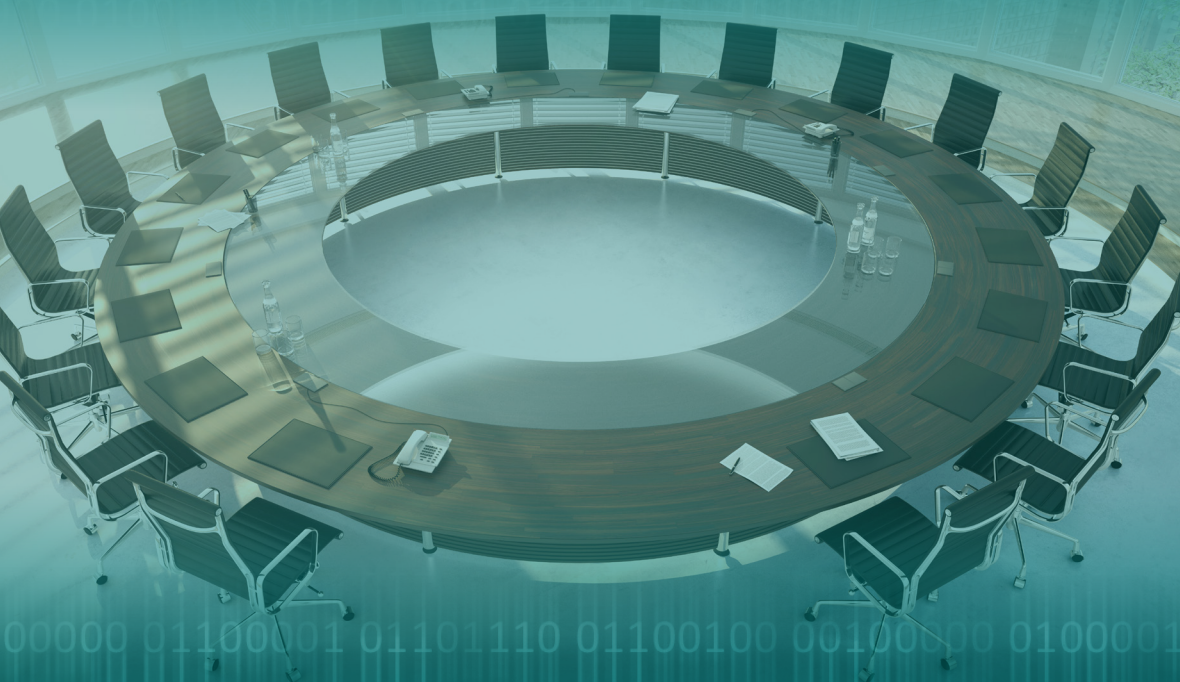
Manual para el desarrollo de una posición nacional sobre el derecho internacional y las actividades cibernéticas

Una guía práctica para los Estados



Kubo Mačák, Talita Dias y Ágnes Kasper

Republic of Estonia
Ministry of Foreign Affairs

MOFA
Ministry of Foreign Affairs of JAPAN

CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

University of Exeter

Primera publicación en 2025. Traducción al español en 2026.

Este manual fue desarrollado en colaboración con el Ministerio de Asuntos Exteriores de Estonia, el Ministerio de Asuntos Exteriores de Japón, el Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN y la Universidad de Exeter.

Esta obra fue apoyada por una Subvención de la Cuenta de Aceleración de Impacto del Concejo de Investigación Económica y Social (número de subvención: ES/X004198/1; referencia de la asignación: ESRC/015).

Diseño y diagramación por el Estudio de diseño multimedia de la Universidad de Exeter.

Citación sugerida: Kubo Mačák, Talita Dias y Ágnes Kasper, *Manual para el desarrollo de una posición nacional sobre el derecho internacional y las actividades cibernéticas: Una guía práctica para los Estados (2025)*

Impreso: ISBN 978-9916-9227-0-5 PDF: ISBN 978-9916-9227-1-2 (pdf)

CONTENIDO

RECONOCIMIENTOS

Este proyecto fue posible gracias al generoso apoyo de la Cuenta de Aceleración de Impacto del Concejo de Investigación Económica y Social (ESRC IAA) del Reino Unido, cuyo financiamiento permitió el desarrollo y producción de este manual. Agradecemos profundamente su contribución.

También queremos extender nuestro más sincero agradecimiento a nuestros socios institucionales, el Ministerio de Asuntos Exteriores de Estonia, el Ministerio de Asuntos Exteriores de Japón, el Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN (CCDCOE, por sus siglas en inglés) y la Universidad de Exeter, por su inquebrantable apoyo y colaboración durante este proyecto.

Agradecemos particularmente a Sra. Karine Veersalu del Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN, quien se desempeñó como directora del proyecto y cuyas habilidades organizativas, constante determinación y actitud positiva permitieron el funcionamiento sin problemas del proyecto en todo momento.

También estamos agradecidos con el personal de todos nuestros aliados institucionales que siempre proporcionaron apoyo fundamental y cuyas dedicación y experticia fueron vitales para la ejecución exitosa de este proyecto. En particular, queremos a agradecer a la Dra. Anna-Maria Osula y la Sra. Liisa Sulavee del Ministerio de Asuntos Exteriores de Estonia; al Sr. Yukiya Hamamoto, al Sr. Munehito Nakatani, al Sr. Kimihiko Okano, al Sr. Satoru Onoda y al Sr. Kentaro Tahara del Ministerio de Asuntos Exteriores de Japón; la Sra. Hedi Jüriöö del Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN; a la Sra. Danielle Payne y el Dr. James Woodhams de la Universidad de Exeter; al igual que a la Sra. Anne Blickhan y al Sr. Yaroslav Halieiev que en ese momento eran académicos visitantes en el Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN.

Damos gracias especiales a nuestro Consejo Asesor, cuya orientación ayudó a dar forma a la dirección del proyecto desde sus inicios y cuya revisión de pares del borrador del manual fue fundamental para su forma final. Reconocemos con agradecimiento a todos los miembros del Consejo Asesor: Kerry-Ann Barrett, Dra. Cordula Droege, profesor Mohamed Helal, profesor Zhixiong Huang, Dr. Giacomo Persi Paoli, profesor Marco Roscini, profesora Johanna Weaver y la Sra. Danielle Yeow.

Agradecemos inmensamente a los representantes de los 46 Estados que participaron en las tres mesas redondas regionales. Su participación comprometida y apertura al diálogo dieron forma al contenido y enfoque del manual de manera significativa. Estamos igual de agradecidos con los asesores expertos que enriquecieron los debates en cada mesa redonda, incluyendo a la Sra. Kristel-Amelie Aimre, la profesora Mariana Salazar Albornoz, el Sr. Benjamin Ang, la Sra. Larissa Schneider Calza, el Sr. Samit D'Cunha, el Sr. Yukiya Hamamoto, el profesor Mamadou Hébié, el

profesor Mohamed Helal, el profesor Zhixiong Huang, la profesora Nnenna Ifeanyi-Ajufo, la Dra. So Jeong Kim, la Sra. Eddah Mogaka, la Sra. Harriet Moynihan, la Dra. Anna-Maria Osula, la Sra. Kimberley Raleigh, el Sr. Marcus Song, la Sra. Liis Vihul, la Sra. Danielle Yeow y el Sr. Robert Young. También reconocemos a quienes abordaron las mesas redondas formalmente en nombre de instituciones asociadas, reflejando su valioso apoyo al proyecto, entre quienes se encuentra el profesor Hajer Gueldich, Su excelencia, el Sr. Jens Hanefeld, la Sra. Irina Höhn, el profesor Mart Noorma, la Sra. Eleliis Rattam, Su excelencia el Sr. Tanel Sepp y Su excelencia el Sr. Priit Turk.

También queremos reconocer a las muchas personas e instituciones que apoyaron la organización de cada mesa redonda.

Para la mesa redonda sobre perspectivas de Latinoamérica y el Caribe, llevada a cabo en Washington, DC, agradecemos a la Organización de Estados Americanos por su alianza y asistencia, en particular al Sr. Kerry-Ann Barrett y el Sr. David Moreno, así como a Sra. Maria Tolppa del Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN por la toma de notas.

Para la mesa redonda de Asia y el Pacífico, llevada a cabo en Singapur, agradecemos al Centro para el Derecho Internacional de la Universidad Nacional de Singapur, especialmente a la Sra. Danielle Yeow, la Sra. Ying Li Loh y la Sra. Geraldine Ng, así como a el Sr. Aayush Mallik de la Universidad Nacional de Singapur y a la Sra. Hanyu Zhang de la Universidad de Wuhan por la toma de notas.

Para la mesa redonda de los países miembros de la Unión Africana, llevada a cabo en Addis Ababa, extendemos nuestros agradecimientos a la Unión Africana, en particular al asesor jurídico, el profesor Hajer Gueldich y al personal de la oficina del asesor legal, incluyendo al Sr. Francis Adanlao, a la Sra. Meseret Assefa, al Sr. Mitchel Mauyakufa y al Sr. Taona Mwanyisa. También agradecemos al Ministerio Federal de Asuntos Exteriores de Alemania y a la Agencia Alemana de Cooperación Internacional (Deutsche Gesellschaft für Internationale Zusammenarbeit, GIZ) por su apoyo a la mesa redonda, especialmente a Sofia Klumpp y Juliane Kolsdorf.

Reconocemos agradecidos el apoyo a las tres mesas redondas proporcionado por la Universidad Tecnológica de Tallin, mediante la Subvención de Investigación para Jóvenes Científicos.

Por último, agradecemos al Dr. Nicolas Bouchet por su cuidadosa revisión del texto, a Roy Chacón Gómez por su trabajo de traducción al español, a Dominique Steinbrecher por su atenta revisión de la traducción, y al Estudio de Diseño de la Universidad de Exeter por su trabajo creativo y profesional para el desarrollo y producción de este manual.

Kubo Mačák, Talita Dias, y Ágnes Kasper,
mayo de 2025

LISTA DE ABREVIATURAS

ACHPR	Carta Africana de Derechos Humanos y de los Pueblos
ACNUDH	Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos
AGNU	Asamblea General de las Naciones Unidas
ARSIWA	Artículos sobre la responsabilidad del Estado por hechos internacionalmente ilícitos
ASEAN	Asociación de Naciones del Sudeste Asiático
CADH	Convención Americana sobre Derechos Humanos
CDH	Comité de Derechos Humanos
CDI	Comisión de Derecho Internacional
CEDH	Convención Europea de Derechos Humanos
CERT	Equipo de Respuesta ante Emergencias Informáticas
CICR	Comité Internacional de la Cruz Roja
CIJ	Corte Internacional de Justicia
Corte IDH	Corte Interamericana de Derechos Humanos
CPA	Corte Permanente de Arbitraje
CPI	Corte Penal Internacional
DIDH	Derecho Internacional de los Derechos Humanos
DIH	Derecho internacional humanitario
DPI	Derecho penal internacional
EE. UU.	Estados Unidos
GEG	Grupo de Expertos Gubernamentales de las Naciones Unidas sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional
GTCA	Grupo de Trabajo de Composición Abierta
IP	Protocolo de Internet
OEA	Organización de los Estados Americanos

ONU	Organización de las Naciones Unidas
OSCE	Organización para la Seguridad y la Cooperación en Europa
OTAN	
CCDCOE	Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN
OTAN	Organización del Tratado del Atlántico Norte
PIDCP	Pacto Internacional de Derechos Civiles y Políticos
PIDESC	Pacto Internacional de Derechos Económicos, Sociales y Culturales
PI	Parte interesada
TEDH	Tribunal Europeo de Derechos Humanos
TIC	Tecnologías de la información y comunicación
TPIY	Tribunal Penal Internacional para la antigua Yugoslavia
UA	Unión Africana
UE	Unión Europea
UK	Reino Unido
UNCDH	Consejo de Derechos Humanos de las Naciones Unidas
UNIDIR	Instituto de las Naciones Unidas para la Investigación sobre el Desarme
UNODA	Oficina de Asuntos de Desarme de las Naciones Unidas

RESUMEN EJECUTIVO

A medida que los Estados participan cada vez más en actividades cibernéticas, los interrogantes sobre la aplicación del derecho internacional a dicha conducta han ganado importancia. Aunque hay consenso general de que el derecho internacional se aplica al contexto cibernético, las perspectivas difieren con relación a cómo se aplican las reglas y principios específicos. Muchos Estados han contribuido al debate emitiendo posiciones nacionales: las declaraciones oficiales describen sus puntos de vista legales sobre aspectos clave del derecho internacional en el contexto cibernético.

Este manual ofrece una orientación práctica para los Estados que están desarrollando o revisando sus posiciones nacionales, basándose en las reflexiones de los 46 Estados que participaron en las mesas redondas regionales llevadas a cabo en Addis Ababa, Singapur y Washington, D.C. en 2024, al igual que en las investigaciones originales realizadas para este proyecto. El manual describe las motivaciones clave, los pasos procedimentales, los cuestiones jurídicas sustantivas y las estrategias de presentación efectivas, ofreciendo un enfoque estructurado que los Estados pueden adoptar en diferentes etapas del proceso.

Conclusiones clave

- **Las posiciones nacionales sirven para múltiples funciones:** Tienen una función comunicativa, al interactuar con partes interesadas nacionales e internacionales; una función transformadora, que clarifica y adapta los marcos jurídicos a las nuevas realidades, y una función preventiva, que reduce el riesgo de interpretaciones erróneas mientras orienta la evaluación de violaciones y las reacciones adecuadas, lo que fomenta la disuasión.
- **El proceso de desarrollo varía dependiendo del contexto nacional, pero sigue algunos pasos comunes:** Estos pasos incluyen asegurar un mandato; reunir un equipo principal con experticia jurídica, política y técnica; realizar análisis jurídicos y políticos; consultar a las partes interesadas y explorar las dinámicas interinstitucionales; determinar el formato final, y obtener las aprobaciones necesarias.
- **Los enfoques de redacción se puede categorizar de modo general como deductivos o inductivos:** El enfoque deductivo parte de reglas establecidas y luego analiza cómo se aplican en el contexto cibernético. El enfoque inductivo empieza a partir de desafíos cibernéticos del mundo real y examina cómo les aplica el derecho internacional. Los Estados pueden combinar ambos, usando casos de estudio o escenarios para brindar mayor claridad.

- **Las posiciones nacionales abordan una amplia gama de cuestiones jurídicas sustantivas:** Estos incluyen principios jurídicos fundamentales, como la soberanía, la no intervención y la prohibición del uso de la fuerza, al igual que regímenes especializados como el derecho internacional humanitario, la derecho internacional de los derechos humano y el derecho penal internacional. Los Estados deben ajustar la elección de temas de acuerdo con sus intereses nacionales y prioridades jurídicas.
- **Aunque existe consenso entre los Estados de que el derecho internacional aplica al contexto cibernético, subsisten diferencias clave:** Estas diferencias están relacionadas con interrogantes tales como si los conceptos como soberanía y diligencia debida constituyen reglas independientes, cómo se pueden determinar los umbrales de los incumplimientos y cómo ciertas actividades cibernéticas (por ejemplo, el espionaje cibernético) se deben clasificar bajo el derecho internacional.
- **El formato y difusión de las posiciones nacionales orienta su impacto:** Los Estados han emitido posiciones como documentos independientes, discursos gubernamentales y declaraciones en foros multilaterales. Su alcance e influencia puede mejorarse con una estructura clara, accesibilidad y difusión estratégica.
- **Las posiciones nacionales contribuyen a la claridad jurídica en la gobernanza del ciberespacio:** Estas esquematizan las áreas de acuerdo, desacuerdo y las posibles brechas jurídicas. A medida que más Estados emitan posiciones, estos documentos continuarán dando forma a la interpretación, implementación y desarrollo del derecho internacional en el contexto cibernético y más allá.
- **Los futuros desarrollos pueden incluir:** Posiciones nacionales más detalladas emitidas por más Estados, mayor coordinación regional, adopción de nuevos instrumentos internacionales si se logran acuerdos sobre brechas específicas, e implementación nacional, como integración de estándares jurídicos internacionales en la legislación, doctrina militar y marcos de política nacionales.

Este manual ofrece un enfoque práctico y estructurado para los Estados que están desarrollando o revisando una posición nacional, ayudando a fomentar mayor claridad jurídica, previsibilidad y estabilidad en el ciberespacio. Al describir las prácticas existentes, los desafíos comunes y las consideraciones estratégicas, ofrece un recurso clave para los gobiernos, profesionales del derecho y responsables de políticas públicas que exploran la aplicación del derecho internacional en el contexto cibernético.

