 7.4.2. ISPM 11 describes risk management as "identifying management options for reducing the risks identified at Stage 2 [risk assessment]. These are evaluated for efficacy, feasibility and impact in order to select those that are appropriate".

524. The risk management that is at issue in this case is the management option – China's prohibitions - that was chosen to control the alleged risks arising from imports of canola seed from Canada's two largest exporters. […]
527. Article 7.4.2 requires Members to design and apply risk management in a manner "as to avoid" arbitrary and unjustifiable discrimination and disguised restrictions on international trade. It provides that:

Each Member shall design and apply risk management in a manner as to avoid arbitrary and unjustifiable discrimination, or a disguised restriction on international trade.

528. The text indicates that a violation of Article 7.4.2 will be established where:

- A Member has failed to design or apply risk management "in a manner as to avoid" arbitrary and unjustifiable discrimination; OR
- A Member has failed to design or apply risk management "in a manner as to avoid" a disguised restriction on international trade.

529. We examine these two elements of the text in the next sections, but to begin, we offer the following observations.

530. The phrase "in a manner as to avoid arbitrary or unjustifiable discrimination, or a disguised restriction on international trade", must be interpreted in accordance with the customary rules of interpretation set out in the *Vienna Convention on the Law of Treaties* (*VCLT*). Article 31 of the *VCLT* prescribes that a treaty shall be interpreted "in good faith in accordance with the ordinary meaning to be given to the terms of the treaty in their context and in the light of its object and purpose." A fundamental rule of treaty interpretation is that a treaty interpreter shall read and interpret the words used by the agreement under examination, and not the words which the interpreter may feel should have been used.

https://doi.org/10.1017/cyl.2023.15 Published online by Cambridge University Press

531. For the reasons that follow, the test to establish whether a Member has failed to design and apply risk management "in a manner as to avoid" arbitrary and unjustifiable discrimination" is whether the risk management measure at issue bears a rational connection to its stated objective. A measure that is designed and applied in a manner as to avoid arbitrary and unjustifiable discrimination is a measure that is reasonably applied and designed to achieve its asserted purpose.

532. Article 7.4.2 imposes an affirmative obligation on Members to design and apply risk management in a manner "as to avoid" any arbitrary and unjustifiable discrimination, or disguised restriction on international trade. The use of the terms "as to avoid" instead of, for example, not to "afford", "create" or "constitute" suggests that the drafters intended to provide a test different from other provisions in the WTO agreements that refer to arbitrary and unjustifiable discrimination, or a disguised restriction on international trade.

533. Unlike any other provision in the WTO agreements that refer to arbitrary and unjustifiable discrimination, or a disguised restriction on international trade, a violation of Article 7.4.2 is not conditioned upon a finding of discrimination. That is, the text of Article 7.4.2 does not require a Complainant to show that the design or application of the risk management at issue constitutes discrimination or a disguised restriction.

534. Further, Article 7.4.2 does not require a Party to demonstrate likeness or that the same/similar conditions prevail between comparators, which is typically required under WTO provisions prohibiting discrimination. The concept of "likeness" is found in many different provisions of the WTO agreements to assess whether there is a competitive relationship in the marketplace between the relevant goods or services at issue. Article 7.4.2 does not refer to any methodology of comparison to assess whether risk management is designed or applied in a manner as to avoid arbitrary or unjustifiable discrimination. Without any methodology of comparison explicitly set out in the text, it is clear that the drafters intended for the concept of discrimination to encompass both making distinctions between similar situations and treating dissimilar situations in a formally identical manner.

535. The object and purpose of Article 7.4.2 supports this interpretation. Article 7.4 aims to facilitate trade by concentrating customs controls on high-risk consignments and expediting the release of low-risk consignments. In particular, Article 7.4 recognizes that for the clearance and release of goods, WTO Members may differentiate between goods, based on an assessment of risk through selectivity criteria. There is an inherent acknowledgement that customs risk management involves making distinctions between goods based on their risk profiles and appropriate selectivity criteria, such as the country of origin.

536. The rational connection test is based on the parallels between the chapeau of Article XX of the *GATT* and Article 7.4.2 of the *TFA* where both provisions

https://doi.org/10.1017/cyl.2023.15 Published online by Cambridge University Press

aim to prevent the abuse and illegitimate use of the Parties' rights under these agreements. In *US – Gasoline*, the Appellate Body explained that the purpose of the chapeau of Article XX is the prevention of abuse of the exceptions of Article XX. The Appellate Body stated that exceptions are not to be abused or misused, in other words, the measures must be applied reasonably, and not be applied so as to frustrate or defeat the legal obligations of a party. In the context of the *TFA*, the Parties have the right to design and apply risk management using appropriate selectivity criteria, such as the country of origin, which may lead to discrimination based on different risk profiles of goods. However, the use of selection criteria should not be abused or misused, and risk management must be based on an assessment of risk.

