# Argentina necesita una declaración sobre la aplicabilidad del derecho internacional en el ciberespacio: ¿Por qué?

Argentina requires a statement on international law´s application in cyberspace: Why?

Por María Pilar Llorens

**Resumen:** En la actualidad, los debates sobre la aplicabilidad del derecho internacional en el ciberespacio se centran en precisar cómo se aplican las normas internacionales en este ámbito. A fin de contribuir con esta discusión los Estados han comenzado a dar a conocer sus posiciones a través de declaraciones sobre la aplicabilidad del derecho internacional en el ciberespacio (DDIC). Este no es el caso de la Argentina. A pesar de su participación en foros internacionales así como el desarrollo de legislación interna, el país no cuenta con una sistematización de su posición en esta cuestión. Como resultado de ello este trabajo propone que la Argentina debería adoptar una DDIC que reúna y estructure la postura que el Estado ha venido expresando de forma incipiente durante los últimos años. A estos efectos se analiza qué es una DDIC examinando su alcance y su contenido. Luego se sistematiza la posición de la Argentina a partir de los diversos documentos que ha producido el Estado. Finalmente, se propone el contenido que debería abordar una DDIC argentina.

**Palabras clave:** Derecho internacional; ciberespacio; declaración de derecho internacional; Argentina.

**Abstract:** On-going debates about the applicability of international law to cyberspace tend to focus on how legal rules and principles apply in this domain. For the last couple of years a growing number of Statements on International Law's Application in Cyberspace (SILACs) has been released. In these documents States share their view regarding this topic. However, this is not the case for Argentina. The country has not laid out its position concerning this matter. In this paper it is argued that Argentina should release a SILAC. This document should analyse and systematise the country's views on some of these issues. Consequently, the paper examines in the first place the scope and the content of a SILAC. Then drawing from various official documents it lays out the Argentine position regarding the applicability of international law to cyberspace. Finally, the paper advances the content that an Argentine SILAC should cover.

**Keywords:** international law; cyberspace; statement of international law; Argentina.

Fecha de recepción: 30/06/2021
Fecha de aceptación: 13/10/2021

# Argentina necesita una declaración sobre la aplicabilidad del derecho internacional en el ciberespacio: ¿Por qué?

Por María Pilar Llorens*

## I. Introducción

En la comunidad internacional existe una preocupación creciente por regular las actividades que tienen lugar en el ciberespacio. Así, desde 1998, la Asamblea General de las Naciones Unidas (AG) ha patrocinado discusiones en el ámbito de los avances en la informatización y las telecomunicaciones en el contexto de la seguridad internacional. Ello le ha permitido adoptar una serie de resoluciones en la materia[1], así como también establecer seis Grupos de Expertos Gubernamentales (GEG) y un Grupo de Trabajo de Composición Abierta (GTCA). De los cuáles los más recientes han culminado sus labores[2].

Los informes finales de los GEG de 2013 (A. G. 68/98), de 2015 (A. G. 70/174), así como el de 2021 (A. G. 76/135) afirmaron la aplicabilidad del derecho internacional al ciberespacio. No obstante, todavía existen profundas diferencias entre los Estados acerca del modo en que las normas y los principios internacionales deben aplicarse en este ámbito (Akande et al., 02 06 2021; Schmitt, 10 06 2021, p.

* Centro de Investigaciones Jurídicas y Sociales (CIJS) – Consejo Nacional de Investigaciones Científicas y Técnicas (CONICET) Universidad Nacional de Córdoba (UNC), Facultad de Derecho. Correo electrónico: mpllorens@derecho.unc.edu.ar

[1] Estas resoluciones se pueden consultar en el sitio web de Naciones Unidas dedicado a este tema: https://www.un.org/disarmament/ict-security/

[2] EL GEG 2019-2021 adoptó por consenso su informe final el 28 de mayo de 2021. El GTCA hizo lo propio el 21 de marzo de 2021. A la fecha, el primero (A.G. 76/135) puede ser consultado en el siguiente enlace: https://front.un-arm.org/wp-content/uploads/2021/08/A_76_135-2104030S-1.pdf. Fecha de acceso: 09 11 2021. El segundo se encuentra disponible en: https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf. Fecha de acceso: 02/06/2021

35)[3]. Como resultado de ello, los miembros de la comunidad internacional han comenzado a explicitar sus puntos de vista con un doble objetivo: por un lado, contribuir a la discusión internacional sobre cómo debe aplicarse el derecho internacional al ciberespacio y, por el otro lado, precisar cuál consideran que es la correcta aplicación de la normativa internacional en dicho ámbito[4].

Hasta el momento menos de veinte Estados han explicitado su posición en la materia; aunque es probable que su número aumente considerablemente, ya que la AG ha exhortado a los Estados a contribuir con el debate internacional compartiendo sus posiciones nacionales (A. G. Res. 73/266). La mayoría de las publicaciones disponibles provienen de Estados del norte global (Alemania (Alemania, 2021); Australia (Australia, 2021); Estonia (Kaljulaid, 2019); Estados Unidos (Egan, 2016; Koh, 2012); Francia (Francia, 2019); Finlandia (Finland, 2020); Nueva Zelanda (Nueva Zelanda, 2020); Países Bajos (Países Bajos, 2019); Suiza (Suiza, 2021); Reino Unido (Wright, 2018)). Aunque también existen declaraciones de dos Estados de Oriente Medio (Israel (Schönford, 2021) e Irán (Irán, 2020)). Los Estados latinoamericanos, con excepción de Brasil (A.G. 76/136, pp. 17-23), no han publicado sus posiciones nacionales en esta materia; solo alguno de ellos (Bolivia, Chile, Costa Rica, Ecuador, Guatemala, Guyana y Perú) han respondido el cuestionario del Comité Jurídico Interamericano sobre la aplicación del derecho internacional dentro de los Estados Miembros de la Organización de Estados Americanos (OEA) en el contexto cibernético (CIJ/doc. 615/20/rev.1) pero sus respuestas completas aún no se encuentran disponibles públicamente.

La Argentina, por su parte, no cuenta con una posición definida en la materia. Si bien ha afirmado su compromiso para contribuir con la construcción de un ciberespacio seguro donde imperen valores como la justicia y el respeto al derecho internacional (Argentina, 2020, p. 1), ni de sus intervenciones en foros

[3] Si bien el informe del GEG de 2021 ha reafirmado las conclusiones de los informes anteriores con relación a la aplicabilidad del derecho internacional en el ciberespacio, dado que a la fecha no se conocen las reacciones estatales a dicho documento su análisis no será abordado en el presente trabajo.

[4] En este trabajo solo se tienen en cuenta aquellos documentos que realizan un examen detallado de las normas internacionales que son de aplicación en el ciberespacio. No así aquellas declaraciones o contribuciones que los Estados han hecho en los foros internacionales.

internacionales ni de su legislación interna se desprende con claridad cuál es su postura. Explicitar y clarificar dicha posición es relevante a los fines de establecer con precisión cuáles son y cuál es el alcance de las reglas que, para el Estado, rigen su comportamiento en este ámbito.

En consecuencia, en este trabajo se sostiene que la Argentina debería adoptar una declaración sobre la aplicación del derecho internacional en el ciberespacio (DDIC). Es decir, un instrumento en el que exprese su posición a partir de un análisis de las normas y principios internacionales que entiende aplicables en el ciberespacio. Precisar esta posición, además, contribuye efectivamente al debate que está teniendo lugar en la comunidad internacional, permitiendo que otras voces participan en el debate y, consecuentemente, en el desarrollo progresivo de la normativa internacional pertinente.

La estructura de este trabajo se compone de cinco secciones. La segunda sección procura examinar qué es una DDIC. A estos efectos se definen las características generales de estas expresiones estatales destacándose especialmente la forma en que han sido emitidas puesto que esto influye en su alcance. Luego se sistematiza el contenido de las DDIC disponibles hasta la actualidad; en este aspecto se identifican dos grandes bloques normativos que facilitan el examen de las normas internacionales que regulan las operaciones cibernéticas[5]. Seguidamente se examina el alcance, es decir el valor jurídico, de estos instrumentos para el derecho internacional contemporáneo señalándose que se trata de documentos vinculantes. Finalmente, se examinan las ventajas y las desventajas de emitir una DDIC; así se concluye que los beneficios exceden las desventajas, por lo que los Estados deberían emitir estos documentos para contribuir en la determinación de la práctica estatal en la materia.

[5] Los términos operaciones cibernéticas y ciberoperaciones se utilizan de manera intercambiable en este trabajo. Por tal se entiende la utilización de capacidades cibernéticas para alcanzar objetivos en y a través del ciberespacio. (Schmitt, 2017, p. 237) (traducción propia). Se limitan a aquellas que tienen lugar en el ciberespacio (Delerue, 2020, p. 35).
También debe tenerse en cuenta que solo se tienen en cuenta aquellas operaciones que son llevadas adelante o que son patrocinadas por Estados.

La tercera sección, por su parte, persigue sistematizar la posición argentina con respecto a esta problemática. Para ello se describen los antecedentes normativos y luego se procura estructurar la posición del Estado a partir de la documentación oficial disponible, los registros de participación del Estado en foros internacionales, así como toda otra documentación relevante producida por los organismos internacionales en donde se ha tratado esta temática. En esta sección se demuestra que si bien la práctica argentina es dispersa, es posible detectar un patrón que permite reconstruir la posición estatal. Este revela que el Estado tiene una posición, aun cuando sea incipiente, con respecto a gran parte de la normativa internacional relevante para el ciberespacio. La cuarta sección, en tanto, retomando los patrones descriptos en la sección anterior delinea una propuesta de contenido para una DDIC nacional.