CAPÍTULO 1:

INTRODUCCIÓN

El rápido desarrollo de las tecnologías de la información y comunicación (TIC) durante las últimas décadas ha traído innumerables beneficios a las personas y sociedades de todo el mundo. El surgimiento del ciberespacio ha facilitado nuevas y más efectivas maneras de comunicación, colaboración y coordinación. Ha transformado las economías, empoderado a comunidades y mejorado el acceso a la información a una escala sin precedentes. Sin embargo, también hay desafíos significativos. Las operaciones cibernéticas hostiles han causado perturbaciones en todo el mundo, produciendo costos humanos significativos y afectando intereses esenciales de los Estados. Hoy en día, internacionalmente existe el consenso de que las actividades cibernéticas maliciosas pueden tener consecuencias devastadoras a nivel económico, social, humanitario y para la seguridad, que con frecuencia trascienden las fronteras nacionales.[1]

A medida que estos acontecimientos se desarrollan a escala mundial, el derecho internacional tiene un papel fundamental en la regulación de las actividades cibernéticas y en mitigar sus impactos. Desde 2013, ha emergido el consenso entre los Estados de que el derecho internacional es aplicable y fundamental para mantener la paz, la seguridad y la estabilidad en el entorno de las TIC.[2] Sin embargo, subsisten diferencias sobre cómo se aplican las reglas y principios del derecho internacional en el contexto cibernético.

Estos debates abordan aspectos fundamentales del derecho internacional, como la responsabilidad del Estado, la soberanía, la no intervención y la prohibición del uso de la fuerza, así como regímenes especializados como el derecho internacional humanitario, el derecho internacional de los derechos humanos y el derecho penal internacional.

La clarificación y desarrollo del derecho en esta área ocurre en gran medida mediante la publicación de posiciones nacionales sobre el derecho internacional y las actividades cibernéticas. Estas declaraciones oficiales articulan cómo interpretan y aplican los Estados las reglas y principios clave del derecho internacional a las actividades cibernéticas, dando forma al discurso jurídico internacional e influenciando el desarrollo de reglas y prácticas. Al momento de escribir este documento, 33 Estados habían emitido tales posiciones, junto con dos organizaciones regionales, la Unión Africana (UA) y la Unión Europea (UE), que han publicado posiciones conjuntas (consulte una lista de estos documentos en el **Anexo B**). Otros Estados están evaluando si deben emitir una posición nacional propia, mientras que algunos que ya tienen posiciones están analizando hacer revisiones o actualizaciones.

1 Asamblea General de las Naciones Unidas, *Informe del Grupo de Trabajo de Composición Abierta sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional*, A/75/816 (18 de marzo de 2021), párr. 18.

2 Asamblea General de las Naciones Unidas, *Informe del Grupo de Trabajo de Composición Abierta sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional*, A/68/98 (24 de junio de 2013), párr. 19.

La clarificación y desarrollo del derecho internacional en el contexto cibernético tiene lugar en gran medida mediante posiciones nacionales, que son declaraciones oficiales sobre cómo aplican los Estados los estándares jurídicos a las actividades cibernéticas.

Este manual examina esta tendencia en aumento, basándose en posiciones nacionales disponibles públicamente, debates en foros multilaterales y reflexiones de consultas a puerta cerrada con representantes de los Estados. Ofrece una orientación práctica para los gobiernos que buscan desarrollar o revisar una posición nacional, ofreciendo un enfoque estructurado al proceso, contenido y presentación de dichos documentos.

Proyecto

Este manual es producto de un proyecto colaborativo liderado por un **consorcio de instituciones** conformado por el Ministerio de Asuntos Exteriores de Estonia, el Ministerio de Asuntos Exteriores de Japón, el Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN (CCDCOE) y la Universidad de Exeter. Este proyecto también se benefició del apoyo de instituciones aliadas, entre las cuales están la Unión Africana (UA), la Organización de Estados Americanos, el Ministerio Federal de Asuntos Exteriores de Alemania, el Centro de Derecho Internacional, la Universidad Nacional de Singapur y la Universidad Tecnológica de Tallin.

Como parte de este esfuerzo, entre septiembre y noviembre del 2024, el equipo del proyecto organizó **tres mesas redondas regionales** a puertas cerradas que reunieron a representantes de Estados de las Américas (Washington, DC), Asia y el Pacífico (Singapur) y África (Addis Ababa). Estas mesas redondas, a las que asistieron 77 funcionarios de 46 Estados, aportaron una fuente invaluable de material para este manual. Permitieron el intercambio directo entre los representantes de aquellos gobiernos que ya habían publicado posiciones nacionales, los que estaban en el proceso de desarrollarlas y los que estaban evaluando si lo hacían. En el **Anexo D** se proporciona una lista completa de los eventos del proyecto llevados a cabo antes de la publicación de este manual.

Los debates de estas mesas redondas se llevaron a cabo de conformidad con la **regla de Chatham House**. De esta manera, el manual no atribuye a personas, Estados o instituciones específicos las reflexiones o puntos de vista expresados durante estas reuniones, ni divulga su identidad ni afiliación. Pero, cuando es pertinente, atribuye si una observación en particular fue hecha por un representante de un Estado participante o un experto invitado, sin identificarlo ni divulgar su afiliación específica. La lista completa de los Estados participantes en este proceso consultivo se incluye en el **Anexo C.**

Este proyecto se fundamenta y complementa otras iniciativas en este campo. En particular, se basa en el proyecto *Cyber Law Toolkit (Kit de herramientas sobre derecho cibernético),* uno de los principales recursos en línea sobre derecho internacional y operaciones cibernéticas.[3] La completa base de datos sobre las posiciones nacionales ha sido una referencia fundamental, que ha permitido los análisis detallados de las perspectivas de los Estados contenidas en este manual. De igual manera, el *Compendio de buenas prácticas: Desarrollo de una posición nacional sobre la interpretación del derecho internacional y el uso de las TIC por los Estados,* publicado por el Instituto de las Naciones Unidas para la Investigación sobre el Desarme en 2024, es una fuente más concisa que identifica las buenas prácticas y reflexiones procedimentales de los Estados que ya han desarrollado posiciones nacionales.[4] *El Manual de Tallin 2.0* también sirvió como un punto de referencia clave para el análisis jurídico de este manual, particularmente en lo relacionado con la interpretación del derecho internacional en el contexto cibernético.[5] Estas iniciativas han contribuido significativamente al campo y este manual está diseñado para apoyar sus trabajos.

3 Consulte https://cyberlaw.ccdcoe.org.

4 UNIDIR, *Compendio de buenas prácticas: Desarrollo de una posición nacional sobre la interpretación del derecho internacional y el uso de las TIC por los Estados* (2024).

5 Michael N Schmitt (editor), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* [Manual de Tallin 2.0 sobre el derecho internacional aplicable a las operaciones cibernéticas]

Posiciones nacionales y conjuntas

Este manual se centra en el desarrollo de **posiciones nacionales** sobre la aplicación del derecho internacional en el contexto cibernético. Uno de los puntos clave de este proyecto es la diversidad de formatos y enfoques que los Estados han utilizado para articular sus posiciones. Algunos han publicado documentos de posición especializados, mientras que otros han expresado sus perspectivas mediante discursos oficiales o declaraciones en foros multilaterales. En ocasiones, esto último fue seguido por la emisión de un documento más exhaustivo. El **Capítulo 5** analiza estas elecciones con mayor detalle, así como sus implicaciones jurídicas y políticas.

Dada la gama de materiales disponibles, fue necesario tener criterios claros para determinar qué documentos incluir en nuestro análisis. Aunque las mentes razonables pueden diferir en qué califica como una posición nacional, para los fines de este manual nos hemos focalizado en los documentos que cumplen todas las siguientes condiciones:

1. **Emitidas públicamente:** El documento debe estar disponible para el público en general, en vez de haber sido compartido únicamente en un entorno de puerta cerrada, reuniones no públicas de asesores jurídicos o sesiones a puerta cerrada del GEG.
2. **Emitidas por un organismo estatal:** El documento debe estar emitido oficialmente por una o más entidades gubernamentales (como un Ministerio de Asuntos Exteriores o la Oficina del Primer Ministro) o impartido por un funcionario que hable en representación del gobierno (como un diplomático de alto rango o el fiscal general).
3. **Disponible en formato escrito en un repositorio público:** El documento debe estar publicado por completo en un formato dirigido a la accesibilidad del público a largo plazo, como un sitio web gubernamental, en el compendio voluntario del Grupo de Expertos Gubernamentales de la ONU (GEG) o como presentación oficial al Grupo de Trabajo de Composición Abierta de la ONU (GTCA).
4. **Publicado con la finalidad de expresar perspectivas jurídicas específicas sobre la aplicación del derecho internacional en el contexto cibernético:** la finalidad principal del documento debe ser abordar las cuestiones jurídicas sustantivas, en lugar de, o al menos además de, limitarse a reafirmar compromisos generales con el derecho internacional o debatir asuntos de política, normas no vinculantes del comportamiento responsable de los Estados, u otros asuntos no jurídicos.

En el **Anexo B** se proporciona una lista completa de los documentos que cumplen estos criterios. Para asegurar uniformidad, las citas en todo este manual se refieren a estos de manera abreviada como 'posición nacional de [Estado]'.

Aunque los foros multilaterales basados en la ONU, como el GTCA, se centran principalmente en los usos de las TIC por parte del Estado, las posiciones nacionales con frecuencia superan este alcance, abordando también la conducta de los actores no estatales. Por ejemplo, algunas posiciones nacionales tratan sobre si las actividades cibernéticas de los actores no estatales pueden constituir un ataque armado, las obligaciones de los grupos armados no estatales conforme al derecho internacional humanitario y las responsabilidades de diligencia debida de los Estados con relación con la conducta cibernética de los actores no estatales en su jurisdicción. Unas pocas posiciones también referencian las obligaciones relacionadas con la ciberdelincuencia, sin embargo, este tema ha sido abordado en gran medida en negociaciones separadas, particularmente en la Tercera Comisión de la Asamblea General de las Naciones Unidas, que llevó a la adopción de la Convención de las Naciones Unidas contra la Ciberdelincuencia a finales de 2024. En general, el alcance de las posiciones nacionales es amplio, e incluye varios temas relacionados con la interpretación y aplicación del derecho internacional a las actividades cibernéticas.

Mientras este proyecto estaba en marcha, tanto la UA como la UE publicaron sus **posiciones conjuntas**, que reflejan las perspectivas compartidas de sus Estados miembros sobre la aplicación del derecho internacional en el contexto cibernético.[6] Estos documentos son muy semejantes a las posiciones nacionales en cuanto a estructura y contenido, pero su proceso fue diferente, ya que fueron desarrollados mediante construcción de consenso entre varios Estados, en vez de expresar una sola perspectiva nacional. Dada su importancia, este manual cita y hace uso de las posiciones conjuntas de la UA y la UE en todo su análisis. En el contexto del GTCA, los grupos de Estados ocasionalmente también han emitido declaraciones interregionales conjuntas que abordan la aplicación del derecho internacional al uso de las TIC. Sin embargo, como dichas posiciones y declaraciones conjuntas involucran dinámicas jurídicas y políticas distintas, este manual no propone orientaciones específicas para su desarrollo. Dicho esto, la mayor parte de sus análisis y recomendaciones se pueden aplicar mutatis mutandis a dichos esfuerzos.

6 Posiciones conjuntas de la UA (2024) y la UE (2024).

Importancia jurídica de las posiciones nacionales

El estado de las posiciones nacionales en el derecho internacional permanece sin definir. Las posiciones mismas mayormente no abordan este tema. Incluso las que hablan de sus objetivos amplios, por lo general los enmarcan como esfuerzos para promover la seguridad jurídica o fomentar entendimientos comunes, en vez de hacer afirmaciones específicas sobre su importancia jurídica.[7] De forma excepcional, algunas posiciones afirman explícitamente que su objetivo es 'desarrollar el derecho consuetudinario' en general[8] o 'ampliar' una perspectiva indicativa del surgimiento de una nueva regla específica.[9]

Los debates durante las mesas redondas del proyecto fueron similarmente inconclusos y amplios. Unos cuantos participantes cuestionaron si las posiciones nacionales son algo más que documentos de política, lo que implica que pueden carecer de cualquier relevancia jurídica independiente. En el otro extremo del espectro, algunos plantearon la idea de que las posiciones nacionales podrían considerarse actos unilaterales de los cuales surgen obligaciones jurídicas internacionales para el Estado emisor. Estas perspectivas divergentes destacan el debate en curso sobre el rol preciso de las posiciones nacionales en dar forma al derecho internacional y la necesidad de aumentar la participación de los Estados y la investigación académica sobre este tema.

Este manual no pretende resolver este debate, por el contrario, destaca las áreas en común. A pesar del escepticismo, la mayoría de los participantes de las mesas redondas del proyecto estuvieron de acuerdo en que las posiciones nacionales son más que meras declaraciones de política. Como son emitidas como declaraciones oficiales sobre la aplicación del derecho internacional, inherentemente conllevan cierto grado de valor jurídico, al menos con relación a las fuentes del derecho internacional que abordan, incluidos los tratados y el derecho internacional consuetudinario.

Cuando las posiciones nacionales interpretan el **derecho de los tratados**, pueden contribuir a la práctica ulteriormente seguida en la aplicación del tratado correspondiente. Conforme a las reglas de la interpretación de tratados, si dicha práctica establece un acuerdo entre las partes sobre una interpretación en particular, podría convertirse en dispositiva de los asuntos en cuestión.[10] Sin embargo, la mayoría de los tratados referenciados en las posiciones nacionales, como la Carta de las Naciones Unidas y los Convenios de Ginebra, tienen más de 150 Estados partes, de los cuales la mayoría aún no ha emitido dichas posiciones. Incluso si hay un acuerdo amplio entre los Estados que lo han hecho, esto es insuficiente para establecer un acuerdo interpretativo definitivo en esta etapa.[11]

7 Consulte, por ejemplo, las posiciones nacionales de Dinamarca (2023), pág. 447, Finlandia (2020), pág. 1, Alemania (2021), págs. 1 y 2, Japón (2021), pág. 1, Polonia (2022), pág. 1, Suecia (2022), pág. 1, Suiza (2021), pág. 1 y los Estados Unidos (2021), pág. 136.

8 Posición nacional de Polonia (2022), pág. 1.

9 Posición nacional de Estonia (2019).

10 Convención de Viena sobre el Derecho de los Tratados (1969), artículo 31(3)(b).

11 CDI, *Proyecto de conclusiones sobre los acuerdos ulteriores y la práctica ulterior con relación con la interpretación de los tratados*, A/73/10 (2018), conclusión 10(1).

Por ahora, los entendimientos comunes emergentes solo pueden servir como un medio complementario de interpretación, que indica las áreas donde puede estar emergiendo el consenso, pero que no es concluyente todavía.[12]

Las posiciones nacionales también se refieren frecuentemente al derecho internacional consuetudinario. Más comúnmente, los Estados lo hacen para afirmar la naturaleza consuetudinaria de una o un conjunto de reglas, como las prohibiciones de intervención[13] y el uso de la fuerza[14] o el derecho de la responsabilidad del Estado[15] En ocasiones, los Estados invocan la costumbre en la negativa, rechazando el surgimiento de una norma particular como parte del derecho internacional consuetudinario.[16]

El derecho internacional consuetudinario se forma mediante la combinación de dos elementos fundamentales: práctica del Estado (un patrón general y constante del comportamiento de los Estados) y opinio juris (aceptación de que dicho

12 Convención de Viena sobre el Derecho de los Tratados (1969), artículo 32.

13 Posiciones nacionales de Australia (2021), pág. 2, Brasil (2021), pág. 18, Costa Rica (2023), párr. 23, Dinamarca (2023), pág. 449, Alemania (2021), pág. 4, Irán (2020), art. III 1, Italia (2021), pág. 4, Noruega (2021), pág. 4, Suiza (2021), pág. 3, Reino Unido (2022) y los Estados Unidos (2021), pág. 139.

14 Posiciones nacionales de Brasil (2021), pág. 19, Costa Rica (2023), párr. 35, Israel (2021), pág. 398, Noruega (2021), pág. 5, Polonia (2022), pág. 5, Suecia (2022), pág. 3 y de los Estados Unidos (2021), pág. 137.

15 Posiciones nacionales de Australia (2021), pág. 5, Canadá (2022), párr. 32, Costa Rica (2023), párr. 10, Estonia (2021), pág. 28, Alemania (2021), pág. 10, Irlanda (2023), párr. 20, Polonia (2022), pág. 6, Suiza (2021), pág. 5 y de los Estados Unidos (2021), pág. 141.