537. The Appellate Body has explained that the assessment of whether discrimination is "arbitrary" or "unjustifiable" should be made in light of the objective of the measure. In *Brazil – Retreaded Tyres*, the Appellate Body found that an analysis of whether discrimination is arbitrary or unjustifiable "should focus on the cause of the discrimination, or the rationale put forward to explain its existence". Similarly, in *US – Poultry (China)* the panel concluded that the meaning of "arbitrary or unjustifiable discrimination" involves a consideration of whether there is a "rational connection" between the reasons given for the discriminatory treatment and "the stated objective of the measure".
538. In the case of risk management, the policy objective is to address the risks that have been identified and evaluated through a risk assessment. Accordingly, a risk management measure that is not rationally related to the objective of addressing the risks that have been identified and evaluated through a risk assessment would not be designed and applied in a manner as to avoid arbitrary and unjustifiable discrimination.

B. Regional trade agreements

United States — Automotive Rules of Origin (USA-MEX-2022-31-01) — Rebuttal Submission of Canada

In its rebuttal submission, dated 10 June 2022, Canada made the following arguments on the Article 32 of the *Vienna Convention on the Law of Treaties* (*VCLT*) (extracts below, confidential information and footnotes have been removed to facilitate reading; the submission is available upon request by contacting jlt@international.gc.ca):

66. The United States attempts to dissuade the panel from considering highly relevant supplementary material that Canada submitted in its initial written submission by: (1) erroneously setting out Canada's position with respect to the use of this material under Article 32 of the *VCLT*; and (2) arbitrarily placing temporal limits on the evidence that can be considered under Article 32. In this section, Canada will explain these errors and demonstrate that the Panel should consider the supplementary material at issue – namely, communications and presentations by officials from the United States Trade Representative (USTR) following the conclusion of the treaty but prior to the treaty coming into effect

https://doi.org/10.1017/cyl.2023.15 Published online by Cambridge University Press

The United States misconstrues Canada's position on Article 32 of the *VCLT*

67. The United States misconstrues Canada's position on the use of supplementary material captured by Article 32. Contrary to the assertions of the United States,[51] Canada has never suggested that this Panel should ignore the general rule of treaty interpretation set out in Article 31 of the *VCLT* and instead interpret the provisions at issue by first relying on supplementary material.

68. However, the Panel has discretion to refer to material under Article 32. These supplementary materials can be used in two ways: (1) to confirm the interpretation that the Panel derived by applying the general rule of interpretation under Article 31; or (2) to determine the meaning of the text of the treaty if the interpretation that was derived by applying Article 31 leaves the meaning ambiguous or obscure, or leads to a result which is manifestly absurd or unreasonable. Thus, determining the meaning of the treaty is not the only function of Article 32. Panels may also rely on supplementary material to confirm their interpretation of the treaty.

69. While the panel in *Canada – Dairy (CUSMA)* reached a clear reading of the disputed provision by applying the general rule of interpretation under Article 31 of the *VCLT*, it also considered supplementary material under Article 32. The panel said it was their responsibility to do so in order "to determine the reality of the situation which the parties wished to regulate by means of the treaty".

70. Canada reiterates here that the Panel has discretion to refer to the supplementary material to confirm its interpretation in this case.[54] Canada did not make specific submissions regarding the Panel's use of the supplementary material to determine the meaning of the text of the treaty because the text of the treaty clearly accords with Canada's interpretation. Thus, Canada does not expect that the Panel will find an ambiguous, obscure, manifestly absurd or unreasonable meaning. However, in light of the high degree of relevance of the supplementary material, the Panel should exercise its discretion to use this material to confirm its interpretation.

The United States erroneously places a temporal limit on the supplementary material captured by Article 32 of the *VCLT*

71. Contrary to the United States' submission, this Panel is free to consider supplementary material from a time period after the conclusion of the treaty, if this material is relevant.[55]

72. The United States argues that there is a temporal condition on the material captured by Article 32. However, in carrying out its analysis, it only focusses on two examples of material captured by Article 32: material that constitutes

https://doi.org/10.1017/cyl.2023.15 Published online by Cambridge University Press

travaux préparatoires[56] and material in connection with the conclusion of the treaty.[57]

73. WTO and CUSMA panels as well as academics have been clear that Article 32 contemplates an open list of material and not just *travaux préparatoires* and material connected with the conclusion of the treaty. The panel in *Canada – Dairy (CUSMA)*, found that the *VCLT* should not be read to limit the type of evidence that may be considered. As long as the proper purpose is identified, a panel may consider materials relevant to the issues in dispute. While Article 32 expressly refers only to the preparatory work of the treaty and to the circumstances of its conclusion, the use of the word "including" means that the list is illustrative and not exhaustive.[58]

74. The Panel must decide whether the material in question can reasonably be thought to assist in either establishing or confirming the meaning of the treaty under consideration. If it does, there are hardly any clear limits to taking into account material under Article 32.[59] Material that can usefully serve as a guide towards establishing the meaning of the disputed provisions should not be deliberately ignored.[60] The supplementary materials that Canada has put forth directly address the meaning of the provisions that this Panel is tasked to interpret.