Finalmente, en la quinta sección se exponen las conclusiones que permiten responder a la pregunta que da título a este trabajo. Si bien la pregunta de la conveniencia de la emisión de la DDIC es de carácter político, en el trabajo se proveen los argumentos jurídicos que justifican su emisión. La Argentina necesita una DDIC por diversas razones; entre ellas se destacan la posibilidad de sistematizar de la posición estatal, la contribución efectiva al debate internacional y el establecer un marco normativo claro para todos los actores que desenvuelven sus actividades en el ciberespacio.

## II. ¿Qué es una declaración sobre la aplicación del derecho internacional al ciberespacio?

¿Cómo se aplica el derecho internacional en el ciberespacio? Es una pregunta que, en la actualidad, no tiene respuesta por la falta de consenso existente entre los miembros de la comunidad internacional. Como resultado de ello, y ante la falta de avances significativos en el ámbito de los GEG (especialmente en el de 2017 en el que no se alcanzó el consenso necesario para adoptar un informe final) (entre otros: Delerue, 2020, p. 19; Roguski, 2020a, p. 2), son varios los Estados que han optado por explicitar su posición en la materia.

Para ello los Estados han emitido discursos, informes y documentos de posición por medio de los cuales procuran explicar su postura y, por extensión, buscan mostrar cuál consideran que es la correcta interpretación de la normativa internacional. A fin de alcanzar este objetivo, los documentos realizan un examen (en general pormenorizado) de las principales normas internacionales aplicables en el ciberespacio.

Las DDIC, por lo tanto, son actos estatales relevantes. Permiten identificar la práctica estatal en esta materia (Roguski, 2020a, p. 2), ya que ayudan a establecer los parámetros relativos a la aplicación de ciertas normas internacionales en el ciberespacio. Un ejemplo sobre este punto es la discusión actual sobre la soberanía como una regla o como un principio de derecho internacional. Como se verá con mayor detalle en el apartado siguiente, la mayoría de los Estados entiende que se trata de una regla internacional que puede ser violada en sí misma (p. ej. la postura adoptada por Francia, Alemania, Finlandia, Estonia) y, por lo tanto, podría entenderse que esta posición prevalece por sobre la que la considera como un mero principio de derecho internacional que no es susceptible de violación (p. ej. la postura adoptada por el Reino Unido).

## II. 1. Contenido

Si bien el contenido de las DDIC emitidas hasta la actualidad varía conforme a las necesidades y los intereses de su autor, es posible identificar un patrón en el abordaje estatal. Dicho análisis, a su vez, es consistente con el tratamiento que el tema ha tenido tanto en los foros internacionales (ver, por ejemplo, A. G. Res. 68/98; A. G. Res. 70/174) como en la doctrina (p. ej. Manual de Tallin 2.0[6], Tsagourias y Buchan, 2015; Roscini, 2014).

Por lo tanto, las DDIC distinguen entre las normas que se aplican a las operaciones cibernéticas que tienen lugar en tiempos de paz y aquellas que se

[6] El Manual de Tallin 2.0 es una iniciativa del Centro de Excelencia para la Ciberdefensa asociado a la Organización del Tratado del Atlántico Norte que procuró definir la normativa aplicable al ciberespacio tanto en tiempos de paz como cuando la ciberoperaciones tienen lugar en el contexto de un conflicto armado internacional. Para más información ver: (Schmitt, 2017).

aplican a las ciberoperaciones que tienen lugar en el contexto de un conflicto armado (internacional o no internacional). Las primeras se refieren a cuestiones tales como la soberanía, el principio de no intervención, el régimen del *ius ad bellum*, la responsabilidad internacional, la atribución de las operaciones, entre otras. Las segundas, en cambio, se vinculan casi exclusivamente con el análisis de la aplicabilidad del derecho internacional humanitario en el contexto de las operaciones cibernéticas.

### II.1.1. El derecho internacional aplicable a las ciberoperaciones en tiempos de paz

Las DDIC abordan el examen de las normas y principios que regulan la conducta de los Estados en el ciberespacio durante aquellos períodos donde no existen conflictos armados, es decir que regulan la mayoría de las operaciones cibernéticas estatales (Delerue, 2020, pp. 41-42), y sobre cuyo alcance no existe consenso. Estas normas se refieren a cuestiones relativas a: obligaciones de los Estados; régimen del *ius ad bellum* y responsabilidad internacional. Estas problemáticas serán examinadas a continuación[7]:

Obligaciones de los Estados:

Bajo este tópico se examinan aquellas normas que, en el contexto cibernético, generarían obligaciones para los Estados: la obligación de respetar la soberanía de otros Estados; la obligación de no intervenir en los asuntos internos de terceros Estados, y la obligación de debida diligencia.

Soberanía[8]: La soberanía constituye uno de los principios fundamentales del derecho internacional. Supone la posibilidad que tienen los Estados de ejercer sus funciones inherentes de manera exclusiva sin interferencia de otros Estados. Lo que a su vez implica la obligación de proteger los derechos de otros Estados en los ámbitos en los que ejerce su jurisdicción (Remiro Brotóns, Riquelme Cortado, Díez-Hochleitner, Orihuela Calatayud, y Pérez-Prat Durbán, 2010, pp. 89-91).

[7] Debe tenerse en cuenta que este abordaje solo pretende realizar una presentación de los debates actuales en torno a estas problemáticas y, por lo tanto, no agota estas discusiones.

[8] Sobre este tema puede verse entre otros: (Moynihan, 2019; Fang, 2018; Corn y Taylor, 2017; Schmitt y Vihul, 2017).

En el contexto cibernético la cuestión de la soberanía se vincula con distintos aspectos. Por un lado, con la posibilidad de ejercer soberanía y jurisdicción sobre el ciberespacio; y por el otro lado, con la pregunta acerca de si una operación cibernética puede violar la soberanía de un tercer Estado.

El primer de estos aspectos se refiere a la posibilidad de que las infraestructuras de la información o bien las actividades vinculadas con estas infraestructuras puedan ser controladas por el Estado siempre que se encuentren ubicadas o se realicen en espacios bajo soberanía o jurisdicción del Estado. Esta discusión, a su vez, se ve influenciada por el debate sobre el modelo de gobernanza de Internet, que procura identificar qué Estados ejercen un control sobre este ámbito (Delerue, 2020, pp. 207-208, ver especialmente nota al pie 62). Debate que también se encuentra vinculado a la determinación de la naturaleza jurídica del ciberespacio (Eichensehr, 2014)[9]. La cuestión del modelo de gobernanza de Internet no será abordada en el presente trabajo porque los informes del GEG de 2013 y de 2015 reflejan el consenso de los Estados sobre la aplicabilidad del principio de soberanía en el ciberespacio.

El segundo aspecto -que es central en la DDIC-, en tanto, pretende determinar si y cuándo una operación cibernética puede violar la soberanía de un tercer Estado. De las expresiones estatales se desprende que existen dos enfoques diferentes para abordar la cuestión. Uno señala que la soberanía constituye una regla de derecho internacional que es susceptible de ser violada por los Estados (p. ej. Finlandia, Suiza). El otro, en tanto, señala que la soberanía es un mero principio de derecho internacional del que se desprenden otras normas de derecho internacional (p. ej. la prohibición de la amenaza y el uso de la fuerza) que si pueden verse afectadas por una operación cibernética (p. ej. Reino Unido).

A su vez, el enfoque de la soberanía como regla tiene diferentes concepciones dependiendo de cuáles sean las condiciones que sean requeridas por los Estados para que pueda entenderse que una ciberoperación violó la soberanía de otro Estado. Así, pueden identificarse una concepción de la penetración y otra de

[9] Sobre la cuestión de la naturaleza jurídica puede verse: (Llorens, 2021) y las obras allí citadas.

*minimis*. La primera entiende que cualquier penetración no autorizada constituye una violación de la soberanía del Estado (p. ej. Francia), mientras que la segunda requiere un mínimo de daño en una infraestructura del Estado para que pueda entenderse que existió una violación a la soberanía (p. ej. Estados Unidos).

No intervención[10]: El principio de no intervención supone el derecho de todo Estado de conducir sus asuntos sin injerencia exterior. Es decir, el derecho que tiene todo Estado de llevar adelante sus asuntos (internos o externos) sin que exista un acto de intervención entendido como el "acto por el que un Estado – o grupo de Estados- se entromete por vía de autoridad en los asuntos que son de la jurisdicción doméstica de otro, imponiéndole un comportamiento determinado" (Remiro Brotóns, Riquelme Cortado, Díez-Hochleitner Rodríguez, Orihuela Calatayud, y Pérez-Prat Durbán, 2007, p. 138).

Conforme lo señaló la Corte Internacional de Justicia en el asunto de las Actividades militares y paramilitares en y contra Nicaragua (1986) (en adelante caso Nicaragua) el principio de no intervención se caracteriza porque: la intervención la lleva adelante un Estado contra otro Estado, la intervención afecta cuestiones que son propias del dominio reservado de los Estados y existe un elemento de coerción por medio del que se procura influir en la conducta de un Estado (pp. 107-108, para. 205).

En el contexto cibernético, se procura establecer cuándo una operación cibernética puede violar el principio de no intervención. Es decir, cuándo afecta los asuntos internos de otro Estado. En general, los Estados coinciden en es preciso que exista un cierto grado de coerción. Ello implica que un Estado, por medio de una ciberoperación, debe influir sustancialmente en el comportamiento de otro Estado de manera tal que provoque una acción o una omisión sobre cuestiones que son del dominio reservado de dicho Estado (p. ej. Alemania y Países Bajos).