16 Consulte, por ejemplo, las posiciones nacionales de Israel (2021), pág. 404, el Reino Unido (2021), párr. 12 y los Estados Unidos (2021), pág. 141, que rechazan el surgimiento de una norma consuetudinaria de diligencia debida.

comportamiento se lleva a cabo como cuestión de obligación jurídica).[17] Es justamente poco controversial que las posiciones nacionales puedan calificar como expresiones de opinio juris, en la medida que articulan la convicción jurídica de un Estado de que cierta categoría de conducta es permitida, requerida, prohibida, o incluso desregulada, conforme al derecho internacional consuetudinario, como pueda ser el caso.[18]

Sin embargo, es más controvertido si las posiciones nacionales también califican como prácticas estatales. Como el derecho internacional consuetudinario por lo general se desarrolla inductivamente, mediante la conducta repetida de los Estados, en vez de deductivamente, mediante declaraciones generalizadas, hay duda sobre si las posiciones escritas en sí mismas puedan contar doblemente como práctica y opinio juris.[19] Dicho esto, se puede considerar que las opiniones nacionales ofrecen evidencia de la práctica del Estado donde describen la conducta específica del Estado relacionada con el ámbito cibernético, pero dichos ejemplos hasta ahora han sido muy raros.[20] Incluso si las posiciones nacionales (o sus partes) fueran aceptadas como instancias de práctica, su cantidad limitada significa que aún no cumplen el requisito de generalidad necesario para que emerja una nueva norma consuetudinaria.[21] Esto, sin embargo, podría cambiar a medida que más Estados publiquen posiciones nacionales.

El significado jurídico del silencio estatal en respuesta a la publicación de las perspectivas de otros Estados está sin resolver. Algunos dicen que los Estados deben refutar las interpretaciones con las que disienten, y otros rechazan que la inacción deba ser tratada como aceptación.

Un interrogante relacionado es si el **silencio de los Estados** que no han emitido posiciones nacionales equivale a la aquiescencia de las interpretaciones prevalentes o al surgimiento de nuevas reglas de costumbre. Este fue un tema de discusión importante en las mesas redondas. Conforme con el derecho internacional, el silencio solo se considera aquiescencia en circunstancias excepcionales, con criterios relevantes que incluyen que el Estado en cuestión permanezca en silencio en circunstancias que requieren una respuesta, que tenga conocimiento de dichas circunstancias y que haya transcurrido un periodo de tiempo razonable.[22]

17 Estatuto de la Corte Internacional de Justicia, artículo 38(1)(b).

18 Consulte también CDI, *Proyecto de conclusiones sobre la identificación del derecho internacional consuetudinario con comentarios*, A/73/10 (2018), conclusión 2, comentario del párrafo 4.

19 Sobre la objeción de la 'doble contabilización' más generalmente, consulte Maurice Mendelson, 'Formación del derecho internacional consuetudinario', (1998) 272 Recueil des Cours 155, 206–207.

20 Consulte, por ejemplo, la posición nacional de Francia (2021), pág. 12, que afirma que la 'mayoría de las operaciones cibernéticas llevadas a cabo por las fuerzas armadas francesas en una situación de conflicto armado son principalmente de recopilación de información y no cumplen la definición de un ataque' (trad. libre). Consulte también el Capítulo 4, sección 3.a, sobre la definición de un ataque conforme con el DIH.

21 CDI, *Proyecto de conclusiones sobre la identificación del derecho internacional consuetudinario con comentarios*, A/73/10 (2018), conclusión 8(1).

22 CDI, *Proyecto de conclusiones sobre la identificación del derecho internacional consuetudinario con comentarios*, A/73/10 (2018), conclusión 10(3); CDI, *Proyecto de conclusiones sobre los acuerdos ulteriores y la práctica ulterior con relación con la interpretación de los tratados*, A/73/10 (2018), 15, conclusión 10(2).

Sigue sin definirse si la publicación de las perspectivas de otros Estados sobre el derecho internacional en el contexto cibernético configura dicha circunstancia. Mientras algunos participantes argumentaron que los Estados deben refutar activamente las interpretaciones con las que disienten, otros rechazaron que la inacción por sí misma deba ser tratada como aceptación jurídica. Más allá del debate jurídico, hubo un acuerdo general de que, en materia de política, es prudente que los Estados respondan a las interpretaciones que consideren incorrectas o contrarias a sus intereses, para que no reciban gradualmente mayor aceptación.

Estructura del manual

Este manual está dividido en seis capítulos que siguen una progresión lógica que refleja las consideraciones y pasos típicos por los que pasan los Estados para desarrollar una posición nacional. Luego de esta introducción:

- El **Capítulo 2** analiza las motivaciones detrás de desarrollar una posición nacional, explorando por qué los Estados eligen articular sus perspectivas sobre el derecho internacional y las actividades cibernéticas o abstenerse de hacerlo.
- El **Capítulo 3** esboza el proceso de redactar una posición nacional, resaltando las buenas prácticas, los desafíos y las lecciones aprendidas de los Estados que ya han abordado este esfuerzo.
- El **Capítulo 4** aborda los interrogantes jurídicos fundamentales que comúnmente se tratan en las posiciones nacionales, identificando las áreas clave de acuerdo, debates en curso y cuestiones jurídicas emergentes.
- El **Capítulo 5** ofrece orientación para la presentación de las posiciones nacionales, tratando sobre las opciones relacionadas con formato, estilo, idioma y difusión.
- La **Conclusión** sintetiza los puntos clave y debate las futuras direcciones de las posiciones nacionales al dar forma al discurso del derecho internacional.

Además de los capítulos sustantivos, el manual incluye una **lista de verificación práctica para desarrollar una posición nacional** (**Anexo A**). Esta herramienta resume los pasos básicos, consideraciones y buenas prácticas descritas en el texto principal, y está diseñada para ayudar a los funcionarios en la planificación, redacción y entrega de sus posiciones nacionales.

Al ofrecer un enfoque estructurado para el desarrollo, contenido y presentación de las posiciones nacionales, este manual tiene como finalidad apoyar a los Estados en todas las etapas del proceso, desde los que están evaluando emitir una primera posición nacional hasta los que están refinando y actualizando una existente. Además, pretende ayudar a gobiernos, profesionales, investigadores y responsables de políticas públicas en su trabajo, contribuyendo así a los esfuerzos más amplios de mejorar la claridad, previsibilidad y estabilidad jurídica en el ciberespacio.

CAPÍTULO 2:

MOTIVACIONES

DE UN VISTAZO

Este capítulo explica por qué los Estados desarrollan posiciones nacionales sobre el derecho internacional en el ciberespacio. Describe las motivaciones clave, como promover la claridad jurídica, prevenir los errores de cálculo y dar forma a las normas internacionales, y además destaca cómo las posiciones pueden servir para metas tanto nacionales como internacionales. Los Estados pueden actuar para construir credibilidad, alinearse con aliados o responder ante amenazas. Entender estas motivaciones puede ayudar a orientar las decisiones sobre qué incluir en la posición y cómo usarla mejor en los debates jurídicos y políticos globales.

1. INTRODUCCIÓN

Hoy en día, existe consenso en que las actividades cibernéticas maliciosas pueden tener consecuencias devastadoras a nivel económico, social, humanitario y para la seguridad.[1] Por esto, los pasos y medidas que se toman para prevenir y responder a las ciber amenazas, mediante el derecho internacional u otros medios, son influidos por motivaciones complejas y con frecuencia superpuestas. Las posiciones nacionales son valiosas herramientas jurídicas y políticas para abordar dichas amenazas y desafíos en el ciberespacio. Se desarrollan por motivos expresos o implícitos, y pueden servir a los intereses y objetivos externos o nacionales, que pueden tener diferente peso para los diferentes Estados. Estas consideraciones orientan las decisiones relacionadas con el desarrollo de una posición nacional, las cuestiones que aborda y con cuánta profundidad, y las perspectivas jurídicas que se toman sobre los asuntos sustantivos elegidos (por ejemplo, soberanía, diligencia debida y contramedidas). Estas opciones también son influidas por factores como el tamaño del territorio, la población, la economía, las capacidades y otros elementos objetivos, pero dependientes del contexto del Estado.

Este capítulo identifica y desglosa los factores motivadores que determinan las decisiones sobre varios aspectos de las posiciones nacionales. Aunque no pretende ser exhaustivo, el objetivo es ayudar a los Estados a identificar coyunturas críticas en la toma de decisiones, a comprender las posibles implicaciones de los diferentes enfoques y a construir argumentos persuasivos que apoyen la ruta preferida. Los **factores motivadores clave** pueden categorizarse de acuerdo con su dimensión interna o externa y en términos de las funciones de las posiciones nacionales: comunicativas, transformadoras y preventivas. Las motivaciones influyen en cómo se implementan las funciones para lograr los **objetivos explícitos o implícitos** de una posición nacional.

1 Asamblea General de las Naciones Unidas, *Informe del Grupo de Trabajo de Composición Abierta sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional*, A/75/816 (18 de marzo de 2021), párr. 18.

Desarrollar y publicar una posición nacional es una **elección**. Sin embargo, no hacerlo en forma de un documento especializado y consolidado, o posponer o prolongar su desarrollo no necesariamente significa que el Estado permanece en silencio. Los Estados pueden optar por expresar sus perspectivas jurídicas mediante otros medios y formatos, como aportes verbales o escritos al Grupo de Trabajo de Composición Abierta de la ONU (GTCA), que pueden ser alternativas que requieren menos recursos. Las siguientes secciones exploran las motivaciones y objetivos que reflejan posiciones nacionales existentes y sintetizan las reflexiones clave producto de las mesas redondas del proyecto.

2. Motivaciones, funciones y objetivos generales

a. Motivaciones generales

El desarrollo de una posición nacional surge de la confluencia de motivaciones interconectadas. Estas declaraciones son contextuales y toman naturalmente las perspectivas del Estado que las adopta.

Articular sus motivaciones políticas más amplias puede ayudar al Estado a ajustar su posición nacional a sus intereses particulares y a formular los objetivos específicos que desean buscar.

Por ejemplo, mientras algunos Estados se centran en el impacto social o económico de las actividades cibernéticas y su relación con el desarrollo[2], otros se focalizan en las implicaciones de estas en un conflicto armado.[3]

Aunque las posiciones nacionales han emergido en el contexto del derecho internacional y podrían considerarse típicamente como un asunto para los abogados internacionalistas, parece que muchos Estados reconocen que el interrogante de cómo aplica el derecho internacional en el contexto cibernético (parafraseando a Georges Clemenceau) es demasiado importante para delegarse por completo a los abogados internacionalistas. Articular una posición nacional sobre el derecho internacional tiene consecuencias reales e influye en cómo el Estado proyecta poder y reacciona ante la proyección de poder en y a través del ciberespacio. De esta manera, los impulsores clave tras la elección de desarrollar una posición nacional y de cómo formularla surgen de consideraciones de política tanto interna como externa. Algunos ejemplos de impulsores externos son la presión percibida de seguir a un grupo de Estados afines o la presión de aliados y la academia. Estos impulsores están centrados en el imperativo de restringir la conducta de los Estados, y definen el alcance de su autonomía en y a través del ciberespacio. Sin embargo, las posiciones nacionales también pueden tener un papel importante en los roles a nivel nacional, además del

2 Consulte, por ejemplo, las posiciones nacionales de China (2021), pág. 1 y Costa Rica (2023), párr. 2 a 4.
3 Consulte, por ejemplo, las posiciones nacionales de Israel (2021), pág. 396.

obvio rol externo de abordar los interrogantes jurídicos internacionales. Por ejemplo, desarrollar una posición nacional puede ayudar al Estado a calibrar su respuesta ante incidentes cibernéticos internacionales, clarificar sus obligaciones jurídicas e identificar las brechas en la gobernanza nacional que requieren atención..

b. Funciones comunicativas, transformadoras y preventivas de las posiciones nacionales

Las posiciones nacionales tienen una **función comunicativa** al interactuar con los actores relevantes a diferentes niveles en todos los diversos elementos del debate más amplio sobre cómo se aplica el derecho internacional al contexto cibernético. Aunque el tema del derecho internacional y el ciberespacio no es nuevo y ha estado en la agenda de las Naciones Unidas desde al menos 1998, la tendencia de redactar y articular públicamente posiciones empezó aproximadamente dos décadas después. Comunicar y declarar una posición sobre la aplicación del derecho internacional a las actividades cibernéticas ante la comunidad internacional y los públicos nacionales señala un alto nivel de madurez en el entendimiento y consideración de los varios intereses involucrados. También indica que el Estado quiere que los demás sepan cuál es su posición y que tiene el interés y la intención de ser parte activa en los procesos jurídicos internacionales relevantes. Una posición nacional es una manera de comunicar internamente y externamente que el Estado obedece las reglas y espera que los demás hagan lo mismo.

Las posiciones nacionales tienen una **función transformadora** al ajustar el marco existente del comportamiento responsable de los Estados ante las nuevas realidades. Las declaraciones en las posiciones nacionales pueden tener efectos jurídicos, por lo que los Estados, como los responsables de políticas públicas primarios del derecho internacional, contribuyen a la clarificación, desarrollo y evolución de las reglas (consulte la **Introducción** sobre el valor jurídico de las posiciones). Las posiciones nacionales con frecuencia aspiran a transformar las reglas de conducta en el ciberespacio, pero pueden diferir significativamente en el nivel deseado de intensidad. Por lo tanto, desarrollar una puede tener como finalidad eliminar las zonas grises para tener mayor claridad, dar forma a los límites y consolidar reglas

existentes, proponer una manera de encontrar intereses comunes, o declarar la intención de establecer otros instrumentos jurídicamente vinculantes en esta área (que sigue siendo controvertida entre los Estados). Incluso si los cambios generales pueden ser sutiles y graduales, al clarificar la aplicación de las reglas existentes, los Estados empiezan a desarrollar expectativas en común y a definir los límites jurídicos de cómo deberían comportarse en el ciberespacio. Por lo tanto, la clarificación es mucho más que un ejercicio técnico; está alimentada por la necesidad percibida o real de reestructurar la dinámica de las relaciones internacionales en el entorno digital.

Las posiciones nacionales tienen una **función preventiva** en términos de mitigar las consecuencias negativas de las acciones llevadas a cabo por actores estatales y no estatales en el ciberespacio, lo que también puede servir como motivación para desarrollar y publicar una posición. Al proponer una interpretación de una regla del derecho internacional, y en ocasiones también añadir ejemplos ilustrativos para mayor claridad, la expectativa se establece sobre las circunstancias en que un Estado consideraría cierta forma de conducta cibernética como una violación del derecho internacional y dónde traza la línea entre el comportamiento legal e ilegal para sí mismo y para los demás. La claridad sobre la aplicación de las reglas fomenta la rendición de cuentas por violaciones y sirve como disuasión. Por lo tanto, la posibilidad de consecuencias jurídicas es un factor para asegurar el control y el respeto por los derechos del Estado.

c. Objetivos generales y resultados esperados

Muchas posiciones nacionales ofrecen al menos cierta explicación sobre los objetivos o razones de su publicación. Como estos textos se redactan cuidadosamente, la explicación puede centrarse en por qué un determinado Estado decide desarrollar una posición y también en arrojar luz sobre los propósitos que tiene la posición, cuáles son los resultados esperados y cómo esta beneficia al Estado y a la comunidad internacional. Los objetivos y expectativas declarados expresamente y aquellos tácitos denotan las maneras en que las funciones comunicativas, transformadoras y preventivas de las posiciones nacionales se implementan y aplican. En otras palabras, **los objetivos son los resultados esperados y las metas orientadas al futuro** que el Estado desea lograr al desarrollar una posición nacional.

Estos objetivos y expectativas con frecuencia se superponen, reflejando la naturaleza compleja y multifacética del dominio cibernético. Algunos temas interconectados surgieron durante las mesas redondas del proyecto, y los objetivos jurídicos y/o políticos específicos o resultados esperados, por lo general se refirieron a algunos aspectos para mejorar la paz y seguridad internacional, fortalecer el orden jurídico internacional o consolidar el entorno nacional.

3. Objetivos específicos y sus motivaciones

a. Prevenir el error de cálculo y la escalada: aumentar la previsibilidad y la estabilidad a escala

Formulación de los objetivos

Al articular explícitamente sus interpretaciones del derecho internacional en el contexto cibernético, los Estados pueden dirigirse a minimizar los malentendidos y a prevenir la escalada no intencional de las actividades cibernéticas, lo que probablemente contribuya a mejorar la paz y seguridad internacionales.