75. In fact, subsequent practice that cannot qualify under Article 31.3(c) of *VCLT* may still qualify under Article 32 if it can shed some light on the meaning of the treaty.[61] For example, the panel in *EC – Chicken Cuts (Brazil)*, in considering practices regarding classification of certain goods after the conclusion of the *General Agreement on Tariffs and Trade* (*GATT* 1994), said that even if the subsequent practice did not quality under Article 31(3)(b), the panel could take it into consideration under Article 32 of the *VCLT*.[62] The Appellate Body also held similar views with respect to documents published, events occurring, or practice followed subsequent to the conclusion of the treaty. It said such material:

[…] may give an indication of what were, and what were not, the 'common intentions of the parties' at the time of the conclusion. The relevance of such documents, events or practice would have to be determined on a case-by-case basis.[63]

76. Therefore, while *travaux préparatoires* or material relating to the conclusion of the treaty may be limited to those that existed before the conclusion of a treaty, this limitation clearly does not apply to all material captured by Article 32.

8. Investor-state dispute settlement

A. North American Free Trade Agreement (NAFTA)

Article 1139(h) — "Interests Arising from the Commitment of Capital or Other Resources in the Territory of a Party to Economic Activity in Such Territory"

https://doi.org/10.1017/cyl.2023.15 Published online by Cambridge University Press

Koch Industries, Inc. and Koch Supply & Trading, LP v. Government of Canada — Canada's Rejoinder Memorial on Jurisdiction and the Merits

In its rejoinder memorial on jurisdiction and the merits, dated 30 September 2022, Canada made the following arguments on the Article 1139(h) of *NAFTA* (extracts below, footnotes omitted to facilitate reading. Submission available at <icsid.worldbank.org/cases/case-database/case-detail>:

Article 1139(h) Is Not a Catch-All Category of Investment

142. In their Reply Memorial, the Claimants rely heavily on their broad notion of the term "interest", standing on its own, and an allegation that Article 1139(h) is "understood to operate as a 'catch-all' category of investment." Contrary to the principles of proper treaty interpretation, the Claimants ignore the context in which the term "interest" appears. As a result, they overlook the specific requirements that must be met for an interest to qualify for protection under Article 1139(h).

143. As Canada explained in its Counter-Memorial, the definition of "investment" in *NAFTA* Article 1139 provides an exhaustive list of the eight types of interest that qualify as "investments" under the treaty. Each subparagraph in the list refers to a different kind of interest, specifically defined and featuring particular requirements. Accordingly, the mere identification of an alleged "interest" does not suffice to qualify the interest as an investment; the "interest" must also meet the particular requirements of the category at issue. *NAFTA* Article 1139(h) is no exception.

144. The requirements of Article 1139(h) are gleaned from both the chapeau and its illustrative sub- paragraphs. The Claimants' attempt to read out the subparagraphs is contrary to the principles of treaty interpretation. The subparagraphs constitute highly relevant context that elucidates the kind of interest captured by Article 1139(h). Prior NAFTA tribunals have dismissed similar attempts to focus exclusively on the chapeau of Article 1139(h), explaining:

The *chapeau* cannot be read by itself. The *NAFTA* does not extend protection to any "commitments of capital", but only to those which exhibit certain features so as to give rise to "interests". These features are defined through two illustrative examples in subparagraphs (h.i) and (h.ii).

145. The Claimants incorrectly argue that the "emission allowances do not need to correspond to either such illustrative examples in order to fall within the scope of Article 1139(h)." Sub- paragraphs (h)(i) and (h)(ii) help to define the features of an investment that qualifies under Article 1139(h). While an alleged interest need not fall squarely within one of the illustrative examples, it must exhibit similar features.

146. The common features of the illustrative examples include references to contracts; the presence of an investor's property or an enterprise in the territory

https://doi.org/10.1017/cyl.2023.15 Published online by Cambridge University Press

of the host Party; and economic activities in the territory of the host Party (e.g. turnkey or construction contracts or concessions; or production, revenue or profits of an enterprise). The types of contractual interests illustrated in subparagraphs (h)(i) and (h)(ii) thus confirm that, for an interest to meet the requirements of Article 1139(h), it must be longer-term and include an important commitment of capital contributing to the economic development of the host State.

147. Articles 1139(i) and (j) further confirm that more is required under Article 1139(h) than "claims to money" (as opposed to capital) arising from cross-border sales agreements for goods or services (1139(i)(i)), the extension of credit in connection with a commercial transaction (1139(i)(ii)), or any other claims to money that do not otherwise fall within the specifically enumerated categories of investment in Article 1139. The Claimants do not dispute that cross-border trading interests do not qualify as investments under Article 1139(h).

Cite this article: Kessel, Alan H. 2022. "At Global Affairs Canada in 2022." *Canadian Yearbook of International Law/Annuaire canadien de droit international*, 60: 292–338, doi:10.1017/cyl.2023.15