Debida diligencia[11]: El principio de diligencia debida constituye un corolario del principio de soberanía e implica la obligación de los Estados de no permitir que

[10] Sobre este tema pueden verse entre otros: (Delrue, 2020, pp. 233-172; Hollis, 2016).

[11] Sobre esta obligación en el contexto cibernético puede verse entre otros: (Banneliere-Christakis, 2015; Kolb, 2015; Schackeldford, Russell, y Kuehn, 2015; Schmitt, 2015)

su territorio sea utilizado para llevar adelante actos que afecten los derechos de otros Estados (*Asunto del Canal de Corfú (Albania vs. Gran Bretaña)*, 1949, p. 22). Constituye una obligación de medios y no de resultados (Delerue, 2020, p. 354).

Es entendido como un estándar de conducta que permite evaluar la conducta del Estado en el caso concreto (Fitzmaurice, 2017, p. 365; Jensen y Watts, 2017, p. 1566). Es decir, permite analizar si las consecuencias de un hecho ilícito podrían haberse evitado si el Estado no hubiera realizado el acto o bien si no hubiera prevenido su realización (Stephens y French, 2016, p. 365).

En el contexto cibernético la debida diligencia supone la obligación de los Estados de no permitir que su territorio sea utilizado para lanzar una ciberoperación que afecte otro Estado o bien para que esta transite por aquel; como resultado de ello, el Manual de Tallin 2.0 señala que hay tres partes que participan de esta relación: el Estado que es atacado, el Estado territorial y una tercera parte que es la autora de la ciberoperación (Schmitt, 2017, p. 32).

La mayoría de las DDIC examinadas señalan que se trata de una obligación de comportamiento (p. ej. Estonia y Finlandia), que tiene una base consuetudinaria (p. ej. Francia) y que impone al Estado la obligación de realizar de adoptar todas las medidas que razonablemente son necesarias para evitar que su territorio sea utilizado para afectar los derechos de terceros Estados (p. ej. Estonia). El análisis sobre la razonabilidad de las medidas se debe realizar caso por caso (p. ej. Países Bajos). Debe destacarse que Israel señala que se trata de una obligación no vinculante para los Estados (Schönford, 2021).

Régimen del *ius ad bellum*[12]:

El régimen del *ius ad bellum* se pregunta acerca de la licitud del uso de la fuerza en el ámbito de la comunidad internacional. Por ende, en el contexto cibernético procura identificar cuándo una operación cibernética constituye un uso de la fuerza prohibido en el derecho internacional. Asimismo, examina si una ciberoperación constituye un ataque armado que dé lugar al ejercicio del derecho de legítima defensa.

[12] Entre otros ver: (Delerue, 2020; Schmitt, 2017; Roscini, 2014).

En el primero de los casos la mayoría de las DDIC examinadas señalan que las disposiciones contenidas en el artículo 2, párrafo 4, de la Carta de las Naciones Unidas (Carta o CNU) son plenamente aplicables al ciberespacio. Para determinar cuándo una ciberoperación constituye un uso de la fuerza contrario al artículo 2 (4) de la CNU las DDIC en general tienden a adoptar el modelo propuesto en el Manual de Tallin (tanto en su primera como en su segunda versión)[13] (p. ej. Alemania y Estonia). Este modelo propone considerar que existe una violación a dicho artículo cuando la escala y los efectos de una operación cibernética sean comparables con los de una operación militar convencional (cinética). Como resultado de ello, son pocas las operaciones cibernéticas que alcanzan a cruzar este umbral.

El segundo aspecto abordado por las DDIC se vincula con la posibilidad de ejercer el derecho de legítima defensa en el contexto cibernético. Los documentos estatales señalan que los Estados cuentan con el derecho de responder un ataque armado convencional tanto a través de operaciones convencionales como por medio de operaciones cibernéticas. Más complejo es precisar cuándo una operación cibernética constituye un ataque armado o ciberataque. En este sentido, las DDIC tienden a señalar que para que ello ocurra se requiere que la operación cibernética sea comparable en su escala y efectos a un ataque armado convencional; siendo este un análisis que se realiza caso por caso (p. ej. Francia). A su vez, las DCCI detallan que la respuesta a un ataque cibernético no se limita a los medios cibernéticos y también se encuentra autorizado el uso de medios convencionales (p. ej. Finlandia).

Responsabilidad internacional:

Bajo esta categoría se agrupa un conjunto de normas relativas al régimen de responsabilidad internacional de los Estados. Entre ellas se encuentra la cuestión de la atribución, así como también la posibilidad de utilizar contramedidas o bien alegar causales de exclusión de la ilicitud como el estado de necesidad.

[13] A su vez, el modelo receptado en los Manuales de Tallin (Schmitt, 2013, pp. 48-52; 2017, pp. 333-337) se basan en el modelo propuesto por Michael Schmitt en su trabajo seminal: Computer network attack and the use of force in international law: Thoughts on a normative framework. (Schmitt, 1999)

Atribución[14]: La cuestión de la atribución constituye una de las cuestiones más complejas en relación con las ciberoperaciones debido a que las propias características del ciberespacio dificultan (especialmente a nivel técnico) la identificación precisa del/los autor/es de la operación. Superado el proceso técnico de atribución, resta que el Estado lleve adelante una atribución legal de la conducta a otro Estado.

La mayoría de las DDIC coinciden en señalar que se aplican las reglas generales recogidas en el Proyecto de Artículos sobre la Responsabilidad Internacional de los Estados por Hechos Ilícitos (Proyecto de artículos) de la Comisión de Derecho Internacional de 2001 (p. ej. Finlandia y Reino Unido). Esto implica, por ejemplo, que un Estado va a ser responsable por aquellas operaciones cibernéticas que le sean atribuibles ya sea porque fueron llevadas a cabo por un órgano del Estado, como un comando de ciberespacio (art. 4) o por una persona que ejerce funciones de poder público (art. 5). El caso más problemático se refiere a aquellos supuestos en los que la ciberoperación es llevada adelante por particulares (art. 8). En este caso el examen de las DDIC varía, ya que difiere el grado de control sobre los particulares que es exigido para que el Estado pueda ser responsabilizado por dichas cibereoperaciones.

Estado de necesidad[15]: El estado de necesidad constituye un mecanismo que permite eximir de responsabilidad internacional al autor de un hecho ilícito siempre que se reúnan una serie de condiciones estrictas que han sido delineadas en el artículo 25 del Proyecto de artículos: a) sea el único modo para salvaguardar un interés esencial del Estado de un peligro grave e inminente y b) no afecte gravemente los intereses de otro Estado.

Algunos Estados consideran en el contexto cibernético es posible alegar el estado de necesidad (p. ej. Alemania y Países Bajos). Señalan que las condiciones para su aplicación son las exigidas en el Proyecto de artículos. Estas deben ser evaluadas en el caso concreto.

---

[14] Sobre este tema se puede consultar entre otros: (Delerue, 2019; Finlay y Payne, 2019; Banks, 2017; Maçák, 2016).

[15] Puede verse: (Arimatsu y Schmitt, 2021; Lahmann, 2020, pp. 201-258).

Contramedidas[16]: Las contramedidas constituyen otra de las eximentes de la responsabilidad internacional de los Estados. Excluyen la ilicitud de aquellas medidas que implican un incumplimiento de una obligación internacional en tanto procuren que otro Estado cese en su hecho ilícito y repare sus consecuencias (art. 22 y concordantes del proyecto de artículos). En el ámbito cibernético han sido reconocidas como uno de los mecanismos de respuesta[17] con los que cuentan los Estados para hacer frente a una ciberoperación internacionalmente ilícita.

Las DDIC señalan que son de aplicación las reglas generales delineadas en el Capítulo II, de la Parte III del Proyecto de artículos de 2001. Estas imponen ciertas condiciones para la procedencia de las contramedidas: a) dirigidas solo contra el Estado responsable; b) el objetivo de la medida es inducir al Estado responsable a cumplir con las obligaciones que le incumban; c) las medidas serán temporales, necesarias y proporcionales; d) las medidas no podrán violar la prohibición del uso de la fuerza, las normas de protección de los derechos humanos, las obligaciones de carácter humanitario que prohíben las represalias, ni tampoco las normas imperativas.

Algunas DDIC señalan que el requisito de la notificación previa puede llegar a no ser viable en el contexto cibernético (p. ej. Estonia y Finlandia). Las propias características de las operaciones cibernéticas que pueden requerir un actuar inmediato y secreto, así como la inexistencia de una norma de derecho internacional que obligue a los Estados a exponer sus capacidades cibernéticas justifican esta posición (p. ej. la postura del Reino Unido, Schmitt, 2017) (en contra de esta postura: Delerue, 2020, pp. 445-448).

Otro punto que causa profundos desacuerdos[18] es la posibilidad señalada por algunos Estados (v.g. Estonia) de utilizar contramedidas colectivas. Es decir, la

[16] Algunos autores que pueden verse: (Delerue 2020, pp. 453-460; Kosseff, 2020a; 2020b; Lahmann, 2020, 113-220; Roguski, 2020b).

[17] Otros mecanismos de respuesta previstos por los Estados en sus DDIC son las retorsiones, así como también la legítima defensa.