Este enfoque proactivo busca **reducir el riesgo de conflictos** derivados de posibles errores de cálculo e interpretaciones erróneas de las acciones en el dominio digital. Por ejemplo, esto se expresa explícitamente en las posiciones nacionales de Australia, Canadá y Francia.[4] Como precondición para alcanzar este objetivo, también es fundamental una **mayor confianza**, como destaca Francia.

Además, los Estados pueden publicar una posición para subrayar y comunicar que no están dispuestos a aceptar cierto nivel de inferencia en sus asuntos soberanos. Como advirtió el representante de un Estado: 'No se quiere que el silencio se interprete como aquiescencia'.[5] Debido a que los Estados más pequeños son presumiblemente más vulnerables al tipo de actividades cibernéticas en cuestión, para ellos es mucho más importante hacer conocer sus posiciones.[6] Esta mayor **claridad** contribuye a disminuir el riesgo de errores de cálculo e interpretaciones erróneas.

Una posición nacional también puede tener como objetivo aumentar la previsibilidad sobre el comportamiento del Estado y la estabilidad en el ciberespacio. Estas se derivan de un entendimiento común de cómo se aplica el derecho internacional en el contexto cibernético, y esta previsibilidad, destacada, por ejemplo, por las posiciones nacionales de Australia, Singapur y los Estados Unidos[7], contribuye a un entorno internacional más estable y seguro. El objetivo puede ser formulado como la 'promoción del comportamiento responsable de los Estados en el ciberespacio', lo que también se espera que contribuya a lograr. Por ejemplo, Canadá afirma en su posición nacional que 'cree que la articulación de las posiciones nacionales sobre cómo aplica el derecho internacional a las acciones de los Estados en el ciberespacio aumentará el diálogo internacional y el desarrollo de entendimientos

4 Posiciones nacionales de Australia (2021), pág. 1, Canadá (2022), párr. 5, Francia (2019), pág. 4.

5 Comentario hecho en la mesa redonda sobre las perspectivas de Asia y el Pacífico (informe en el archivo con autores) (Trad. libre).

6 Comentario hecho en la mesa redonda sobre las perspectivas de Asia y el Pacífico (informe en el archivo con autores).

7 Consulte, por ejemplo, las posiciones nacionales de Australia (2021), pág. 1, Singapur (2021), pág. 85 y los Estados Unidos (2021), pág. 136.

comunes y concesos sobre el comportamiento legal y aceptable de los Estados'.[8] La posición nacional de Australia añade que, 'incluso cuando las perspectivas difieren, desarrollar entendimientos de las posiciones respectivas de los Estados puede aumentar la previsibilidad y reducir el riesgo de errores de cálculo que podrían conducir a la escalada de la conducta del Estado'.[9] Muchos Estados consideran que el derecho internacional es un elemento fundamental del marco de comportamiento responsable de los Estados en el ciberespacio.

Se puede argumentar que estos objetivos se podrían lograr mejor si muchos Estados expresasen su posición por lo tanto, algunos han alentado a que se añadan más voces y diversidad al debate, promoviendo el desarrollo de posiciones nacionales y liderando con el ejemplo, lo que incluye la participación y membresía en diversos procesos y foros multilaterales.[10] Esto puede aumentar la **legitimidad** de estos procesos y sus logros.

Motivaciones

Los anteriores objetivos posiblemente surgen de la necesidad de garantizar la seguridad nacional, promover la prosperidad económica, mejorar la vida de los ciudadanos y mejorar la posición del Estado ante la comunidad internacional. Estas motivaciones no son exclusivas del contexto cibernético. Para estar seguros, el concepto de posiciones nacionales es **relativamente nuevo**, y los Estados hace mucho que manejan sus relaciones en el ciberespacio sin ellas. Después de todo, el derecho internacional se aplica a las actividades cibernéticas aun en ausencia de posiciones nacionales. Sin embargo, cuando existe incertidumbre sobre cómo aplica, el ciberespacio puede ser percibido como un dominio jurídicamente opaco o ambiguo, y los malentendidos e interpretaciones erróneas de los incidentes cibernéticos pueden aumentar el riesgo de controversias no intencionales. Por lo tanto, posiblemente sea más difícil promover la estabilidad y previsibilidad en el ciberespacio sin una articulación clara de las reglas aplicables del derecho internacional.[11] Por lo general, la expresión de las perspectivas **facilita saber la posición de los Estados**. En otras palabras, un Estado que tenga una posición nacional con conceptos y definiciones compartidos[12] puede permitir que otros comprendan su perspectiva y actúen en consonancia.

Si un Estado tiene una posición nacional con conceptos y definiciones compartidos, puede permitir que otros comprendan su perspectiva y actúen en consonancia.

8 Consulte la posición nacional de Canadá (2022), párr. 5 (Trad. libre).
9 Consulte la posición nacional de Australia (2021), pág. 1 (Trad. libre).
10 Consulte, por ejemplo, las posiciones nacionales de Canadá (2022), párr. 6, y Costa Rica (2023), párr. 5.
11 Comentario hecho en la mesa redonda sobre las perspectivas de Asia y el Pacífico (informe en el archivo con autores).
12 Consulte, por ejemplo, la posición nacional de Alemania (2021), pág. 2

Varios representantes de los Estados expresaron preocupación porque las voces de muchas regiones están **subrepresentadas** y esto conduce a debates **desequilibrados**. La marginalización o exclusión de regiones presenta el riesgo de crear favoritismos y sesgos reales o percibidos en la cristalización de cómo se aplican las reglas existentes. Esto podría ser perjudicial para la efectiva gobernanza, el cumplimiento y la rendición de cuentas. Por lo tanto, el argumento es que, entre más Estados se expresen, más inclusivo será el debate y menos reclamos podrán presentarse luego para cuestionar la legitimidad de los procesos en el marco de la ONU y regionales. Es más, el campo del ciberespacio ofrece una oportunidad única para articular las perspectivas del Estado, ser proactivos y mantener el impulso con la finalidad de mantener la paz y seguridad internacional.[13]

b. Mejorar el cumplimiento y la rendición de cuentas: disuadir y prevenir las violaciones

Formulación de los objetivos

Publicar las posiciones nacionales puede incentivar a los Estados a **cumplir sus obligaciones legales internacionales** y a mejorar la **rendición de cuentas** por las violaciones. Esto, a su vez, contribuye a la paz y seguridad internacional, al igual que fortalece el orden jurídico internacional. Las posiciones nacionales también se pueden usar para disuadir a los actores maliciosos, un objetivo que tiene alta importancia entre las prioridades de los Estados. Por ejemplo, Estonia argumenta que tener una posición nacional 'también puede tener efectos disuasivos, ya que ahora tenemos más claridad sobre cómo percibiremos y reaccionaremos a las operaciones cibernéticas en el futuro'.[14]

13 Comentario hecho en la mesa redonda sobre las perspectivas de Latinoamérica y el Caribe (informe en el archivo con autores).

14 Posición nacional de Estonia (2019) (Trad. libre).

En su posición nacional, Japón afirma que 'espera que la profundización de un entendimiento conjunto, particularmente con relación a las actividades en el ciberespacio que constituyen una violación del derecho internacional y qué herramientas hay disponibles conforme al derecho internacional para los Estados cuyos intereses fueron violados por operaciones cibernéticas, disuadirá actividades maliciosas en el ciberespacio'.[15] La posición nacional de Francia de 2019, una de las primeras en emitirse, indica que, 'aunque Francia pretende prevenir, protegerse, anticipar, detectar y responder ante los ataques cibernéticos, y hacer lo que sea necesario para atribuirlos, también se reserva el derecho a responder a aquellos que tienen como objetivo sus intereses'.[16] Irán también emplea su posición nacional para expresar intenciones de disuasión usando un lenguaje fuerte, incluida la promesa de 'consecuencias firmes y decisivas' por la violación de sus 'políticas'.[17] Sin embargo, dichas formulaciones son una excepción y la mayoría de las posiciones nacionales utilizan un tono más cooperativo y menos confrontativo, incluso al comunicar sus líneas rojas.

Motivaciones

Las herramientas cibernéticas son parte integral de los conflictos de hoy en día. Por lo tanto, cada líder del gobierno debe responder interrogantes sobre **cómo actuar, cómo reaccionar y cuáles son las opciones jurídicas** en caso de violaciones llevadas a cabo en el ciberespacio o medio de este.[18] El cumplimiento y la rendición de cuentas solo son posibles si la aplicación de las reglas de conducta es **suficientemente clara** y los Estados comprenden dónde están las limitaciones de su autonomía. Esto también es necesario para reclamar por la posible violación de las reglas, al igual que para determinar y elegir las respuestas jurídicas adecuadas. Además, producir una posición exhaustiva y coherente no es algo trivial y es indicativo de un tipo de 'poder cibernético' blando: la capacidad de **ejercer influencia** con relación al ciberespacio.[19] Los Estados pueden tener interés en proyectar la imagen de que tienen poder cibernético.

Además, como lo enfatiza la posición nacional de Australia, la efectividad del derecho internacional gira en torno a la implementación diligente de los Estados y el cumplimiento de sus obligaciones, al igual que en los esfuerzos colaborativos para hacer cumplir estas obligaciones y garantizar la rendición de cuentas por las violaciones.[20]

15 Posición nacional de Japón (2021), pág. 2 (Trad. libre).

16 Posición nacional de Francia (2019), pág. 5 (Trad. libre).

17 Posición nacional de Irán (2020) (Trad. libre).

18 Comentario hecho en la Semana Internacional Cibernética en Singapur en el panel 'Posiciones nacionales sobre el derecho internacional en el ciberespacio: Desafíos, oportunidades y buenas prácticas', 15 de octubre de 2024, Singapur (informe en el archivo con autores).

19 George Christou, 'Ciberdiplomacia: Del concepto a la práctica', *Tallinn Paper* n.º 14, OTAN CCDCOE (2024), 5.

20 Consulte la posición nacional de Australia (2021), pág. 1.

Esta declaración enfatiza en los factores interconectados que contribuyen al éxito del derecho internacional, incluidos la claridad de las reglas, la coherencia de los temas que siguen las reglas, la divulgación de información, y la denuncia de los incumplimientos y sus consecuencias. En otras palabras, el derecho internacional no puede ser eficaz si para los Estados solo es de boca para fuera.

c. Dar forma a la evolución del derecho internacional: abordar la inseguridad jurídica

Formulación de objetivos

Las declaraciones en las posiciones nacionales pueden ser muy claras al enfatizar que el Estado emisor tiene como fin '**contribuir al debate** sobre las modalidades de aplicación del derecho internacional',[21] o que la posición nacional es un instrumento dedicado a **clarificar** la aplicación del derecho internacional a las actividades cibernéticas.[22]

Se han usado otras formulaciones similares.[23] Estos objetivos pueden estar relacionados con la meta general de fortalecer el orden jurídico internacional. Otro objetivo puede ser clarificar el fundamento para la respuesta a los actos ilícitos por parte de otros Estados y actores no estatales en el ciberespacio.[24] Por ejemplo, se cree ampliamente que la soberanía, la prohibición del uso de la fuerza y el principio de no intervención son los tres criterios clave para determinar la legalidad de las operaciones cibernéticas. La mayoría de las posiciones nacionales emitidas hasta ahora prestan mucha atención a estos tres temas y a las medidas de respuesta relacionadas en caso de violaciones (esto se trata con mayor profundidad en el **Capítulo 4**).

Las posiciones nacionales no están estrictamente limitadas a la interpretación y clarificación de las reglas existentes; también se pueden usar para **proponer nuevas**, enfatizar la importancia de ciertas reglas o advertir sobre otras. Por ejemplo, en sus posiciones nacionales, Rusia y Cuba defienden la adopción de una nueva convención universal vinculante sobre la seguridad internacional de la información.[25] Por lo tanto, es claro que esas posiciones nacionales están dirigidas a comunicar un punto sobre las perspectivas del Estado sobre cómo se debe desarrollar el derecho internacional en esta área. Por el contrario, algunos Estados han indicado claramente que, por el momento, no ven **la necesidad de desarrollar un nuevo instrumento jurídicamente vinculante**.[26]

21 Consulte la posición nacional de Alemania (2021), pág. 1.

22 Consulte la posición nacional de Austria (2024), pág. 3.

23 Consulte, por ejemplo, las posiciones nacionales de Dinamarca (2023), pág. 447, Estonia (2019), Países Bajos (2019), pág. 1 y Suiza (2021), pág. 2.

24 Consulte la posición nacional de Dinamarca (2023), pág. 447.

25 Consulte las posiciones nacionales de Cuba (2024), párr. 4, y Rusia (2021), pág. 80.

26 Consulte, por ejemplo, las posiciones nacionales de Austria (2024), pág. 3, República Checa (2020), pág. 2, Estonia (2021), pág. 24, Rumania (2021), pág. 75 y Suecia (2022), pág. 1.

Para intentar trazar una línea media, otros han expresado la perspectiva de que estas opciones pueden no ser mutuamente excluyentes. Por ejemplo, la posición nacional de Brasil afirma que 'es importante identificar la **convergencia** entre los Estados sobre este asunto y, cuando se identifican divergencias, trabajar conjuntamente para aumentar la coherencia en la interpretación de las reglas existentes'. Si es necesario, el desarrollo de normas adicionales también debe considerarse como un medio para llenar las lagunas jurídicas y resolver las incertidumbres restantes'.[27] Las **lagunas jurídicas**, las interpretaciones divergentes sobre reglas existentes y la aplicación de un conjunto de reglas diferentes a casos similares no son algo poco común en el derecho internacional. Por esto, aunque la convergencia sobre las perspectivas jurídicas es una meta valiosa, no necesariamente requiere completa uniformidad. En contraste, el desarrollo de un nuevo tratado vinculante requeriría el consenso de todas las disposiciones negociadas, un objetivo que por lo general involucra deliberaciones y acuerdos más extensos entre los Estados.

Durante las mesas redondas del proyecto surgió que las posiciones nacionales también podrían tener como fin crear conciencia sobre los debates clave e identificar las necesidades de creación de capacidades sobre estos problemas. Los Estados deben tener en cuenta la **compleja red de intereses** de sus relaciones internacionales. Como acotó un representante de un Estado, existe el riesgo de que apoyar un nuevo instrumento jurídicamente vinculante para el ciberespacio podría utilizarse como una moneda de cambio en las negociaciones entre Estados en otros asuntos no relacionados, especialmente donde existe poca conciencia de la importancia del debate sobre la aplicación del derecho internacional en el contexto cibernético.[28]

Motivaciones

Un impulsor clave para emitir una posición nacional es el deseo de contribuir **activamente** al Estado de derecho internacional en el contexto cibernético dinámico, en lugar de limitarse a aceptar las reglas establecidas. Divulgar sus perspectivas permite a los Estados influenciar y dar forma a la interpretación y evolución del derecho internacional en el contexto cibernético. Por ejemplo, Suiza considera las posiciones nacionales de los Estados como una 'importante contribución para desarrollar la aplicación del derecho internacional en el ciberespacio'.[29] Pareciera haber una conciencia y entendimiento amplios de este impulsor, expresamente en las posiciones nacionales emitidas hasta ahora e intuitivamente entre los Estados que aspiran a desarrollar una.[30]

27 Posición nacional de Brasil (2021), pág. 18 (Trad. libre). (Énfasis añadido).

28 Comentario realizado en el Tercer Simposio Anual Presencial sobre Derecho Cibernético e Internacional, Conflicto Futuro: Convergencia del Derecho Internacional Cibernético y de la Información, en el panel sobre 'Navegando por la dinámica jurídica: perspectivas nacionales sobre el derecho internacional y las posibilidades de convergencia', Universidad Americana, 24 de septiembre de 2024, Washington, DC (informe en archivo con autores).

29 Consulte la posición nacional de Suiza (2021), pág. 1 (Trad. libre).

30 Varios comentarios hechos en las tres mesas redondas del proyecto (informe en archivo con autores).

A primera vista, desarrollar una posición nacional puede parecer un ejercicio académico. En realidad, es un **trabajo mucho más complejo y consecuente** relacionado con las reglas fundamentales del derecho internacional en su relación con los asuntos de la paz y la seguridad en el ciberespacio. En este sentido, las posiciones nacionales son un registro de las perspectivas del Estado sobre estos temas críticos. Por lo tanto, mantener el silencio y no participar puede tener un costo significativo para el consenso emergente sobre estos asuntos. Durante las mesas redondas del proyecto, los representantes de varios Estados expresaron preocupación sobre que el silencio restante se pueden (mal) interpretar como aquiescencia de los entendimientos de los demás sobre conceptos jurídicos clave, como la soberanía, la no intervención y la prohibición del uso de la fuerza.[31] Posiblemente, este riesgo se haga más significativo con el tiempo, a medida que más Estados articulen sus perspectivas y el entendimiento internacional de estos conceptos jurídicos siga cristalizándose.