[18] La posibilidad de adoptar contramedidas colectivas genera profundos desacuerdos incluso en el régimen general. Sobre este tema ver: (Gutiérrez Espada, 2002; Huesa Vinaixa, 2008).

posibilidad de que las medidas sean adoptadas por Estados que no se encuentran directamente lesionados por el hecho ilícito.

Finalmente, las DDIC señalan que frente a una ciberoperación las contramedidas no se encuentran limitadas solo al ámbito cibernético y, por lo tanto, también es posible adoptar contramedidas convencionales.

### II.1.2. El derecho internacional aplicable a las ciberoperaciones en tiempos de conflictos amados.

Conforme a los informes finales del GEG de 2013 y de 2015 el derecho internacional humanitario es aplicable a las conductas estatales que tienen lugar en el ciberespacio. Lo propio ha sido reafirmado por el informe final del GEG 2021. Esto implica que cuando una operación cibernética se da en el contexto de un conflicto armado (internacional o no internacional) queda regida por las normas propias del *ius in bello.*

Las DDIC en general, no realizan un examen exhaustivo de toda la normativa del derecho internacional humanitario, sino que se centran en examinar el alcance de los principios fundamentales de esta rama del derecho. Así, señalan que los principios de distinción, proporcionalidad y humanidad deben ser tenidos en cuenta a la hora de planificar y llevar adelante ciberoperaciones.

Además, algunas DDIC exploran cuándo existe un ataque armado en los términos del *ius in bello* (p. ej. Alemania y Francia). Así como también el alcance de las normas de neutralidad en el contexto cibernético (p. ej. Francia y Países Bajos).

## II.2. Alcance

¿Cuál es el alcance que tiene una DDIC? Es decir, ¿Cuál es el valor jurídico que puede asignarse a esta expresión estatal? Dar respuesta a estos interrogantes supone determinar si las DDIC constituyen documentos de carácter vinculante para quienes las emiten o bien si solo se trata de expresiones de carácter político y, por lo tanto, no vinculantes para sus autores.

Parte de la doctrina sostiene que se trata de documentos no vinculantes para los Estados (Johanson, 2021). En general los Estados no han manifestado una posición respecto de la obligatoriedad de las DDIC.

Los Estados tienden a señalar que las DDIC constituyen sus contribuciones al debate actual sobre la aplicabilidad del derecho internacional al ciberespacio (p. ej. Francia, Alemania). A través de ellas procuran explicitar qué normas internacionales son pertinentes para regular el comportamiento de los diferentes actores en el ciberespacio, así como también pretenden fijar el alcance que tienen estas reglas internacionales.

En este trabajo, y coincidiendo con otro sector de la doctrina (Roguski, 2020a, p. 2), se considera que las DDIC pueden llegar a tener cierto valor jurídico puesto que son relevantes para identificar la práctica estatal en la materia. En este sentido, las DDIC podrían constituir un mecanismo de identificación de la *opinio iuris* alrededor del modo en que las normas internacionales deben aplicarse en el ciberespacio; especialmente cuando existen los Estados expresan opiniones concordantes respecto de ciertas materias[19].

En apoyo de esta posición puede señalarse el segundo informe a la CDI sobre la identificación del derecho internacional consuetudinario (Wood, 2014). En dicho documento el relator especial Michael Wood indicó una serie de ejemplos sobre la forma en que pueden adoptar las expresiones de los Estados sobre la existencia (o inexistencia) de derechos u obligaciones de conformidad con el derecho internacional (Wood, 2014, para. 75 y ss). Muchas de las cuáles han sido utilizadas por los Estados para expresar su posición respecto del derecho internacional en el ciberespacio. Por ejemplo: Estados Unidos e Israel han optado por opiniones de

[19] Las DDIC también pueden ser consideradas como actos unilaterales, ya que a *prima facie* reunirían los elementos para ser consideradas como tal: a) ser una declaración pública de un Estado; b) que manifiesta la intención del Estado de quedar obligado por ella. La buena fe justificaría la obligación del Estado de cumplir con esta manifestación de voluntad. No obstante, no es tan sencillo otorgarle este carácter, ya que ni siquiera existe un acuerdo doctrinario en cuanto a la definición y el alcance de esta institución del derecho internacional (ver, por ejemplo: Saganek, 2016; Martínez Puñal, 2013; Eckart, 2012). Si bien esta discusión es interesante, excede el alcance de este trabajo por lo que no será abordada.

asesores jurídicos de los gobiernos; Alemania y Francia por publicaciones oficiales y Países Bajos por los memorandos internos de funcionarios del Estado.

Dado que explicitan las normas internacionales que los Estados entienden aplicables a sus actividades y a sus relaciones interestatales en el ciberespacio es razonable pensar que se trata de documentos vinculantes. Esto se debe a que el principio de buena fe, con el objetivo de garantizar la confianza en el sistema internacional, obliga a que los Estados respeten y se comprometan a cumplir sus declaraciones públicas (Reinhold, 2015, pp. 47-48).

### II.3. Ventajas y desventajas de una declaración sobre la aplicación del derecho internacional al ciberespacio

Algunos Estados pueden considerar que explicitar su posición respecto de esta materia es una desventaja ya sea porque no se encuentran en condiciones de hacerlo o bien porque consideran que es mejor no hacerlo. Un ejemplo de ello es la postura de la mayoría de los Estados Latinoamericanos que han señalado que no cuentan con las capacidades técnicas, legales y, a veces, las condiciones políticas necesarias para manifestar su posición en la materia (Hollis, 2020, pp. 7-8, para. 17-21).

Sin embargo, las ventajas de emitir una DDIC son indudables. Una DDIC constituye la forma que un Estado tiene de contribuir efectivamente al debate actual acerca de la aplicabilidad del derecho internacional al ciberespacio.

Tiene la función de explicitar la posición de ese Estado en la temática al explicar cuál es el alcance que tiene cierta norma internacional en relación con las operaciones cibernéticas. Consecuentemente permite identificar la práctica estatal en la materia y, eventualmente, la *opinio iuris* relevante vinculada con las operaciones cibernéticas.

Clarificar las normas internacionales en el ciberespacio es necesario para contribuir a la construcción de ámbito pacífico y seguro. Además, asegura que el debate y la definición de las normas internacionales se den entre todos los miembros de la comunidad internacional. Ello, a su vez, garantiza que exista una

pluralidad de voces y puntos de vista en el desarrollo progresivo del derecho internacional en el ámbito del ciberespacio.

## III. La posición argentina respecto de la aplicación del derecho internacional en el ciberespacio

La Argentina cuenta con un amplio marco normativo tendiente a regular distintos aspectos y actividades que tienen lugar en el ciberespacio. Ejemplo de ello son las leyes 25.326 sobre protección de datos personales; la 26.388 sobre delito informático y la 26.904 sobre *grooming*. Además, se han elaborado una serie de decretos y resoluciones ministeriales que también se ocupan del tema como por ejemplo la resolución SGM 829/2019 que adopta la Estrategia Nacional de Ciberseguridad de la República Argentina así como la resolución 1523/2019 que contiene la definición de las infraestructuras críticas de la información.

La ENC constituye un primer paso importante en materia de definir la posición y la acción del Estado en relación con el ciberespacio. Sin embargo, al mismo tiempo, se trata de un documento incompleto porque si bien señala varios de los problemas más relevantes que se están analizando en el contexto internacional (particularmente en el ámbito del GEG y el GTCA)[20] no explicita cuál es la postura de la Argentina frente a ellos.

Del mismo modo, a nivel internacional la República Argentina solo ha ido manifestando su posición en aspectos muy limitados y conforme a los tópicos que convocaban a las reuniones internacionales pertinentes. Lamentablemente, el Estado tampoco manifestó su posición durante el proceso llevado adelante por el CJI, ya que no respondió el cuestionario (ver Hollis, 2020) y la metodología de trabajo adoptada (Hollis, 2020, pp. 5-6, para. 11) impide conocer si el Estado intervino en las conversaciones informales propiciadas por dicho Comité.

[20] Entre estos tópicos la Argentina señala: cuestiones de atribución, soberanía, protección de los derechos humanos (particularmente en lo referido al derecho a la privacidad y a la protección de los datos personales), aplicación extraterritorial del derecho internacional de los derechos humanos y la posibilidad de utilizar las operaciones cibernéticas como armas.

Como resultado de ello, precisar cuál es la posición del Estado argentino respecto de la aplicabilidad del derecho internacional en el ciberespacio es una tarea compleja. No obstante, es posible realizar una sistematización de la incipiente postura estatal a partir de la revisión de su legislación interna, así como de su participación en los foros internacionales pertinentes.

El punto de partida de esta sistematización es la definición específica del ciberespacio que adoptó la Argentina, ya que esta noción permite identificar aquellos ámbitos que son susceptibles de ser regulados (Llorens, 2021). En este sentido, la Argentina define el ciberespacio como el "dominio global y dinámico compuesto por las infraestructuras de tecnología de la información, incluida Internet, las redes y los sistemas de información y de telecomunicaciones" (Argentina, 2019a, p. 2 y Argentina, 2017).

Esta conceptualización no es innovadora. Se alinea con la mayoría de las definiciones presentes en las estrategias de ciberseguridad de los Estados, así como la brindada por la literatura especializada[21]. Todas ellas entienden que el ciberespacio constituye un entramado de capas entrelazadas que se identifican con los distintos componentes del ciberespacio: la capa física (la infraestructura), la capa lógica (el *software*) y la capa social (los usuarios).

De la elección de la definición se desprende que el Estado entiende que el ciberespacio es un ámbito que requiere regulación. Se trata de un espacio de interés donde el Estado puede desarrollar sus competencias y donde tienen lugar diferentes actividades que el Estado puede (y debe) regular.