Además, no es suficiente que los Estados desarrollen su propio entendimiento de las normas. Estos entendimientos también deben ser **comunicados y divulgados** si han de influenciar la aplicación del derecho internacional existente o su futuro desarrollo en el contexto cibernético. Como lo expresa la posición nacional de Polonia, 'la práctica de presentar públicamente las posiciones sobre asuntos clave relacionados con el derecho internacional aumenta el nivel de certidumbre y transparencia jurídica, al tiempo que contribuye a fortalecer el respeto por los compromisos con el derecho internacional y ofrece la oportunidad de desarrollar el derecho consuetudinario'.[32] Reducir la inseguridad jurídica está estrechamente relacionado con el respeto del estado de derecho, ya que la incertidumbre dificulta más la implementación y el cumplimiento.

Reconociendo la naturaleza evolutiva del ciberespacio, los Estados han admitido la necesidad de abordar y reducir las incertidumbres jurídicas, identificando posibles lagunas en la aplicación del derecho internacional en este contexto. Al articular sus posiciones, los Estados pueden contribuir a llenar estos vacíos y a **reducir los riesgos asociados a las interpretaciones jurídicas ambiguas**.

Además de estas consideraciones, los **Estados más pequeños** pueden considerar la articulación de una posición nacional como un medio para **hacer valer y proteger sus derechos** en el ámbito internacional, donde con frecuencia dominan los grandes poderes. Por otro lado, los Estados más grandes, de manera predeterminada, ya tienen un asiento en la mesa, pero, como notaron representantes de los Estados durante las mesas redondas del proyecto, esto trae **responsabilidades y presión** para liderar el debate.[33]

31 Comentario hecho en la mesa redonda sobre las perspectivas de África (informe en el archivo con autores).

32 Posición nacional de Polonia (2022), pág. 1 (Trad. libre).

33 Comentario hecho en la mesa redonda sobre las perspectivas de Latinoamérica y el Caribe (informe en el archivo con autores).

Por otro lado, hay factores que motivan a los Estados a **restringirse** y no tomar decisiones aceleradas anunciando la necesidad de nuevas reglas. Muchos Estados consideran que, en este momento, esta área está evolucionando demasiado rápido y es demasiado volátil para permitir la negociación de un tratado global eficaz. Tampoco está claro **cuál podría ser el contenido sustantivo** de dicho tratado cuando los Estados apenas han comenzado a considerar sus posiciones y existen tanto convergencias como divergencias en cuestiones clave. Por lo tanto, estas consideraciones también alimentan formulaciones donde los Estados aclaran lo que **no es su objetivo** o que no tienen intenciones de debatir en ese sentido.

Al **decidir** cuáles asuntos sustantivos se deben incluir en su posición nacional, por lo general, el Estado debe considerar la **importancia** del asunto en el contexto cibernético, su **capacidad** de contribuir a la clarificación del asunto relevante, y el alcance hasta el cual es probable una **coordinación nacional exitosa**.[34] En algunos casos, esto puede incluir un creciente reconocimiento de la necesidad de un enfoque de la ciberseguridad centrado en los humanos que aborde las diversas necesidades y vulnerabilidades de las personas y comunidades.[35] También hay espacio para presentar asuntos de política más amplios en las posiciones nacionales. Algunos Estados, como China, enfatizan la necesidad de abordar la brecha digital y prevenir la politización de los asuntos de tecnología y ciberseguridad.[36] Los Estados con infraestructura cibernética poco desarrollada pueden estar particularmente interesados, por ejemplo, en los aspectos jurídicos internacionales de las embajadas de datos y, más generalmente, en la computación en la nube,[37] y siguen retomando la necesidad de la creación de capacidades.

34 Comentario hecho en la mesa redonda sobre las perspectivas de Asia y el Pacífico (informe en el archivo con autores).

35 Consulte la posición nacional de Costa Rica (2023), párr. 5.

36 Posición nacional de China (2021), pág. 1.

37 Comentario hecho en la mesa redonda sobre las perspectivas de África (informe en el archivo con autores).

Por su lado, los Estados pequeños tienen un interés natural en las respuestas colectivas a las violaciones del derecho internacional.[38] Cuando una interpretación u opinión planteada es **divergente** de las demás o se destaca de alguna forma (por ejemplo, Brasil considera que la interceptación de las telecomunicaciones es una violación de la soberanía,[39] y Estonia añade la perspectiva de que las contramedidas colectivas están permitidas por el derecho internacional[40]), se hace aún más importante saber cuáles son las **perspectivas de la mayoría silenciosa**, ya que la ley está evolucionando en este campo.[41]

Las posiciones nacionales tienen influencia **más allá del contexto** cibernético, ya que con frecuencia involucran interrogantes más amplios del derecho internacional. Para este fin no hay objetivos claramente formulados en las posiciones nacionales, pero este tema fue planteado repetidamente durante las mesas redondas del proyecto. Esta consecuencia de los debates sobre la aplicación del derecho internacional a las actividades cibernéticas es particularmente visible cuando los Estados articulan perspectivas sobre el alcance, contenido y elementos de las varias reglas primarias y secundarias del derecho internacional en términos generales, antes de aplicarlas al contexto cibernético específico. Estas expresiones tienen el potencial de influenciar la interpretación y el entendimiento de las reglas relevantes en otras áreas del derecho internacional.

Un ejemplo claro es el asunto de la soberanía. En 2018, el Reino Unido expresó la opinión de que la soberanía es un principio del derecho internacional, pero no una regla que se puede violar como tal.[42] Muchos Estados respondieron rápidamente, declarando en sus posiciones nacionales que la soberanía es una regla autónoma del derecho internacional que implica una obligación independiente.[43] Aunque el tema surgió en el contexto cibernético, las declaraciones en las posiciones nacionales respecto a esta asunto son **amplias** y con frecuencia también se relacionan con el derecho internacional general. Otro tema puntual es el relacionado con la asistencia de terceros Estados en la toma de contramedidas. Estonia plantea el asunto de las contramedidas colectivas en su posición nacional,[44] pero ahora hay un **debate en curso** donde varios Estados tienen algo que añadir.[45] Los dos asuntos se tratan con mayor detalle en el **Capítulo 4** en el contenido de las posiciones nacionales.

38 Consulte, por ejemplo, las posiciones nacionales de Costa Rica (2023), párr. 15, y Estonia (2019 y 2021, pág. 28).

39 Posición nacional de Brasil (2021), pág. 18.

40 Posiciones nacionales de Estonia (2019 y 2021, pág. 28).

41 Comentario hecho en la mesa redonda sobre las perspectivas de Latinoamérica y el Caribe (informe en el archivo con autores).

42 Posición nacional de Estonia (2018).

43 Consulte, por ejemplo, las posiciones nacionales de Austria (2024), pág. 4, Brasil (2021), pág.18, Dinamarca (2023), pág. 448-449 y Nueva Zelanda (2020), párr. 12.

44 Consulte la posición nacional de Estonia (2019).

45 Consulte, por ejemplo, las posiciones nacionales de Austria (2024), pág. 9, Canadá (2022), párr. 37, Costa Rica (2023), párr. 15, Francia (2021), pág. 4 e Irlanda (2023), párr. 26.

d. Marco nacional mejorado para la acción y mayor resiliencia cibernética

Formulación de los objetivos

Aunque los objetivos nacionales rara vez se expresan en las posiciones nacionales, en las mesas redondas del proyecto surgió que muchos Estados consideran el entendimiento más claro de la conducta permitida como un resultado esperado clave de desarrollar dicha posición. Este entendimiento más claro puede servir como marco para orientar las propias actividades cibernéticas de los Estados y las respuestas ante los incidentes cibernéticos. Este marco asegura que las acciones del Estado sean coherentes con el derecho internacional, y reduce el riesgo de consecuencias no intencionales.[46] La publicación de una posición nacional también ofrece a los actores nacionales un **punto de referencia** sobre el comportamiento esperado.

El desarrollo de una posición nacional puede tener como objetivo aumentar la **resiliencia cibernética** del Estado. Tener una posición nacional contribuye a mejorar la resiliencia y a la preparación para abordar las operaciones cibernéticas maliciosas. En este sentido, las posiciones nacionales y conjuntas permiten a los Estados calibrar sus respuestas, ya que en el proceso deben determinar, consolidar y clarificar sus perspectivas internas. Es más, trabajar el tema posiblemente mejore la **coordinación interinstitucional** sobre temas cibernéticos al crear líneas de comunicación, clarificar áreas de responsabilidad y movilizar a las partes interesadas clave de los gobiernos.

Aunque rara vez lo dicen explícitamente, muchos Estados consideran el desarrollo de posiciones nacionales como un medio para clarificar las conductas cibernéticas que son permisibles.

Motivaciones

The development of a national El desarrollo de una política nacional puede considerarse como una **verificación de la realidad**. Permite al Estado comprender mejor su preparación, identificar y entender los intereses de los diferentes actores nacionales, y descubrir los conceptos erróneos y desajustes. Aunque desarrollar una posición nacional es un ejercicio jurídico, las conversaciones con las partes interesadas dan forma al lenguaje, estructura y alcance del documento. Estas conversaciones también enriquecen las perspectivas jurídicas con argumentos técnicos y de política significativos, y pueden arrojar nuevas luces sobre las diferentes implicaciones de adoptar interpretaciones jurídicas. Un ejemplo de esto es debatir si un estándar de diligencia debida más alto es viable y realista, y si el Estado puede cumplirlo.[47]

46 Por ejemplo, consulte la posición nacional de Estados Unidos (2021), pág. 136.

47 Comentario hecho en la mesa redonda sobre las perspectivas de Latinoamérica y el Caribe (informe en el archivo con autores).

Además, aportar más claridad sobre cómo aplica el derecho internacional en el contexto cibernético implica **medidas nacionales correspondientes**, que pueden adoptar la forma de regulación.[48] Las partes interesadas nacionales también deben considerar su realidad y la aplicación del derecho. Como indicó un representante de un Estado, tener una posición nacional ayuda a garantizar que varias partes del aparato del Estado y otros actores no participen en actos que puedan constituir actos internacionalmente ilícitos.[49] Las posiciones nacionales sirven como un buen **punto de referencia** para que diversos órganos se comuniquen con sus contrapartes, pares y el público en general. Estas centralizan y alinean las expresiones relevantes a la conducta del Estado en el ciberespacio, y las partes interesadas toman la posición nacional como una orientación y limitación sobre declaraciones no coordinadas. Por lo tanto, el documento es útil para proporcionar asesoría jurídica concisa y para coordinar lo que se debe comunicar sobre los asuntos cibernéticos a nivel interno y externo.

Cuando ocurre un incidente cibernético, con frecuencia no hay suficiente tiempo para pensar en cómo aplica el derecho internacional. La **resiliencia y preparación cibernética** requieren tomar medidas por adelantado ante cualquier incidente.

Al establecer una posición nacional clara y coherente, los Estados pueden fortalecer sus marcos jurídicos y políticas internas, proporcionar una base sólida para la toma de decisiones en el complejo y a menudo ambiguo ámbito de las operaciones cibernéticas. El entorno digital es amplio y varios órganos gubernamentales tienen responsabilidades que abarcan diferentes aspectos del ciberespacio. Sin atención y esfuerzo especializado, los gobiernos no pueden tener el panorama completo ni darse cuenta de cuáles de sus órganos tienen las competencias y las capacidades. Desarrollar una posición nacional es una excelente oportunidad para **mapear** cómo funcionan las redes gubernamentales y qué se puede reunir en caso de crisis.[50] Es posible que también pueda traer cambios nacionales en los roles, competencias y procedimientos, al igual que la creación de escenarios probables para ejercicios de simulación y trabajo en opciones de respuesta potenciales. Esto es especialmente importante para construir resiliencia en tiempos de crisis.[51]

48 Comentario hecho en la mesa redonda sobre las perspectivas de Asia y el Pacífico (informe en el archivo con autores).

49 Comentario hecho en la mesa redonda sobre las perspectivas de Asia y el Pacífico (informe en el archivo con autores).

50 Comentario hecho en la mesa redonda sobre las perspectivas de Latinoamérica y el Caribe (informe en el archivo con autores).

51 Varios comentarios hechos en las tres mesas redondas del proyecto (informe en archivo con autores).

Además, para las partes interesadas nacionales que participan en el desarrollo de la posición nacional, la participación en la mesa es por sí misma un ejercicio de creación de capacidades. Las consideraciones internas y el proceso de redactar una posición nacional pueden reunir a los actores nacionales (por ejemplo, los que trabajan en defensa, cumplimiento de la ley o asuntos económicos) en un solo lugar para estudiar juntos los asuntos clave. Uno de los representantes de los Estados resumió que, 'El proceso en sí mismo tiene su valor'.[52]

4. Factores limitantes y riesgos

Aunque muchas de estas articulan algunas de sus motivaciones y razones de ser, las posiciones nacionales y conjuntas publicadas hasta la fecha típicamente **guardan silencio sobre los riesgos y limitaciones** del ejercicio. De nuevo, las razones para esto son altamente contextuales y difieren de país en país, dependiendo del clima económico, social y geopolítico y de los rasgos particulares del entorno nacional y externo.

Los Estados tienen **la libertad de permanecer en silencio** y elegir no desarrollar una posición nacional. Habiendo entendido la importancia y relevancia de hacerlo, muchos están en el proceso de producir una, y parece haber dos razones principales por las cuales los Estados (aún) no tienen una posición nacional: **falta de concienciación y capacidad**.

Asimismo, como surgió en las mesas redondas del proyecto, las preguntas clave también incluyen qué asuntos dejar por fuera y por qué; cómo priorizar varios asuntos; el nivel de detalle que se desea lograr, cómo lograr un acuerdo nacional sobre las divergencias; si se debe publicar el texto, cuándo y cómo hacerlo; y si se debe revisar una posición existente y cuándo hacerlo.

a. Falta de capacidad

La falta de capacidad debida a la escasez de recursos es una limitación importante que afecta las decisiones en todo el proceso de desarrollar una posición nacional. Hacerlo es un trabajo **complejo y que requiere muchos recursos**. Muchos (o la mayoría) de los Estados carecen de los recursos para hacerlo, o hacerlo eficazmente, al menos en algunos aspectos. Esto puede conducir a una nueva priorización del desarrollo de la posición nacional: incluso si todos los beneficios señalados en la sección anterior se comprenden, estos aún pueden ser superados por los asuntos que se perciben como más urgentes o importantes. Varios asuntos (como barreras de idioma, falta de conocimientos técnicos o jurídicos, costo prohibitivo de la

52 Comentario hecho en la mesa redonda sobre las perspectivas de Latinoamérica y el Caribe (informe en el archivo con autores) (Trad. libre).

participación, falta o desconocimiento del material de orientación y referencia, o las limitaciones del mismo, y la falta de coordinación y claridad sobre las competencias en el gobierno) pueden hacer que el desarrollo de una posición nacional parezca una tarea abrumadora. Por lo tanto, la decisión de desarrollarla inevitablemente será política. Sin embargo, rehusarse por completo a participar en el proceso tiene el riesgo de conceder una influencia desproporcionada sobre la interpretación del derecho internacional a otros Estados.

Muchos Estados también pueden desconocer o tener experiencia insuficiente en el proceso de reunir la práctica del Estado como un elemento del derecho internacional consuetudinario, lo que con frecuencia no está disponible públicamente. Del mismo modo, la necesidad de contar con una posición nacional o conjunta puede parecer distante si aún no se ha materializado un incidente cibernético a gran escala. Por lo tanto, los Estados se beneficiarían de **compartir** sus experiencias y ser transparentes sobre sus prácticas[53]

b. Ausencia de voluntad política

Algunos líderes gubernamentales pueden no ser conscientes o no reconocer la importancia de desarrollar una posición nacional sobre el derecho internacional en el contexto cibernético. Otros pueden carecer por completo de interés en vincularse con el derecho internacional. Como consecuencia, algunos Estados simplemente carecen de la voluntad política necesaria para desarrollar una posición nacional. Pero esto puede suponer el **costo** de no contribuir al desarrollo de la práctica del Estado como un elemento del derecho internacional consuetudinario en el contexto cibernético, y de no mantener el margen para ser un objetor persistente de la práctica de los demás.