Para el Estado argentino, el derecho internacional, el derecho internacional de los derechos humanos, así como también el derecho internacional humanitario (Grupo de Trabajo de Composición Abierta, 2020) constituyen el marco normativo aplicable en el ciberespacio, especialmente en relación con las operaciones cibernéticas. Esto significa que para la Argentina las ciberoperaciones no se producen en un vacío normativo. Deben respetar ciertas normas internacionales

[21] Sobre este tema puede verse (Llorens, 2021) especialmente las obras y las definiciones allí citadas.

que regulan la conducta estatal tanto en tiempos de paz como cuando se producen conflictos armados (internacionales o no internacionales).

### III.1. El derecho internacional aplicable a las ciberoperaciones en tiempos de paz

#### III.1.1. Obligaciones de los Estados

*Soberanía:* La posición del Estado argentino respecto de la posibilidad o no de ejercer soberanía sobre el ciberespacio es un ejemplo de la falta de consenso existente en la comunidad internacional. La postura del Estado se caracteriza por no ser consistente. Por un lado, en la ECN señala:

> Este último concepto en particular [la soberanía], entendido como el ejercicio supremo del poder del Estado, está necesariamente vinculado a lo territorial. Sin embargo, Internet representa un dominio global intangible y un flujo infinito de datos sobre el cual no se ejerce dominio ni soberanía [énfasis agregado], poniendo a prueba el concepto antes mencionado e instaurando un nuevo paradigma que es necesario entender. (Argentina, 2019a, p. 3).

Por otro lado, la Argentina ha apoyado los informes del GEG de 2013 y de 2015 que reafirman que la soberanía constituye uno de los principios de derecho internacional aplicables en el ciberespacio (p. ej. Argentina, Misión Permanente de la República Argentina ante las Naciones Unidas, 2019, p. 5). A su vez, el Llamamiento de París al que ha adherido la Argentina[22] sostiene que las normas consuetudinarias (dentro de las que se encuentra la soberanía) son plenamente aplicables en este ámbito[23].

A pesar de las inconsistencias se puede considerar que la Argentina sí apoya la aplicabilidad de las normas de soberanía en el ciberespacio, ya que ello le brinda consistencia a la actuación del Estado en distintos foros y ámbitos: sostener que el derecho internacional es aplicable en el ciberespacio supone considerar que la

[22] El Estado se adhirió en el año 2018 (Argentina, 2019, p. 5).
[23] El texto completo del Llamamiento de Paris se puede consultar en: https://pariscall.international/en/call.

soberanía también es aplicable en este espacio. No obstante, el Estado debería precisar su visión en la materia.

*No intervención:* La Argentina no ha adoptado una postura explícita en relación con el principio de no intervención. No obstante, su apoyo a los informes finales de los GEG de 2013 y de 2015, así como al Llamamiento de París permite asumir que el Estado argentino considera que la no intervención resulta aplicable en el ciberespacio.

Estos documentos ponen de relieve que el principio de no intervención es una de las normas aplicables en este ámbito. Por ejemplo, el informe del GEG de 2015 señala que el principio de no intervención es uno de los principios que debe guiar la conducta de los Estados cuando utilicen las TIC (A. G. Res. 70/174, p. 16, para. 28 inc b), mientras que el Llamamiento de París indica que el derecho consuetudinario (donde se enmarca el principio de no intervención conforme lo señaló la CJI en el caso Nicaragua (1986, pp. 106-107, para. 202)) es aplicable en el ciberespacio (para. 3).

De todas maneras, la postura del Estado es incompleta. Ello se debe a que al no explicitar su posición no es posible identificar cuáles son las condiciones mínimas para que pueda ser aplicado.

*Debida diligencia:* En materia de debida diligencia la posición del Estado no es clara. Ha afirmado que no existe una obligación de debida diligencia en el ámbito de la ciberseguridad (Grupo de Trabajo de Composición Abierta, 2020). Pero en el mismo ámbito también ha sostenido que los Estados deben realizar "el mayor esfuerzo posible para evitar que su territorio sea utilizado por agentes no estatales para cometer actos internacionalmente ilícitos utilizando las TIC. Sin embargo, no es posible pretender que puedan garantizarlo". (A/74/120, p. 6)

Frente a estas expresiones se considera que el Estado considera que la obligación de debida diligencia puede llegar a aplicarse en el ciberespacio, aunque para ello entiende que es necesario que existan más consensos en la materia (Schmitt, 09 03 2021).

### III.1.2. Regimen del *ius ad bellum*

En cuanto al régimen del uso de la fuerza la Argentina no ha expresado de manera explícita cuál es su posición. No obstante, tanto los informes del GEG de 2013 y de 2015, así como el Llamamiento de París manifiestan que la Carta de las Naciones Unidas es aplicable en su totalidad al ciberespacio; posición que ha sido reafirmada por el Estado en el GTCA (Grupo de Trabajo de Composición Abierta, 2020).

Esto implica que el análisis sobre la licitud o no de una ciberoperación se realiza a la luz de las normas pertinentes de la Carta de las Naciones Unidas. Una operación cibernética puede constituir una violación al artículo 2, párrafo 4 de la CNU si afecta la integridad territorial, la independencia política o de cualquier modo es incompatible con los propósitos de la Carta de las Naciones Unidas. No obstante, la falta de precisión sobre la postura argentina impide conocer cuándo el Estado considera que una ciberoperación alcanza los umbrales necesarios para ser considerada como un uso de la fuerza en los términos del artículo 2 (4) de la CNU.

En materia de legítima defensa se aplican las mismas consideraciones: esta institución queda gobernada por las normas pertinentes de la Carta, es decir el artículo 51. Como resultado de ello, un Estado puede responder un ataque armado utilizando operaciones cibernéticas siempre que estas sean proporcionales, inmediatas y necesarias. La falta de posición explícita del Estado respecto de esta institución dificulta comprender cuándo una operación cibernética puede ser considerada como un ataque armado que dé lugar al derecho de legítima defensa.

Cabe destacar que para la Argentina el reconocimiento de la aplicabilidad de estas normas en el ciberespacio no implica una legitimación de la militarización en este ámbito (Grupo de Trabajo de Composición Abierta, 2020). Simplemente, reconoce que existen ciberoperaciones que pueden dar lugar a la aplicación del derecho internacional y, eventualmente, del derecho internacional humanitario.

### III.1.3. Responsabilidad internacional

*Atribución:* El Estado argentino no ha manifestado una posición específica sobre el modo en que debe atribuirse una operación cibernética a nivel técnico o legal, ya que considera que debe existir un enfoque común entre los Estados (Argentina, 2020; Grupo de Trabajo de Composición Abierta, 2020). Su apoyo a la resolución 73/27 de la Asamblea General de las Naciones Unidas solo indica que las atribuciones de ciberoperaciones deben ser fundadas; posición que ha sido reafirmada en las contribuciones escritas del Estado a la reunión bajo la fórmula Arria del Consejo de Seguridad de mayo de 2020 (Argentina, Misión Permanente de la República Argentina ante las Naciones Unidas, 2020). Por consiguiente, la cuestión de en qué casos debería hacerse la atribución continúa sin resolverse.

*Estado de necesidad:* La postura del Estado en esta materia no es explicita. Ni de los documentos internos ni de sus intervenciones en foros internacionales se puede extraer una posición al respecto.

*Medidas de respuesta:* El Estado no se ha expresado respecto de aquellas cuestiones vinculadas al modo en que los Estados pueden responder a operaciones cibernéticas maliciosas. Solo ha manifestado que los Estados pueden solicitar auxilio luego de haber detectado un acto malicioso y que debe tenerse presente que las respuestas pueden poner en peligro la paz y la seguridad internacional (Grupo de Trabajo de Composición Abierta, 2020). En consecuencia, brega por establecer un marco común con el objeto de facilitar la adopción de respuestas legales frente a ciberoperaciones maliciosas (Argentina, Misión Permanente de la República Argentina ante las Naciones Unidas, 2020, p. 2).

Partiendo de estas consideraciones se puede señalar que la adopción de retorsiones o contramedidas frente a operaciones cibernéticas es posible. Aunque no se definen cuáles son los criterios que deben tenerse en cuenta a la hora de adoptarlas.

## III. 2. El derecho internacional aplicable a las ciberoperaciones en conflictos armados

En materia de Derecho Internacional Humanitario, la Argentina considera que se trata de una rama del derecho plenamente aplicable al ciberespacio (Grupo de Trabajo de Composición Abierta, 2020). No obstante, no expresa ninguna posición respecto de normas particulares de este ordenamiento jurídico. Así, se puede entender que para la Argentina todas las normas y principios contenidas en el derecho internacional humanitario son aplicables, especialmente el principio de distinción, humanidad y proporcionalidad.

## IV. Una propuesta de declaración para la República Argentina

La Argentina ha demostrado interés por participar y, eventualmente, contribuir con los procesos de desarrollo progresivo de la normativa internacional vinculada con el ciberespacio. En este contexto, el Estado se beneficiaría con la adopción de una DDIC, ya que a través de ella sistematizaría y explicitaría su posición en la materia.

Como se ha señalado, la Asamblea General ha exhortado a los Estados a emitir documentos de posición sobre la aplicabilidad del derecho internacional en el ciberespacio. Con su adopción la Argentina podría contribuir efectivamente con el debate internacional, siendo esta otra de las razones que justifican la emisión de un documento de este tipo.

La DDIC debería adoptar la forma de un documento de posición, ya que de esta manera el Estado podría analizar de modo exhaustivo las implicancias que tienen las normas internacionales aplicadas en el ciberespacio. Un documento escrito, además, presenta la ventaja que permite controlar el alcance las expresiones utilizadas y brindarles un contexto específico.

Se considera que la DDIC tiene que abordar el alcance que se le da a las normas del derecho internacional general, así como el que se otorgue a las de los regímenes específicos como el derecho internacional humanitario. De esta forma, siguiendo el modelo de análisis propuesto en el presente trabajo se sugiere que la DDIC de la Argentina debería analizar, por un lado, las obligaciones internacionales, el régimen del *ius ad bellum* y la responsabilidad internacional de los Estados por operaciones

cibernéticas ilícitas; y, por el otro lado, las pautas fundamentales del derecho internacional humanitario. Tal vez, también sería interesante que la Argentina le dedicara un párrafo especial a las normas del derecho internacional de los derechos humanos, puesto que el Estado manifiesta que estos deben ser garantizados en el contexto cibernético.

La DDIC debería organizarse en tres o cuatro grandes bloques. El primero, un bloque de carácter introductorio, donde se explicite el objetivo de la DDIC. Además, en este primer apartado el Estado podría explicar las razones que lo llevan a adoptar la DDIC, así como analizar la normativa que considera aplicable. Este espacio también es el adecuado para hacer todas las salvedades que se consideren pertinentes a la hora de excluir o limitar la aplicación de la normativa internacional en el ciberespacio.

El segundo bloque de la DDIC se refiere a la aplicación del derecho internacional en tiempos de paz. Dado que el Estado promueve la solución pacífica de controversias en el ciberespacio (Argentina, 2019; Grupo de Trabajo de Composición Abierta, 2020, p. 1), el segundo apartado debe orientarse al examen de la normativa internacional que rige la mayor parte de las actividades que se desarrollan en el ciberespacio lo que, al mismo tiempo, resalta el carácter de excepción que tiene el derecho internacional humanitario.

Este bloque, por lo tanto, debería examinar aquellas normas que el Estado considera relevantes en el ámbito cibernético. Este análisis debería dar a conocer con claridad cuál es el alcance que se le asigna a cada norma internacional y cuáles son los criterios que se deben tener en cuenta a la hora de determinar si existió o no una violación al derecho internacional.

El contenido mínimo de esta sección debería incluir al menos un análisis de las obligaciones internacionales de los Estados, del régimen del *ius ad bellum* y de la responsabilidad internacional de los Estados. Teniendo en cuenta la posición de la Argentina respecto de estos temas, así como los desarrollos progresivos que están teniendo lugar en la comunidad internacional se sugiere que la DDIC argentina recepte los siguientes puntos.

1. *Obligaciones de los Estados*

a. *Soberanía*: Dado que el Estado argentino considera que la soberanía es aplicable en el contexto cibernético, la DDCI debería manifestar cuál es el alcance que se le otorga a esta norma internacional. Se entiende que la posición que adopte la DDIC debería ser la de la soberanía como regla, es decir la soberanía es una norma de derecho internacional que puede ser violada en sí misma. Adoptar esta posición requiere, además, explicar cuándo y bajo qué condiciones una ciberoperación puede afectar la soberanía de un Estado. Así, se sugiere que la DDCI adopte el enfoque de la penetración, puesto que es el que más se adecúa a las reglas de responsabilidad internacional vigentes en la comunidad internacional.
b. *No Intervención*: Ya que es posible asumir que la Argentina entiende que el principio de no intervención es aplicable al ciberespacio es preciso que la DDIC examine cuáles son las condiciones necesarias para que se configure una intervención en los asuntos internos del Estado. En este caso, se considera que se deberían seguir las pautas establecidas por el derecho internacional y que han sido desarrolladas por la Corte Internacional de Justicia en el caso Nicaragua: cierto grado de coerción sobre el accionar del Estado (comisivo u omisivo) en materias que forman parte de su dominio reservado.
c. *Debida diligencia*: En este punto la posición argentina debe ser esclarecida. La obligación de debida diligencia constituye la contracara de la soberanía y como tal le exige al Estado que proteja dentro de su territorio los derechos de otros Estados (*Asunto del Canal de Corfú (Albania vs. Gran Bretaña),* 1949, p. 22). Esto implica que los Estados deben realizar los esfuerzos necesarios para evitar que su territorio sea utilizado para afectar los derechos de otros Estados. En consecuencia, si el Estado considera que en el ciberespacio son aplicables las reglas de soberanía debe reconocer la existencia de la debida diligencia como uno de los criterios que regulan las conductas de los Estados; en este punto se debería precisar cuál es el alcance que se le debe dar a este estándar conforme a las capacidades técnicas del Estado.

2. *Régimen del* ius ad bellum

En relación con el régimen del uso de la fuerza la DDCI cumpliría la función de explicitar la posición del Estado que se ha delineado en varios de los instrumentos que ha apoyado. El principio de prohibición de la amenaza y el uso de la fuerza es aplicable en el ciberespacio. Consecuentemente, la legítima defensa como excepción a esta prohibición también resulta de aplicación a las operaciones cibernéticas.

La DDIC debería indicar cuáles son los criterios que deben tenerse en cuenta a la hora de determinar el umbral en el que una ciberoperación viola la prohibición de la amenaza y el uso de la fuerza. En este sentido, se entiende que el criterio de la escala y los efectos es el criterio indicado para distinguir cuando una operación cibernética constituye un uso de la fuerza.

Asimismo, sería necesario analizar en qué casos puede acudirse al derecho de legítima defensa. En primer lugar, debería indicarse que las operaciones cibernéticas pueden ser utilizadas como un mecanismo de defensa independientemente de que el ataque haya sido llevado adelante por medios convencionales (cinéticos) o por medios cibernéticos. En segundo lugar, sería preciso examinar cuándo se reúnen las condiciones necesarias para que una operación cibernética pueda ser considerada como un ataque armado que dé lugar al derecho de legítima defensa. Para lo cual sería útil que se utilizase el criterio de la escala y los efectos: una operación cibernética cuya escala y efectos (muerte, destrucción) sean comparables a los de una operación convencional que se califique como un ataque armado será considerado como tal. En tercer lugar, el Estado debería examinar la posibilidad o no de que la legítima defensa frente a ataques cibernéticos pueda ser utilizada de forma anticipada; y, al mismo tiempo, señalar que la legítima defensa preventiva no es posible.

3. *Responsabilidad internacional*

La declaración argentina debería enfatizar que la cuestión de la responsabilidad internacional se rige por las reglas generales recogidas en el

proyecto de artículos de la CDI de 2001. Esta elección se justifica porque refleja las normas consuetudinarias en la materia.

*Atribución*: Debido a la posición de la Argentina en materia de atribución, la DDCI debería abordar diversos aspectos. En primer lugar, distinguir entre los tipos de atribución: técnica, política y legal; así como manifestar cuándo procede cada tipo; aunque señalando que cuando se realice la atribución legal esta debe ser fundada. En segundo lugar, y vinculado con lo anterior, precisar los criterios de atribución (legal) de las operaciones cibernéticas a los Estados; para ello se considera que se debería hacer referencia a los criterios de atribución previstos en el proyecto de artículos de 2001. Finalmente, la DDIC debe señalar que la decisión de atribuir es una decisión de carácter político, lo que permitiría cierto margen de acción frente a operaciones cibernéticas maliciosas.

*Medidas de respuesta*: En este aspecto la DDIC debería abordar específicamente las medidas que el Estado puede utilizar para responder las operaciones cibernéticas maliciosas: retorsiones y contramedidas. Las primeras pueden o no ser abordadas por la DDIC, ya que se trata de medidas lícitas que el Estado puede adoptar frente a una operación cibernética estatal. Las contramedidas, en cambio, requieren un análisis más exhaustivo, puesto que en su origen son actos cuya ilicitud se excluye porque procuran el cumplimiento de la obligación violada por parte del otro Estado. La declaración, por lo tanto, debería referirse a las reglas generales delineadas en el proyecto de artículos de 2001. Siendo especialmente relevante señalar si la notificación previa constituye un requisito para poder hacer uso de las contramedidas; dependiendo esta decisión de las capacidades técnicas del Estado. Asimismo, sería importante que el Estado se expidiera acerca de la posibilidad o no de utilizar contramedidas colectivas.

El tercer bloque, aunque no es indispensable, se considera que sería un aporte original y relevante de la Argentina. Este apartado debería contener un examen de las normas de derechos humanos que el Estado considera imprescindibles para garantizar que el ciberespacio sea un ámbito seguro y pacífico.

Finalmente, el cuarto bloque, se encuentra dedicado al examen de las normas del *ius in bello*. En este apartado el Estado debería señalar el alcance que considera que estas normas tienen en caso de que las operaciones cibernéticas se den en el contexto de un conflicto armado (internacional o no internacional). Este, conforme al último informe del GEG 2021, constituye el único ámbito de aplicación de esta normativa (pp. 13-14 para. 71 g)).

Conforme a los criterios explicitados se debe realizar un examen exhaustivo de los principios de distinción, proporcionalidad, necesidad y humanidad. En particular, el Estado debe dar a conocer con qué alcance y cómo se implementarán estas normas por parte de sus fuerzas armadas.

## V. Conclusiones

La República Argentina necesita una declaración sobre la aplicabilidad del derecho internacional al ciberespacio. El momento no puede ser más oportuno. Los debates que están teniendo lugar en la comunidad internacional son propicios y hacen necesario que el Estado argentino manifieste su postura en relación a cómo entiende que las normas internacionales se aplican en el ciberespacio.