La prudencia también se puede **explicar** por la cantidad limitada de Estados que han emitido hasta ahora posiciones nacionales, lo que puede conducir a renuencia a hacer lo mismo. De hecho, formular una posición significa que se necesita consideración cuidadosa desde el principio, ya que los Estados normalmente son renuentes a posteriormente alterar drásticamente su posición publicada sobre principios fundamentales como la prohibición del uso de la fuerza.[54] Sobre esta base, los Estados pueden sentir la necesidad de esperar hasta que la importancia del asunto aumente y se logre mayor claridad, manteniendo la flexibilidad para futuros debates.

Sin embargo, el desarrollo de posiciones nacionales no tiene que ser un ejercicio de una sola vez, y se entiende mejor como parte de un proceso, internamente y externamente, como parte del desarrollo del derecho internacional. Por lo tanto,

53 Comentario hecho en el taller y lanzamiento del proyecto en CyCon, 'Posición nacional sobre el derecho internacional en el ciberespacio: Desafíos, oportunidades y buenas prácticas', 28 de mayo de 2024, Tallin (informe en el archivo con autores).

54 Comentario hecho en la Semana Internacional Cibernética en Singapur en el panel 'Posiciones nacionales sobre el derecho internacional en el ciberespacio: Desafíos, oportunidades y buenas prácticas', 15 de octubre de 2024, Singapur (informe en el archivo con autores).

las posiciones nacionales no son necesariamente documentos finales, sino vivos, y los Estados pueden decidirse a revisarlos. Durante los eventos del proyecto, varios representantes de los Estados notaron que los Estados que han publicado su posición deberían estudiar las de los demás y revisar continuamente sus propias posiciones con miras a gradualmente llegar a entendimientos conjuntos o comunes.[55] Esto no necesariamente significa dar un giro en las interpretaciones sino construir sobre versiones anteriores y elaborar y clarificar ciertos asuntos, a medida que el entendimiento de los temas relevantes se profundiza y el debate madura.

c. No divulgación

Desarrollar una posición nacional no significa automáticamente que hay que divulgarla de inmediato o rápidamente. Los Estados no tienen que publicar sus posiciones por completo o en parte para obtener algunos de los beneficios de atravesar el proceso de desarrollarlas. Pueden elegir no priorizar la publicación de sus perspectivas por varias razones, como:

- Deseo de ser ágiles y no prematuros en el posicionamiento.
- Un enfoque conservador de esperar a que los demás presenten sus posiciones antes de divulgar la propia, y evitar confrontaciones geopolíticas innecesarias.
- La falta de disposición para comunicar ciertas opiniones, dejando sin revelar cuestiones delicadas, controvertidas o poco claras.
- Falta de confianza y abstenerse de tener debates francos.[56]

d. Omisiones estratégicas

El proceso de desarrollar una posición nacional o posición conjunta puede conducir a la decisión de omitir estratégicamente ciertos asuntos de la posición nacional, para continuar discutiéndolos internamente, y centrarse en asuntos sobre los que el Estado ya tiene una posición sólida y alta confianza. Por ejemplo, los Estados miembros de la UA decidieron no abordar asuntos como las inmunidades diplomáticas, la legalidad de las contramedidas y las condiciones para invocar el estado de necesidad en su posición conjunta, dadas las discrepancias sobre esas cuestiones.[57] Los Estados **no deben sentir que están presionados** a abordar todos los asuntos tratados en el **Capítulo 4** ni a abordarlos de inmediato.

Es más, puede que los Estados no quieran **revelar lo que piensan** más allá de cierto nivel de generalidad, y por lo tanto, limiten la profundidad del debate

55 Comentario hecho en el taller y lanzamiento del proyecto en CyCon, 'Posición nacional sobre el derecho internacional en el ciberespacio: Desafíos, oportunidades y buenas prácticas', 28 de mayo de 2024, Tallin (informe en el archivo con autores).

56 Comentario realizado en el Tercer Simposio Anual Presencial sobre Derecho Cibernético e Internacional, Conflicto Futuro: Convergencia del Derecho Internacional Cibernético y de la Información, en el panel sobre 'Perspectivas nacionales sobre el derecho internacional y los potenciales de convergencia', Universidad American, 24 de septiembre de 2024, Washington, DC (informe en archivo con autores)

57 Posición conjunta de la UA (2024), párr. 10.

en áreas sensibles, como el umbral requerido para calificar una conducta en el ciberespacio como un ataque armado. En cualquier caso, los Estados por necesidad son **selectivos** en términos de los asuntos que desean abordar, ya que no pueden tratarlos todos.[58] Es más, si ciertos temas se dejan sin abordar, existe el riesgo de que las partes interesadas puedan interpretar varias intenciones en el silencio del Estado o decidir interpretar el texto de maneras que no son la intención de los redactores. Finalmente, la importancia de un asunto para la comunidad internacional en épocas geopolíticamente difíciles también puede ser un factor que determina qué asuntos omitir. Con relación a esto, las mesas redondas del proyecto revelaron cierto grado de desconcierto sobre la atención modesta que las posiciones nacionales existentes prestan a asuntos clave como el arreglo pacífico de controversias o el derecho a la autodeterminación.[59] Para responder a esta necesidad, este manual cubre los dos asuntos con cierto detalle en el **Capítulo 4**.

e. Mantener la flexibilidad política y operativa

A los Estados les preocupa que sus declaraciones públicas los limiten. Ciertamente, en el ciberespacio, las circunstancias pueden cambiar rápidamente, ya que la tecnología se desarrolla a un ritmo que no pueden igualar las políticas ni el derecho. Por lo tanto, las posiciones nacionales no se diseñan para ser integrales ni exhaustivas, sino que, como señaló un representante de un Estado durante las mesas redondas del proyecto, ayudan a mitigar algunas preocupaciones y es posible que deban ser un *tanto* flexibles.[60]

Emitir declaraciones muy detalladas también puede ser contraproducente si el Estado no puede comportarse de acuerdo con los estándares que él mismo fija, lo que conlleva el riesgo de repercusiones políticas. En este sentido, permanecer en silencio puede ser considerado como una manera de evitar la rendición de cuentas. Otro inhibidor importante es la renuencia de los Estados a expresar su *opinio juris* porque esta puede carecer de flexibilidad para hacer ajustes posteriores. Esto puede conducir a la indecisión sobre la publicación de cualquier cosa que no sea una **declaración amplia y general**.[61] Aunque las declaraciones generales de todos modos pueden ser útiles, ser demasiado general puede ser considerado como la incapacidad de expresar un compromiso genuino de atenerse a las reglas del juego.

Conservar la ambigüedad constructiva y la flexibilidad operacional son razones clave por las que los Estados se abstienen de desarrollar una posición nacional. Las partes interesadas nacionales, especialmente las fuerzas armadas y los órganos

58 Comentario hecho en la mesa redonda sobre las perspectivas de Asia y el Pacífico (informe en el archivo con autores).

59 Comentario hecho en la mesa redonda sobre las perspectivas de Latinoamérica y el Caribe (informe en el archivo con autores).

60 Comentario hecho en la Semana Internacional Cibernética en Singapur en el panel 'Posiciones nacionales sobre el derecho internacional en el ciberespacio: Desafíos, oportunidades y buenas prácticas', 15 de octubre de 2024, Singapur (informe en el archivo con autores).

61 Comentario hecho en la mesa redonda sobre las perspectivas de Latinoamérica y el Caribe (informe en el archivo con autores).

de inteligencia, también pueden ver la clarificación de las reglas como una posible limitación de sus actividades y salir de la zona gris que les brinda ciertas ventajas y libertades, además de máximo espacio para maniobrar. Esto tiene el potencial de **crear fricciones** entre las partes interesadas nacionales, quienes pueden tener enfoques diferentes sobre las relaciones internacionales. Por ejemplo, los representantes de los Estados hicieron hincapié en que ciertos órganos gubernamentales tienen mentalidades más diplomáticas, mientras que otros están entrenados y piensan en términos de seguridad o estrategia militar. **Conciliar** estas perspectivas diversas puede ser un desafío significativo que necesita un debate franco y la disposición a hacer concesiones. También es importante tener en cuenta que la claridad sobre las reglas no solo limita, sino que **también protege** a quienes las obedecen.[62] Por ejemplo, muchos Estados pueden ser renuentes a aceptar la diligencia debida como una obligación vinculante, ya que puede ser difícil prevenir, detener o rectificar actividades en el ciberespacio cuando no se tiene control de la infraestructura.[63] Por otro lado, precisamente debido a las interdependencias de las infraestructuras cibernéticas, puede haber cierto apetito por parte de otros Estados de definir expectativas de diligencia debida.[64] Esta lógica no es diferente de aquella de la diligencia debida en el derecho medioambiental.[65]

f. Falta de consenso

El derecho internacional continúa evolucionando, y no hay un consenso claro sobre cómo se deben interpretar y aplicar reglas específicas en el contexto cibernético. Esto puede dificultar que los Estados desarrollen una posición nacional coherente. Para algunos, la falta de consenso puede dar lugar a **escepticismo** sobre dichas iniciativas, o crear dudas sobre la utilidad de tener una posición nacional o conjunta. Esto también puede disminuir el impulso o desanimar a los Estados, ya que no tienen seguridad sobre cómo las posiciones nacionales o conjuntas contribuyen al desarrollo del derecho internacional consuetudinario.[66]

Mientras que la falta de consenso puede considerarse un factor limitante, no precluye la articulación de las perspectivas jurídicas ni el progreso significativo en esa área. El sistema jurídico internacional ha funcionado mucho tiempo sin acuerdos universales sobre cada punto del derecho, y las **diferencias en las obligaciones jurídicas** entre Estados, como las variaciones en la membresía de los tratados, **son una característica bien arraigada** del sistema. En este contexto, el desarrollo de posiciones nacionales puede ayudar a clarificar entendimientos jurídicos, y con el tiempo, promover la convergencia, incluso en ausencia de un acuerdo completo.

La diversidad de las perspectivas existentes también puede incitar a algunos Estados a abogar por un nuevo instrumento jurídicamente vinculante, ya sea para

62 Comentario hecho en la mesa redonda sobre las perspectivas de Latinoamérica y el Caribe (informe en el archivo con autores).

63 Varios comentarios hechos en las tres mesas redondas del proyecto (informe en archivo con autores).

64 Comentario hecho en la mesa redonda sobre las perspectivas de Latinoamérica y el Caribe (informe en el archivo con autores).

65 Comentario hecho en la mesa redonda sobre las perspectivas de Asia y el Pacífico (informe en el archivo con autores).

66 Comentario hecho en la mesa redonda sobre las perspectivas de Latinoamérica y el Caribe (informe en el archivo con autores).

abordar las brechas percibidas o para armonizar las interpretaciones. Aunque esta opción permanece abierta, podría, como cualquier esfuerzo para crear un tratado, requiere de consenso significativo entre los Estados. Vale la pena recordar que en otras áreas del derecho internacional donde existen divergencias desde hace mucho tiempo, como en el derecho de la responsabilidad del Estado, los Estados siguen dependiendo del derecho internacional consuetudinario en vez de tratar de adoptar un tratado multilateral vinculante. Esto destaca la **complejidad** que tiene lograr un acuerdo sobre un instrumento vinculante e invita a mayor reflexión sobre el papel que pueden tener las posiciones nacionales en dar forma a las expectativas jurídicas y a fomentar entendimientos comunes en el contexto cibernético.

5. Conclusión

Es importante tener una percepción clara de ***por qué*** un Estado desarrolló o está desarrollando una posición nacional. Las posiciones nacionales tienen una función comunicativa al interactuar con los actores nacionales y externos pertinentes. También tienen una función transformadora para ayudar a brindar claridad y ajustar el marco jurídico existente a las nuevas realidades. A su vez, al expresar y clarificar la posición de los Estados, las posiciones nacionales cumplen una función preventiva, ya que reducen el riesgo de interpretaciones y errores de cálculo, y ayudan a establecer el estándar para evaluar la ilicitud de la conducta, así como las respuestas a las violaciones, lo que fomenta la disuasión. Las posiciones nacionales también fijan objetivos y resultados esperados, lo que puede formularse en términos prospectivos. Estos objetivos y resultados esperados por lo general incluyen mejorar la paz y seguridad internacional, fortaleciendo el orden jurídico internacional, logrando un entendimiento más claro entre las partes interesadas nacionales y contribuyendo a construir resiliencia cibernética.

Es importante tener una percepción clara de por qué un Estado desarrolló o está desarrollando una posición nacional.

La decisión de producir una posición nacional está **determinada por factores internos y externos**. Cada posición refleja las prioridades e inquietudes particulares del Estado en cuestión, con frecuencia informadas por las amenazas cibernéticas más urgentes que enfrenta. Sin embargo, cada Estado opera dentro de su propio conjunto de circunstancias que van desde su extensión territorial, población, economía o capacidades, hasta el grado de alineación interinstitucional, voluntad política y disponibilidad de recursos. La elección de no desarrollar una posición nacional puede estar influenciada por consideraciones jurídicas, políticas o económicas. Las mesas redondas del proyecto revelaron dos razones recurrentes para esta elección: falta de capacidad y de voluntad política. Sin embargo, también hay factores que limitan el contenido o el uso previsto de las posiciones nacionales, incluidos la falta de divulgación completa, el mantenimiento de la flexibilidad política y operacional o la ausencia de consensos internos.

Esto nos lleva al proceso mediante el cual se hace, que es el tema del próximo capítulo.

CAPÍTULO 3:

PROCESO

DE UN VISTAZO

Este capítulo describe los pasos prácticos para la preparación de una posición nacional. Destaca el valor de la coordinación temprana, la participación de todo el gobierno y un proceso de redacción estructurado. También considera quiénes deben participar, desde asesores jurídicos hasta partes interesadas externas, y cómo navegar las dinámicas interinstitucionales. Aunque el proceso de cada Estado será diferente, la claridad, la inclusividad y la planeación estratégica son aspectos clave. Este capítulo ofrece un mapa de ruta flexible que ayuda a los Estados a redactar posiciones nacionales coherentes, creíbles y adecuadas para el contexto.

1. Introducción

El proceso de desarrollar una posición nacional varía significativamente dependiendo del Estado, ya que no hay un modelo de aplicación universal para orientar cada caso. Sin embargo, por lo general hay ciertos elementos clave involucrados, incluso si la secuencia puede ser diferente: obtener el mandato, designar redactores, llevar a cabo la investigación de los recursos y prácticas existentes, consultar a las partes interesadas y redactar, adoptar y difundir la posición.

Conceptualmente, el desarrollo de una posición nacional está anclado al ciclo de política pública, pero está inherentemente entrelazado con las perspectivas del derecho internacional, lo que requiere la integración de consideraciones políticas, jurídicas y operacionales.

Como resultado, el proceso considera todas estas dimensiones.

Cada uno de estos pasos necesita recursos y capacidad institucional. La creación de capacidades sigue siendo un habilitador fundamental para todos los Estados, particularmente para los que tienen poca experiencia o marcos institucionales en esta área, para desarrollar y articular posiciones nacionales sobre cómo aplica el derecho internacional en el contexto cibernético.

Este capítulo comienza explorando brevemente la doble naturaleza política y jurídica del proceso antes de describir las etapas prácticas que los Estados pueden recorrer para desarrollar una posición nacional. Estas etapas incluyen identificar lo que podría motivar a embarcarse en el proceso; determinar las partes interesadas pertinentes y sus roles; la preparación, planificación e iniciación; la creación de capacidades; la realización de la investigación; el análisis y la redacción; la adopción y difusión, y finalmente, seguimiento, reflexión y revisión.

2. Posiciones nacionales en los procesos de política pública y jurídicos

La reciente tendencia de los Estados a desarrollar y publicar su posición nacional sobre la aplicación del derecho internacional en el contexto cibernético demuestra una **evolución gradual** de los esfuerzos para abordar las amenazas posibles y existentes relacionadas con el uso de las tecnologías de la información y comunicación (TIC).[1] El derecho internacional es una herramienta, junto con medidas de fomento de la confianza, mecanismos técnicos y otras intervenciones, que emplean los Estados para abordar los desafíos de la ciberseguridad. Desarrollar una posición nacional es, en el fondo, una respuesta política intencionada ante los problemas de ciberseguridad que afronta el Estado.

Por lo tanto, las posiciones nacionales son una parte inherente del **proceso de política pública**, ya que la legislación encarna los valores y las elecciones políticas en evolución. Formular una posición involucra abordar las preocupaciones de política nacional y exterior, al igual que las consideraciones del derecho internacional, ya que están inextricablemente vinculadas. Esta complejidad se ve agravada por la naturaleza técnica del dominio. Como resultado, el interrogante sobre cómo hacerla (tratado en este capítulo) con frecuencia es tan desafiante como lo que debe incluir (tratado en el **Capítulo 4**).

Existen una amplia bibliografía y modelos que capturan los mecanismos del proceso de la política pública.[2] Por lo general, el proceso se describe en etapas genéricas, como identificación del problema y agenda, formulación de políticas, toma de decisiones, implementación y evaluación. La orientación específica para cada campo, como los marcos para desarrollar estrategias nacionales de ciberseguridad,[3] puede brindar información importante para gestionar el proceso de desarrollo de política más amplio. Estas estrategias a menudo se refieren al derecho internacional, como se observa en el reconocimiento de Chile de que 'el desafío consiste principalmente en identificar e interpretar las normas relevantes del derecho internacional aplicables'.[4] De manera similar, la Estrategia de Ciberseguridad 2020 de la Unión Europea[5] comprometió al bloque a desarrollar una posición conjunta, que fue adoptada en 2024. Sin embargo, aunque dichas estrategias pueden ayudar a iniciar el proceso, generalmente carecen de orientación detallada sobre las tareas jurídicas involucradas, que requieren la experticia de profesiones en derecho. Desarrollar una posición nacional necesariamente se basa en metodologías jurídicas y procesos especializados del derecho.

1 Asamblea General de las Naciones Unidas, *Informe del Grupo de Expertos Gubernamentales sobre los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional*, A/68/98 (24 de junio de 2013), párr. 1 y 2.

2 Para ver un resumen de los principales enfoques y académicos, consulte Evangelia Petridou, 'Teorías sobre el proceso de las políticas' (2014) 42 *Policy Studies Journal* S12.

3 *Guía para desarrollar una estrategia nacional de seguridad*, segunda edición (2021).

4 Gobierno de Chile, *Política de ciberseguridad nacional*, (2017-2022), 22.

5 Comisión Europea, *La estrategia de ciberseguridad de la Unión Europea para la década digital* (2020), 20.

La tendencia a desarrollar y publicar posiciones nacionales exhaustivas es relativamente reciente. Con la recomendación repetida del Grupo de Trabajo de Composición Abierta (GTCA) de la ONU, hasta ahora más de 30 Estados han emitido posiciones nacionales y la cantidad sigue aumentando. Sin embargo, como varios representantes de los Estados resaltaron en el contexto de este proyecto, esta atención puede traer consigo expectativas sin precedentes. Los Estados pueden sentir presión para que se presente, en un solo documento, todo su entendimiento sobre cómo aplica el derecho internacional, lo que está a un nivel de exhaustividad rara vez visto en otros contextos.[6] La complejidad, junto con estas **nuevas expectativas**, presenta interrogantes importantes sobre cómo diseñar el proceso de desarrollo de una posición nacional y si para este fin sería más adecuada una combinación de diferentes métodos.

Estas observaciones tienen implicaciones significativas para el proceso de desarrollar una posición nacional. Primero, no existe un proceso universalmente válido que garantice el éxito. Sin embargo, ciertos elementos comunes han emergido de los procesos analizados durante la preparación de este manual. Segundo, dada la complejidad y naturaleza interdisciplinaria de este ejercicio, a menudo los Estados incorporan una **combinación de pasos y técnicas** usados en los procesos de política pública y de metodologías del derecho internacional. Tercero, las diferencias en las posiciones nacionales señalan que las interpretaciones de las reglas están entrelazadas con diferencias en los supuestos de política pública. Esto resalta el beneficio de emplear métodos empíricos y debates basados en escenarios en el proceso.

Las siguientes secciones exploran los elementos clave del proceso, reflexionando sobre las prácticas y desafíos existentes. Sin embargo, no es necesario seguir el orden de presentación de estos elementos. Cada Estado puede ajustar el proceso para alinearlo con su distribución de competencias, procedimientos administrativos y cultura institucional. Para ayudar a los funcionarios estatales a navegar este esfuerzo, el manual también incluye una lista de verificación concisa que enumera los pasos clave, consideraciones y buenas prácticas para desarrollar una posición nacional (consulte el **Anexo A**).

6 Comentario hecho en el taller y lanzamiento del proyecto en CyCon, 'Posición nacional sobre el derecho internacional en el ciberespacio: Desafíos, oportunidades y buenas prácticas', 28 de mayo de 2024, Tallin (informe en el archivo con autores).

3. Desencadenantes

Los Estados pueden verse motivados a empezar el desarrollo de una posición nacional debido a varios factores, aunque a veces puede ser desafiante incluso lograr poner el tema **en la agenda**. En algunos casos, un ataque cibernético significativo es un catalizador evidente,[7] así que las partes interesadas necesitan poca persuasión. Sin embargo, no siempre es necesario sufrir experiencias dolorosas para crear conciencia sobre el asunto.

En muchos casos, participar en debates internacionales motiva a los Estados a desarrollar una posición, o en algunos casos, a formalizar sus opiniones ya formadas.[8] Por ejemplo, los informes del Grupo de Trabajo de Composición Abierta (GTCA) repetidamente han alentado a los Estados a compartir sus perspectivas nacionales sobre cómo se aplica el derecho internacional al uso de las TIC,[9] haciendo que la presentación de dicho documento ante la ONU sea un objetivo tangible.[10] Luego de comprometerse a presentar una posición nacional en un foro internacional, los Estados pueden sentirse obligados a cumplir, para demostrar liderazgo y dar el ejemplo.[11]

Desarrollar una posición nacional también puede obedecer a la necesidad de apoyar los mensajes de disuasión o clarificar el marco jurídico que rodea las capacidades de ofensiva cibernética.

Por ejemplo, la Estrategia de Ciberseguridad 2016 de Australia reconoce públicamente la existencia de capacidades de ofensiva cibernética e indica que el Estado podría usarlas de conformidad con el derecho internacional.[12] Dicha declaración puede incitar a una articulación más detallada de cómo las reglas existentes se entienden al aplicarlas a las operaciones cibernéticas.

Las presiones nacionales también pueden influir. La crítica de la academia o la sociedad civil sobre la inacción percibida del Estado puede priorizar el tema en

7 Comentario realizado en el Tercer Simposio Anual Presencial sobre Derecho Cibernético e Internacional, Conflicto Futuro: Convergencia del Derecho Internacional Cibernético y de la Información, en el panel sobre 'Navegando por la dinámica jurídica: perspectivas nacionales sobre el derecho internacional y las posibilidades de convergencia', Universidad Americana, 24 de septiembre de 2024, Washington, DC (informe en archivo con autores).

8 Comentario hecho en la mesa redonda sobre las perspectivas de Asia y el Pacífico (informe en el archivo con autores).

9 Consulte, por ejemplo, Asamblea General de la ONU, *Informe del Grupo de Trabajo de Composición Abierta sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional Informe sustantivo final*, A/AC.290/2021/CRP.2 (10 de marzo de 2021), párr. 38; Asamblea General de la ONU *Informe del Grupo de Trabajo de Composición Abierta sobre la seguridad y el uso de las tecnologías de la información y comunicación 2025*, A/77/275 (8 de agosto de 2022), párr. 15; Asamblea General de la ONU, *Informe del Grupo de Trabajo de Composición Abierta sobre la seguridad y el uso de las tecnologías de la información y comunicación 2021 a 2025*, A/78/265 (1 de agosto de 2023), párr. 33; Asamblea General de la ONU, *Informe del Grupo de Trabajo de Composición Abierta sobre la seguridad y el uso de las tecnologías de la información y comunicación 2021 a 2025*, A/79/214 (22 de julio de 2024), párr. 40.

10 Comentario hecho en la mesa redonda sobre las perspectivas de Asia y el Pacífico (informe en el archivo con autores).

11 Comentario hecho en la mesa redonda sobre las perspectivas de Asia y el Pacífico (informe en el archivo con autores).

12 Gobierno de Australia, *Estrategia de Ciberseguridad de Australia* (2016), 28.

la Comentario realizado en el Tercer Simposio Anual Presencial sobre Derecho Cibernético e Internacional, Conflicto Futuro: Convergencia del Derecho Internacional Cibernético y de la Información, en el panel sobre 'Navegando por la dinámica jurídica: perspectivas nacionales sobre el derecho internacional y las posibilidades de convergencia', Universidad Americana, 24 de septiembre de 2024, Washington, DC (informe en archivo con autores). agenda política.[13] Alternativamente, los Estados pueden verse abocados a iniciar el proceso debido a la necesidad de implementar una estrategia de ciberseguridad, como se observa en el caso de la Unión Europea.[14] Algunas posiciones nacionales implican lo que motivó su desarrollo (o consolidación), y pocas hacen referencia explícita a esos motivadores. Por ejemplo, la posición nacional de Japón indica que 'fue preparada como una contribución nacional a solicitud del Presidente del Grupo de Expertos Gubernamentales de la ONU (GEG)'.[15] El desarrollo de una posición nacional también puede ser motivado por políticas más generales, por ejemplo, la posición nacional de Polonia señala que es 'una continuación natural de la membresía no permanente de dos años de Polonia en el Consejo de Seguridad (2018 a 2019), donde el tema del respeto por el derecho internacional fue una de las prioridades de Polonia'.[16]

Estos desencadenantes han sido importantes para crear conciencia, orientar la asignación de roles en el proceso y asegurar el mandato necesario para iniciar los pasos preliminares.

Figura 1: Posibles desencadenantes para el desarrollo de una posición nacional.

13 Comentario hecho en la mesa redonda sobre las perspectivas de Latinoamérica y el Caribe (informe en el archivo con autores).

14 Comisión Europea, *La estrategia de ciberseguridad de la Unión Europea para la década digital* (2020), 20.

15 Posición nacional de Japón (2021), pág. 1 (Trad. libre).

16 Posición nacional de Polonia (2022), pág. 1 (Trad. libre).

4. Partes interesadas y roles

A medida que aumenta la conciencia sobre la importancia y los desafíos de aplicar el derecho internacional en el contexto cibernético, también lo hace la cantidad de partes interesadas involucradas en el desarrollo de las posiciones nacionales. Lo que empezó como un debate más cerrado ahora incluye **una amplia gama de voces**. Mapear a las partes interesadas y clarificar sus roles es un paso clave del proceso. Generalmente, las partes interesadas incluyen órganos gubernamentales, consultores, actores de la sociedad civil y académicos, cada uno con diferentes niveles de influencia.

Los Estados deben intentar conformar un equipo multidisciplinario que incluya expertos en los campos **jurídicos, políticos y técnicos**. Esto se debe a que el desarrollo de una posición nacional requiere una comprensión matizada de las tres dimensiones que se intersecan: marcos jurídicos (lo permitido y lo prohibido), implicaciones estratégicas de las decisiones políticas (lo que se prefiere) y las realidades técnicas del ciberespacio (lo que es posible). En últimas, una posición nacional debe tener un equilibrio entre las tres.

Figura 2: Composición del equipo redactor

Es importante **identificar qué órganos** tienen que participar en el proceso, quién tiene la suficiente autoridad para interactuar en el proceso y/o adoptar la posición, y las competencias que pueden aportar.[17] En algunos casos, esto puede ser sencillo, por ejemplo, cuando la legislación confiere la autoridad para interpretar el derecho internacional a determinado órgano. Más a menudo, varios órganos tienen intereses en el proceso, incluidos los que manejan, por ejemplo, seguridad nacional, asuntos económicos, infraestructura y datos digitales, defensa, asuntos exteriores, cuestiones jurídicas y comunicaciones.[18]

Algunos Estados pueden considerar que es adecuado involucrar a varios órganos, por ejemplo, uno con competencias respecto al derecho internacional y otro con la experticia técnica. En algunos casos, como lo explicó un experto gubernamental, 'la decisión sobre a quiénes involucrar y quién lidera fue tomada orgánicamente'.[19] En otros casos, la decisión se toma a nivel central y los roles se asignan mediante canales formales. Sin importar qué organismo asuma el liderazgo, es fundamental crear conciencia entre las instituciones pertinentes, particularmente las que inicialmente no consideran el asunto como una prioridad.[20] Durante las mesas redondas del proyecto, representantes de los Estados repetidamente enfatizaron en la necesidad de contar con **apoyo político** amplio, porque sin este, el proyecto corre el riesgo de estancarse, o incluso de quedar incompleto.

Las posiciones nacionales tienen impacto en el trabajo y los límites de los órganos técnicos y operacionales. Estas son entidades cuyas actividades pueden calificar como práctica del Estado y que tienen la experiencia práctica y la información de las operaciones cibernéticas. Por esto, su aporte puede orientar significativamente el desarrollo de las posiciones nacionales. Los expertos técnicos y órganos tales como los equipos de respuesta ante emergencias informáticas, los equipos de respuesta ante incidentes de seguridad informática y los centros de operaciones de seguridad tienen un papel fundamental, particularmente en el análisis de los efectos de las operaciones cibernéticas a nivel nacional e internacional. Estos órganos por lo general tienen la responsabilidad de detectar, responder y mitigar los incidentes cibernéticos, mientras que también interactúan con sus contrapartes internacionales. Con frecuencia tienen **información crítica** sobre las operaciones cibernéticas atribuibles a los Estados, aunque dicha información puede ser técnicamente compleja, clasificada o de otra forma inaccesible para

Los aportes de las agencias técnicas y operacionales pueden orientar significativamente las posiciones nacionales y esas posiciones, a su vez, influenciar su trabajo.

17 Comentario hecho en la mesa redonda sobre las perspectivas de Latinoamérica y el Caribe (informe en el archivo con autores).

18 Comentario hecho en la mesa redonda sobre las perspectivas de Asia y el Pacífico (informe en el archivo con autores).

19 Comentario hecho en la mesa redonda sobre las perspectivas de Asia y el Pacífico (informe en el archivo con autores) (Trad. libre).

20 Comentario hecho en la mesa redonda sobre las perspectivas de Latinoamérica y el Caribe (informe en el archivo con autores).

los profesionales jurídicos. Dependiendo de cómo se distribuyan las capacidades y competencias, lo mismo puede ser cierto para los órganos operacionales, como los servicios de inteligencia y los órganos de cumplimiento de la ley, que a menudo tienen **acceso de primera mano a los datos sobre las actividades cibernéticas** de varios actores, incluidos los Estados. Sucede lo mismo con relación a la información que controlan las agencias de defensa y las fuerzas armadas, que pueden tener información valiosa sobre las operaciones cibernéticas. Involucrar a todos estos actores en el proceso, al menos a nivel consultivo, puede contribuir a garantizar que las posiciones nacionales estén informadas por realidades operativas y reflejen un enfoque nacional coherente, especialmente en cuestiones en las que se entrecruzan consideraciones jurídicas, técnicas y militares.

Uno de los roles más influyentes del proceso es el de **redactor**. Aunque la redacción de una posición nacional es un esfuerzo de equipo que involucra actores del gobierno, y en ocasiones, externos a este,[21] la designación de uno o más redactores especializados es fundamental. Son responsables de liderar el proceso jurídico, redactar el texto inicial y garantizar que el producto final sea claro, coherente y refleje el consenso de todas las partes involucradas.

Es importante tener presente que el redactor no siempre es el organismo líder ni el líder político del proceso de desarrollo. Si el organismo líder también es el redactor, posiblemente oriente el contenido de la conversación. Sin embargo, si los dos roles son separados, el organismo líder probablemente tenga control político y la autoridad para la toma de decisiones finales mientras que garantiza los aportes técnicos y jurídicos de las instituciones que lo apoyan. En un tercer modelo, el organismo que sirve como redactor puede tener un apoyo fuerte de organizaciones internacionales o expertos externos para la coordinación y avance del proceso (en algunos casos, los expertos externos incluso han sido encargados de producir el primer borrador de la posición).

Algunos participantes de las mesas redondas indicaron que designar uno o más redactores y un organismo líder puede conducir a **competencia**, e incluso a guerra de influencias entre las instituciones. En contraposición, otros afirmaron que ciertos órganos pueden ser **renuentes** a asumir el rol de redactor, llevando a una situación donde la tarea 'pertenece a todos, y a nadie'.[22] Para evitar esto, la elección de redactor y organismo líder debe hacerse temprano en el proceso y deben tener competencias fuertes en derecho internacional y la capacidad para manejar la coordinación, negociación y compromiso necesarios para impulsar el proceso. De igual manera, el organismo líder por lo general tendrá que coordinar e interactuar con las otras partes interesadas involucradas en el proceso para buscar concesiones.

21 Comentario hecho en la mesa redonda sobre las perspectivas de Asia y el Pacífico (informe en el archivo con autores).

22 Comentario hecho en la mesa redonda sobre las perspectivas de Asia y el Pacífico (informe en el archivo con autores) (Trad. libre).