Por lo tanto, una DDIC constituye un mecanismo adecuado para contribuir de manera constructiva y efectiva a este debate. Al mismo tiempo permite que el Estado delinee y exprese su parecer en esta materia, ya que posibilita precisar la posición del Estado respecto de la aplicabilidad y el alcance de la normativa internacional en el ciberespacio.

Para que resulte útil es necesario que la DDIC examine la mayor cantidad de aspectos posibles en la materia. A estos efectos, se considera que debería adoptar la forma de un documento de posición porque al tratarse de un documento escrito se puede controlar de una manera más efectiva el alcance que se le asigne a cada una de las normas internacionales que aborde. Esto es especialmente relevante si se tiene en cuenta que las DDIC constituyen documentos vinculantes para los Estados que las emiten y que, potencialmente, tienen la capacidad de identificar la *opinio iuris* en la materia.

En este trabajo se considera que la DDIC debería abordar un contenido mínimo que se refiera a las normas que se aplican a las operaciones cibernéticas que tienen lugar durante tiempos de paz y a aquellas que se aplican a las ciberoperaciones que se dan en el contexto de un conflicto armado (internacional o no internacional). Las primeras se refieren a las obligaciones internacionales (soberanía, no intervención y debida diligencia); el régimen del *ius ad bellum* (prohibición de la amenaza y el uso de la fuerza y legítima defensa) y a la responsabilidad internacional (atribución y medidas de respuesta). Las segundas, en tanto, se vinculan con la aplicabilidad del derecho internacional humanitario. Finalmente, se considera que sería importante incluir una sección que se refiera al derecho internacional de los derechos humanos donde se examinen los derechos fundamentales que deben ser garantizados en este ámbito, así como también el alcance que debería otorgárseles.

Esta expresión de la posición estatal es relevante por varios motivos. En primer lugar, obliga a que el Estado sistematice su entendimiento de la normativa internacional aplicable; lo que, a su vez, impide que el Estado adopte posiciones inconsistentes en los distintos foros en los que participa. En segundo lugar, ayuda al desarrollo progresivo del derecho internacional, ya que la emisión de DDIC constituye un mecanismo para la identificación de la práctica estatal y, eventualmente, de la *opinio iuris* en el ciberespacio. En tercer lugar, al sistematizar y dar a conocer la posición del Estado en la materia facilita la tarea del cuerpo diplomático, debido a que le brinda las herramientas necesarias para enfrentarse a los nuevos desafíos de la comunidad internacional. Además, establece un marco normativo preciso para todos los actores que participan en el ciberespacio. En cuarto lugar, la elaboración de la DDIC brinda la oportunidad para la colaboración entre la academia, el Estados y los demás actores implicados en el ciberespacio. Ello, a su vez, permite que cada uno pueda realizar los aportes que crean convenientes. En suma, una DDIC lleva a la práctica el compromiso estatal de construir un ciberespacio pacífico y seguro.

## Bibliografía[24]

### Libros y artículos

ARITMASU, Louise y SCHMITT, Michael N. (2021). "The Plea of Necessity: An Oft Overlooked Response Option to Hostile Cyber Operations", *International Law Studies. 97*. 1171-1199.

AKANDE, Dapo; COCO, Antonio; DE SOUZA DIAS, Talita; HOLLIS, Duncan B.; O'BRIEN, James y VAN BENTHEM, Tseveletina. (02 06 2021). "The Oxford Statement on International Law Protections in Cyberspace: The Regulation of Information Operations and Activities", *EJIL:Talk!* Disponible en https://www.ejiltalk.org/the-oxford-statement-on-international-law-protections-in-cyberspace-the-regulation-of-information-operations-and-activities/

BANNELIERE-CHRISTAKIS, Karine. (2015). "Is the principle of distinction relevent in cyberwarefare?", en TSAGOURIAS, Nicholas y BUCHAN, Rusell (ed.), *Research Handbook of International Law and Cyberspace*. Gloucestershire: Edward Eldgar Publishing.

BANKS, William. (2019). "State Responsibility and Attribution of Cyber Intrusions After Tallinn 2.0", *Texas Law Review, 95* (7), 1487-1513.

CORN, Gary P. y TAYLOR, Robert. (2017). Sovereignty in the Age of Cyber. *AJIL Unbound, 111*, 207-212.

DELERUE, François. (2019). "Attribution to State of Cyber Operations Conducted by Non-State Actors", en CARPANELLI, Elena y LAZZERINI, Nicole (eds.). *Use and Misuse of New Technologies*: *Contemporary Challenges under International and European Law*. Berlin: Springer.

DELERUE, François. (2020). *Cyber Operations and International Law*. Cambridge: Cambridge University Press.

ECKART, Christian. (2012). *Promises of States under International Law*. Oxford: Hart Publishing.

[24] Todos los enlaces fueron verificados el 30 de junio de 2021.

EICHENSEHR, Kristen. I. (2014). "The Cyber-Law of Nations", *The Georgetown Law Journal, 103*, 317-380.

FANG, Bixing. (2018). *Cyberspace Sovereignty. Reflections on Building a Community of Common Future in Cyberspace.* Beijing: Springer.

FINLAY, Lorraine y PAYNE, Christian (2019). "The Attribution Problem and Cyber Armed Attacks", *AJIL Unbound, 113*, 202-206.

FITZMAURICE, Malgosia (2017). "Legitimacy of International Environmental Law. The Sovereign States Overwhelmed by Obligations: Responsibility to React to Problems Beyond National Jurisdiction?", *Zeitschrift für ausländisches öffentliches Recht und Völkerrecht, 77*, 339-370.

GUTIÉRREZ ESPADA, Cesáreo (2002). "Las Contramedidas de Estados ´´erceros´´ por Violación a Ciertas Obligaciones Internacionales, *Anuario Argentino de Derecho Internacional, XI* (2000-2001), 15-49.

HOLLIS, Duncan B. (27 07 2016) 'Russia and the DNC Hack: What Future for a Duty of Non-intervention?, *Opinio Juris*. Disponible en https://opiniojuris.org/2016/07/25/russia-and-the-dnc-hack-a-violation-of-the-duty-of-non-intervention/

HUESA VINAIXA, Rosario (2008). "Auge y Declive de las ´Contramedidas Colectivas´ en la Construcción de un Sistema de Responsabilidad Internacional, en HUESA VINAIXA, Rosario (ed.), *Derechos humanos, responsabilidad internacional y seguridad colectiva. Intersección de sistemas. Estudios en homenaje al profesor Eloy Ruiloba Santana*. Madrid: Marcial Pons

JENSEN, Eric T., y WATTS, Sean (2017). "A Cyber Duty of Due Diligence: Gentle Civilizer or Crude Destabilizer?", *Texas Law Review, 95* (7), 1555-1577.

JOHANSON, Sarah. (2021). "Definitional doom: How Iran and Israel derail legal application in cyberspace". Disponible en https://www.mei.edu/publications/definitional-doom-how-iran-and-israel-derail-legal-application-cyberspace.

KOLB, Robert (2015). "Reflections on Due Diligence Duties and Cyberspace", *German Yearbook of International Law Studies, 58*, 113-128.

KOSSEFF, Jeff (2020a). "Collective Countermeasures in Cyberspace", *Notre Dame Journal of International & Comparative Law, 10,* 18-34.

KOSSEFF, Jeff. (2020b), "Retorsion as a Response to Ongoing Malign Cyber Operations" en JANČÁRKOVÁ; LINDSTRÖM; SIGNORETTI; TOLGA y VISKY (eds.), *2020 12th International Conference on Cyber Conflict. 20/20 Vision: The Next Decade*. NATO CCDCOE Publications.

LAHMANN, Henning (2020). *Unilateral Remedies to Cyber Operations: Self-Defence, Countermeasures, Necessity, and the Question of Attribution*. Cambridge: Cambridge University Press.

LLORENS, María Pilar (2021). "Ciberespacio y Derecho Internacional", *Anuario del Centro de Investigaciones Jurídicas y Sociales, 19,* 383-402.

MAČÁK, Kubo (2016). "Decoding Article 8 of International Law Commission's Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors", *Journal of Conflict and Security Law*, *21* (3), 405-428.

MARTÍNEZ PUÑAL, Antonio (2013). *Actos Unilaterales, Promesa, Silencio y Nomegénesis en el Derecho Internacional (2º reimpresión)*. Santiago de Compostela: Andavira.

MOYNIHAN, Harriet (2019). "The Application of International Law to State Cyberattacks. Sovereignty and Non-Intervention", *Research Paper, Chatham House, The Royal Institute of International Affairs*.

REINHOLD, Stephen (2015). "Good Faith in International Law", *UCL Journal of Law and Jurisprudence, 2*, 40-63.

REMIRO BROTÓNS, Antonio; RIQUELME CORTADO, Rosa M.; DÍEZ-HOCHLEITNER, RODRÍGUEZ Javier; ORIHUELA CALATAYUD, Esperanza y PÉREZ-PRAT DURBÁN, Luis (2010). *Derecho Internacional. Curso General*. Valencia: Tirant Lo Blanch.

REMIRO BROTÓNS, Antonio; RIQUELME CORTADO, Rosa M.; DÍEZ-HOCHLEITNER RODRÍGUEZ, Javier; ORIHUELA CALATAYUD, Esperanza y PÉREZ-PRAT DURBÁN, Luis (2007). *Derecho Internacional* , 2º ed. Valencia: Tirant Lo Blanch.

ROSCINI, Marco. (2014) *Cyber Operations and the Use of Force in International Law*. Oxford: Oxford University Press.

ROGUSKI, Przemysław (2020a). Application of International Law to Cyber Operations: A Comparative Analysis of States' Views, *The Hague Program for Cyber Norms Policy Brief. March 2020*.

ROGUSKI, Przemysław (2020b). "Collective Countermeasures in Cyberspace – *Lex Lata*, Progressive Development or a Bad Idea?", en JANČÁRKOVÁ; LINDSTRÖM; SIGNORETTI; TOLGA y VISKY (eds.), *2020 12th International Conference on Cyber Conflict. 20/20 Vision: The Next Decade*. NATO CCDCOE Publications.

SHACKELFORD, Scott. J., RUSSELL, Scott, y KUEHN, Andreas. (2015). *Defining Cybersecurity Due Diligence Under International Law: Lessons from the Private Sector Kelley School of Business Research Paper.* Indiana: Kelley School of Business.

SCHMITT, Michael N. (2021). *Germany's Positions on International Law in Cyberspace*, Part I. Disponible en https://www.justsecurity.org/75242/germanys-positions-on-international-law-in-cyberspace/

SCHMITT, Michael N. (10 06 2021). The Sixth United Nations GGE and International Law in Cyberspace. *Just Security.* Disponible en https://www.justsecurity.org/76864/the-sixth-united-nations-gge-and-international-law-in-cyberspace/

SCHMITT, Michael N. (1999). Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework. *Columbia Journal of Transnational Law, 37* (2), 885-937.

SCHMITT, Michael N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge Universtity Press.

SCHMITT, Michael N. (2015). In Defense of Due Diligence in Cyberspace. *The Yale Law Journal Forum, 125*, 68-81.

SCHMITT, Michael N. (2017). *Tallinn Manual 2.0 on International Law Applicable to Cyber Operations* . Cambridge: Cambridge University Press.

SCHMITT, Michael N. y Vihul, Liis. (2017). Respect for Sovereignty in Cyberspace. *Texas Law Review*, 95 (7), 1639-167.

SAGANEK, Przemysław. (2016). *Unilateral Acts of States in Public International Law.* Leiden: Brill-Nihoff.

STEPHENS, Tim, y FRENCH, Duncan. (2016). *ILA Study Group on Due Diligence in International Law. Second Report.*

TSAGOURIAS, Nicholas y BUCHAN, Russell. (2015). *Research Handbook on International Law and Cyberspace.* Cheltenham: Edward Elgar Publishing.

## Documentos

ALEMANIA, THE FEDERAL GOVERNMENT (2021). "On the Application of International Law in Cyberspace *Position Paper"*. Disponible en Disponible en https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf

ARGENTINA (2017). "Creación del Comité de Ciberseguridad". Decreto 577/2017.

ARGENTINA (2019a) "Estrategia Nacional de Ciberseguridad". Jefatura del Gabinete de Ministros. Resolución 829/2019.

ARGENTINA (2019b). "Jefatura del Gabinete de Ministros. Resolución 1523/2019.

ARGENTINA (2020). "Initial ´Pre-draft´ of the report of the OEWG on developments in the field of information and telecommunications in the context of international security". Comentarios ARGENTINA. Disponible en https://front.un-arm.org/wp-content/uploads/2020/04/oewg-ict-comentarios-argentina-2.pdf

ARGENTINA, MISIÓN PERMANENTE DE LA REPÚBLICA ARGENTINA ANTE LAS NACIONES UNIDAS (2019). "Evaluación general de los temas relacionados con la seguridad de la información". Disponible en https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/09/Argentina-2019.pdf

ARGENTINA, MISIÓN PERMANENTE DE LA REPÚBLICA ARGENTINA ANTE LAS NACIONES UNIDAS (2020). "Arria Formula – UN Security Council. Cyber Stability, Conflict Prevention and Capacity Building". New York, 22 May 2020. Permanent Mission of Argentina - Written contribution. Disponible en https://vm.ee/sites/default/files/Estonia_for_UN/formula_arria_csun_-_ciberseguridad_y_capacitacion_-_intervencion_escrita_argentina.pdf

ASAMBLEA GENERAL DE LAS NACIONES UNIDAS, Documento A/68/98, Informe del Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional (23 de junio de 2013).

ASAMBLEA GENERAL DE LAS NACIONES UNIDAS, Documento A/70/174, Informe final del Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional (22 de julio de 2015).

ASAMBLEA GENERAL DE LAS NACIONES UNIDAS, Documento A/76/135, Informe del Grupo de Expertos Gubernamentales sobre la Promoción del Comportamiento Responsable de los Estados en el Ciberespacio en el Contexto de la Seguridad Internacional (14 de julio de 2021).

ASAMBLEA GENERAL DE LAS NACIONES UNIDAS, Documento A/76/136, Compendio oficial de las contribuciones nacionales voluntarias sobre la cuestión de cómo se aplica el derecho internacional al uso de las tecnologías de la información y las comunicaciones por los Estados, presentadas por los expertos gubernamentales participantes en el Grupo de Expertos Gubernamentales sobre la Promoción del Comportamiento Responsable de los Estados en el Ciberespacio en el Contexto de la Seguridad Internacional, establecido en virtud de la resolución 73/266 de la Asamblea General (13 de julio de 2021).

ASAMBLEA GENERAL, Resolución 73/266, Promoción del comportamiento responsable de los Estados en el ciberespacio en el contexto de la seguridad internaciona (22 de diciembre de 2018)

AUSTRALIA, DEPARTMENT OF FOREIGN AFFAIRS AND TRADE (2021). Australia's International Cyber and Critical Technology Engagement Strategy. Disponible en https://www.internationalcybertech.gov.au/sites/default/files/2021-05/21066%20DFAT%20Cyber%20Affairs%20Strategy%202021%20update%20Internals%201%20Acc.pdf

EGAN, BRIAN J., LEGAL ADVISOR (2016, 10 Noviembre 2016). "Remarks on International Law and Stability in Cyberspace". Disponible en https://2009-2017.state.gov/s/l/releases/remarks/264303.htm

FINLANDIA, MINISTRY OF FOREIGN AFFAIRS (2020). "International Law and Cyberspace. Finland's Nationals Positions". Disponible en https://valtioneuvosto.fi/en/-/finland-published-its-positions-on-public-international-law-in-cyberspace

FRANCIA, MINISTÈRE DES ARMÉES (2019). "International Law Applied to Operations in Cyberspace". Disponible en https://www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+operations+in+cyberspace.pdf

GRUPO DE TRABAJO DE COMPOSICIÓN ABIERTA (2020) (02:15:00-02:17:33). Intervención argentina: Second substantive session (10–14 February 2020). Disponible en: https://media.un.org/en/asset/k18/k18w6jq6eg

KOH, HAROLD H., LEGAL ADVISOR U.S. DEPARMENT OF STATE (2012, 18 Septiembre 2012). "International Law and Cyberspace". Disponible en https://2009-2017.state.gov/s/l/releases/remarks/197924.htm

HOLLIS, Duncan B. (RELATOR ESPECIAL) (2020). "Derecho Internacional y Operaciones Cibernéticas del Estado: Mejora de la Transparencia - Quinto Informe" (CJI/doc. 615/20 rev. 1).

IRÁN, GENERAL STAFF OF THE ARMED FORCES (2020). "Declaration of General Staff of the Armed Forces of the Islamic Republic of Iran Regarding International Law Applicable to the Cyberspace". Disponible en https://www.aldiplomasy.com/en/?p=20901

KALJULAID, KERSTI, PRESIDENTE DE ESTONIA (2019, 29 Mayo 2019). "President of the Republic at the opening of CyCon 2019". Disponible en https://www.president.ee/en/official-duties/speeches/15241-president-of-the-republic-at-the-opening-of-cycon-2019/index.html

NUEVA ZELANDIA, FOREIGN AFFAIRS & TRADE (2020). "The Application of International Law to State Activity in Cyberspace". Disponible en https://dpmc.govt.nz/publications/application-international-law-state-activity-cyberspace

PAÍSES BAJOS, MINISTRY OF FOREIGN AFFAIRS (2019, 5 Julio 2019). "Letter to the Parliament on the International Legal Order in Cyberspace". Disponible en https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace

SCHÖNFORD, Roy (2021). "Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations", *International Law Studies, 97*, 395-406.

SUIZA, FEDERAL DEPARTMENT OF FOREIGN AFFAIRS, DIRECTORATE OF INTERNATIONAL LAW. (2021). "Switzerland's Position Paper on the Application of International Law in Cyberspace Annex", UN GGE 2019/2021. Disponible en https://www.eda.admin.ch/dam/eda/en/documents/aussenpolitik/voelkerrecht/20210527-Schweiz-Annex-UN-GGE-Cybersecurity-2019-2021_EN.pdf

WOOD, Michael (Relator Especial). (2014). "Segundo Informe sobre la Identificación del Derecho Internacional Consuetudinario", UN Doc A/CN.4/672.

WRIGHT, Jeremy QC MP, Attorney General. (2018, 23 Mayo 2018). "Cyber and International Law in the 21st Century". Disponible en https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century

**Jurisprudencia**

CORFU CHANNEL CASE (U.K. v. Alb.), Merits, 1949 I.C.J. Rep. 4 (April 9).

MILITARY AND PARAMILITARY ACTIVITIES IN AND AGAINST NICARAGUA (Nicar. v. U.S.), Merits, 1986 I.C.J. Rep. 14 (June, 27).