Cuando llega este momento, depende de cómo está diseñado el proceso y la madurez de la conversación sobre cibernética en el Estado.

Algunas posiciones nacionales se destacan por su estructura y enfoque. Un ejemplo es la posición nacional de Francia de 2019, que dedica atención considerable al derecho internacional humanitario (DIH) mucho más que la mayoría de las otras.[23] Es posible que esto indique el hecho de que la posición fue producida por el Ministerio de Fuerzas Armadas, y muestra que el redactor y/o el organismo líder tenía una amplia experticia en el derecho aplicable en tiempos de conflicto armado.[24]

Como las competencias y roles relacionados con el derecho internacional con frecuencia son de ellos, los ministerios de asuntos exteriores son frecuentemente los primeros promotores de la política y el proceso. Sin embargo, puede que no haya un solo organismo líder para el derecho internacional.[25] En algunos Estados, las **competencias en derecho internacional** pueden estar en dos o más órganos y las responsabilidades pueden ser compartidas, mientras que en otros casos puede haber solo un organismo (o ninguno) que tenga el conocimiento y la experiencia necesarios. Es más, muchas partes interesadas que participan en el proceso pueden carecer de formación jurídica, y mucho menos experticia en derecho internacional. En cualquier caso, el organismo líder debe poder explicar la importancia de una posición nacional a las demás partes interesadas, lo que incluye cómo las decisiones sobre la aplicación del derecho internacional a las actividades cibernéticas pueden afectarlas. Sin embargo, esto es una calle de doble sentido; tiene la misma importancia que los órganos operacionales expliquen lo que hacen como que los expertos jurídicos y en política tengan un buen entendimiento de la práctica y no se alejen de la realidad.

El organismo líder debe tener la capacidad para explicar la importancia de la posición nacional a las demás partes interesadas. Los órganos operacionales deben explicar lo que hacen, para que los expertos jurídicos y en política tengan un buen entendimiento de la práctica y no se alejen de la realidad.

23 Posición nacional de Francia (2019), pág. 12 a 16.

24 Comentario hecho en la mesa redonda sobre las perspectivas de Asia y el Pacífico (informe en el archivo con autores).

25 Comentario hecho en la mesa redonda sobre las perspectivas de Asia y el Pacífico (informe en el archivo con autores).

Dada la escasez de experticia relevante, las **redes informales** tienen un papel importante. Por ejemplo, la participación en los debates del Grupo de Expertos Gubernamentales (GEG) o las consultas del Manual de Tallin han ayudado a los Estados a construir capacidad y les ha permitido acudir a esas redes al redactar su posición.[26] Por lo tanto, crear y participar en redes informales permite a los Estados tener acceso a un recurso muy valioso y abordar sus debilidades. Sin embargo, la contratación de expertos y consultores externos puede requerir acuerdos formales y enfrentarse a restricciones, como asuntos de seguridad o límites en las comunicaciones externas.[27]

Muchos de los representantes de los Estados consultados para la elaboración de este manual enfatizaron el **rol de la participación pública** en el desarrollo de las posiciones nacionales.[28] Esto puede crear conciencia, ofrecer nuevas reflexiones, legitimar el producto final y aumentar la receptividad de la posición en la sociedad. En algunos Estados, puede que incluso sea un requisito de ley involucrar al público. En otros casos, esto se puede hacer de manera más informal.[29] Como anotó un representante, el rol de gobierno se puede limitar a coordinar las posiciones y opiniones de los sectores relevantes, donde el Ministerio de Asuntos Exteriores actúa como una especie de vocero.[30] En este caso, la inclusividad es una prioridad muy alta.

Sin embargo, la inclusión también puede complicar el proceso, y posiblemente ocasionar retrasos en la finalización de la posición nacional. También presenta el interrogante de cuándo dirigirse al público para permitir que primero los órganos involucrados piensen y no revelen información delicada prematuramente. Aunque, en principio, las consultas son deseables, no fueron una característica prevalente en el desarrollo de las posiciones nacionales existentes.[31] Como mínimo, las consultas deben involucrar a las partes interesadas clave, incluso si el público en general no participa.

Finalmente, no se debe pasar por alto el rol de los **emprendedores de política**. Estos pueden ser personas altamente motivadas, visionarios o académicos especializados que asumen y habilidosamente promueven la agenda para desarrollar una posición. Estas personas pueden aportar beneficios significativos al proceso en términos de liderazgo, experticia específica en el campo, y, sencillamente, lograr que las cosas sucedan.

---

26 Comentario hecho en la mesa redonda sobre las perspectivas de Latinoamérica y el Caribe (informe en el archivo con autores).

27 Comentario hecho en la mesa redonda sobre las perspectivas de África (informe en el archivo con autores).

28 Varios comentarios hechos en las tres mesas redondas del proyecto (informe en archivo con autores).

29 Comentario hecho en la mesa redonda sobre las perspectivas de Asia y el Pacífico (informe en el archivo con autores).

30 Comentario hecho en la mesa redonda sobre las perspectivas de Asia y el Pacífico (informe en el archivo con autores).

31 Varios comentarios hechos en las tres mesas redondas del proyecto (informe en archivo con autores).

5. Preparación, planificación e inicio

Los preparativos para el desarrollo de una posición nacional pueden empezar poniendo el asunto en la agenda, o con esfuerzos para persuadir a los tomadores de decisiones de hacerlo (consulte la **Sección 3** de este capítulo). Durante las etapas preliminares, se deben tener en cuenta los roles y la autoridad, lo que incluye identificar un organismo líder (consulte la **Sección 4** de este capítulo). Depende de las condiciones específicas de cada Estado si esto sucede antes, en paralelo o después del inicio formal del proceso y la asignación del mandato al organismo responsable.

En la **fase de preparación y planificación** se deben clarificar varios detalles clave. Entre estos está la definición del alcance que tendrá la posición nacional, quién estará involucrado y en qué rol, y cómo será el proceso (es decir, los pasos que se tomarán y en qué secuencia, al igual que el cronograma).[32] Aunque algunos representantes de los Estados promovieron un enfoque proactivo (simplemente tomar el bolígrafo y preparar un esquema inicial),[33] esto puede no alinearse con la cultura burocrática de todos los Estados.[34]

Una herramienta metodológica para la preparación y planificación de proyectos es el marco de las 5 preguntas clave: **¿Quién? ¿Qué? ¿Por qué? ¿Cuándo? ¿Dónde? ¿Cómo?** Cada categoría obliga a preguntarse interrogantes esenciales para orientar el proceso:

¿Quién?	Partes interesadas clave, incluidos tomadores de decisiones, expertos, autoridades, otros participantes, etc.
¿Qué?	Alcance, características, entregables, resultados, eventos, recursos, etc.
¿Por qué?	Objetivos, motivaciones, consideraciones políticas y jurídicas, etc.
¿Cuándo?	Etapas, hitos, fechas límite, etc.
¿Dónde?	Ubicación física y virtual de recursos, eventos, etc.
¿Cómo?	Métodos, proceso, procedimientos, planes, puntos de referencia, monitoreo, asignación de recursos, etc.

32 UNIDIR, *Compendio de buenas prácticas: Desarrollo de una posición nacional sobre la interpretación del derecho internacional y el uso de las TIC por los Estados* (2024), 17 a 18.

33 Comentario hecho en la mesa redonda sobre las perspectivas de Latinoamérica y el Caribe (informe en el archivo con autores).

34 Comentario hecho en la mesa redonda sobre las perspectivas de Latinoamérica y el Caribe (informe en el archivo con autores).

Al **principio**, se deben establecer los puntos de referencia y las presunciones necesarias, como que el derecho internacional aplica a la conducta cibernética y que la posición abordará cómo. Es importante tener claro el 'porqué' al desarrollar la posición nacional. El alcance y la naturaleza de la tarea (así como el resultado esperado) deben determinarse cuidadosamente, ya que esto dará forma a los requisitos institucionales. La interpretación del derecho internacional puede recaer en la competencia exclusiva de un determinado órgano, y puede que la emisión de una declaración formal tenga que ser aprobada por el organismo correspondiente, como el gabinete, lo que puede afectar las fechas límite, procedimientos y otros elementos del plan.

Al principio, definir el **alcance** de una posición nacional puede ser una tarea difícil. Como se discute en el **Capítulo 4**, muchas áreas del derecho internacional son pertinentes a las TIC. Pero estas deben ser priorizadas de acuerdo con las necesidades e intereses actuales del Estado. En este contexto, algunos representantes de los Estados destacaron la importancia de temas transversales como el uso de Internet y el impacto de las tecnologías emergentes en la paz internacional, mientras que otros señalaron el asunto de contrarrestar los discursos de odio, la discriminación en línea y la hostilidad y violencia en las redes sociales.[35] Otras estrategias para abordarlos incluyen empezar con lo más alcanzable, como la Carta de las Naciones Unidas o interrogantes menos controversiales antes de abordar los temas más difíciles.[36]

La planificación debe equilibrar los **recursos disponibles**. Es importante evaluar cómo hacer el mejor uso posible de los recursos limitados del Estado para producir una posición nacional adecuada. Estos recursos incluyen tiempo, personal y financiamiento de elementos como equipos, suministros, consultores externos, documentación y telecomunicaciones. La escasez de recursos puede afectar el modo de organización de los debates relevantes a nivel nacional, regional e internacional. Puede ser necesario utilizar diferentes estrategias para maximizar los recursos y el pensamiento creativo. Para abordar la falta de recursos, las estrategias creativas pueden incluir:

- Involucrar pasantes y voluntarios.
- Involucrar a la comunidad académica nacional y a expertos de la industria.
- Solicitar subvenciones y buscar oportunidades de financiamiento.
- Colaborar con organizaciones regionales.
- Participar en cursos, mesas redondas, seminarios y conferencias (presenciales o a distancia).
- Aprovechar los recursos que están disponibles sin costo y los proyectos internacionales existentes.

35 Comentario hecho en la mesa redonda sobre las perspectivas de África (informe en el archivo con autores).

36 Comentarios hechos en las mesas redondas sobre las perspectivas de Asia, Pacífico, Latinoamérica y el Caribe (informe en el archivo con autores).

La duración del proceso de desarrollo de una posición nacional puede ir desde meses hasta años, dependiendo de la complejidad de los temas y la capacidad del Estado. Sin embargo, durante las mesas redondas del proyecto surgió que esto no se puede considerar como un esfuerzo de una sola vez, y que las posiciones pueden y deberían ser revisadas y actualizadas periódicamente para que reflejen los nuevos desarrollos en las políticas nacionales, regionales y multilaterales, al igual que en el derecho internacional y el entorno cibernético en evolución. Para garantizar el desarrollo oportuno de la posición nacional, se deben definir cronogramas con fechas límite concretas. El objetivo es manejar el proceso con eficiencia, lo que incluye el tiempo necesario para las consultas y revisiones internas y externas, y la aprobación definitiva.

6. Creación de capacidades

Para desarrollar eficientemente una posición nacional sobre el derecho internacional y las actividades cibernéticas, es fundamental **mejorar** las capacidades de todas las partes interesadas pertinentes. Esto involucra desarrollar experticia jurídica y técnica para garantizar que haya un entendimiento exhaustivo del derecho internacional y su aplicación a las TIC. Las actividades de creación de capacidades pueden incluir ejercicios, talleres, programas de capacitación y conferencias, y se benefician mucho de la colaboración a niveles bilaterales, regionales e internacionales. Estas actividades deben cumplir los **principios de creación de capacidades** acordados por el GTCA de 2019 a 2021.[37] Estos están divididos en tres categorías relacionadas con proceso y finalidad, alianzas y personas.

a. Proceso y propósito

- El desarrollo de la capacidad debe ser un proceso sostenible y comprender actividades específicas por y para distintos agentes.
- Determinadas actividades deben tener un objetivo claro y centrarse en el logro de resultados y, al mismo tiempo, apoyar el objetivo común de establecer un entorno de la TIC abierto, seguro, estable, accesible y pacífico.
- Las actividades de desarrollo de la capacidad deben contar con una base empírica y ser políticamente neutrales, transparentes, responsables e incondicionales.
- El desarrollo de la capacidad debe llevarse a cabo respetando plenamente el principio de la soberanía de los Estados.
- Es posible que deba facilitarse el acceso a las tecnologías pertinentes.

37 Asamblea General de las Naciones Unidas, *Informe del Grupo de Trabajo de Composición Abierta sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional*, A/75/816 (18 de marzo de 2021), párr. 56.

b. Alianzas

- El desarrollo de la capacidad debe basarse en la confianza mutua y en la demanda, corresponder a unas necesidades y prioridades determinadas a nivel nacional y llevarse a cabo reconociendo plenamente la implicación nacional. Los aliados deben participar voluntariamente.
- Dado que las actividades de desarrollo de la capacidad deben adaptarse a necesidades y contextos específicos, todas las partes son asociados activos en ellas, con responsabilidades compartidas pero diferenciadas, en particular las de colaborar en el diseño, la ejecución, el seguimiento y la evaluación de dichas actividades.
- Todos los asociados deben proteger y respetar la confidencialidad de las políticas y los planes nacionales.

c. Personas

- El desarrollo de la capacidad debe respetar los derechos humanos y las libertades fundamentales, tener en cuenta las cuestiones de género y ser inclusivo, universal y no discriminatorio.
- Debe garantizarse la confidencialidad de la información sensible.

La creación de capacidades sigue siendo un **desafío** para la mayoría de los Estados, incluso para los que tienen experticia avanzada, ya que la tecnología se desarrolla rápidamente y los debates siguen ampliándose. Esto no pretende sugerir que la creación de capacidades debe ser uniforme. Algunos Estados ahora tienen un conocimiento profundo y equipos de expertos que están disponibles inmediatamente para desarrollar o revisar su posición nacional y pueden actuar como donantes para la creación de capacidades. Puede que otros Estados tengan capacidades fuertes, como en derecho internacional general y algunos regímenes especializados, en cuyo caso, los esfuerzos de creación de capacidades deben centrarse en asuntos más específicos de la cibernética. Sin embargo, en algunos casos, puede ser necesario emplear un enfoque más integral para la creación de capacidades.

También es importante tener en cuenta que la mera presencia de profesionales calificados no necesariamente se traduce en una capacidad efectiva al interior de los órganos gubernamentales. Lo que importa es si la experticia relevante está disponible para los funcionarios directamente involucrados en el desarrollo de la posición nacional del Estado y si ellos están equipados para entender y abordar los desafíos legales y políticos relacionados. Esto tiene una particular importancia, dado que los expertos y diplomáticos pueden ser reasignados, rotar en sus cargos, o dejar por completo el servicio público: por lo tanto, el mismo grupo de competencias no siempre estará **disponible constantemente** en el órgano.

A menudo, familiarizarse con este campo también requiere cierto grado de **capacitación técnica**.[38] Después de todo, el dominio cibernético es un entorno hecho por el ser humano basado en técnicas y estándares de ingeniería, pero sus impactos son amplios, y afectan a las sociedades y a la vida cotidiana de maneras tangibles e intangibles. Muchos de los interrogantes jurídicos en este campo dependen del entendimiento de detalles específicos de la tecnología.

Los Estados deben promover activamente iniciativas de creación de capacidades para todas las partes interesadas involucradas en el desarrollo de su posición nacional, pero hay necesidad de priorizar los órganos líderes y partes interesadas clave. El desarrollo de una posición nacional y la creación de capacidades **van de la mano**. De hecho, la creación de capacidades es un paso necesario para garantizar que la posición esté fundamentada, sea integral y esté alineada con las realidades del dominio cibernético.

La variedad y éxito de las iniciativas de creación de capacidades a nivel global, regional y nacional son una demostración de los beneficios de las experiencias compartidas y de la participación con partes interesadas no estatales, como la academia y la sociedad civil. Entender los debates actuales del campo también puede ayudar a los Estados a detectar los asuntos que quieren cubrir en su posición nacional y las perspectivas que desean tomar sobre estos.[39]

38 Comentario hecho en la mesa redonda sobre las perspectivas de Latinoamérica y el Caribe (informe en el archivo con autores).

39 Comentario hecho en la mesa redonda sobre las perspectivas de Asia y el Pacífico (informe en el archivo con autores).

El GTCA ha puesto un énfasis particular en la creación de capacidades, que es uno de los elementos centrales de su mandato. En la ONU hay **programas e iniciativas en el campo de la creación de capacidades cibernéticas**, y ejemplos recientes (pero generales) son la Mesa Redonda Mundial 2024 sobre creación de capacidades sobre las TIC,[40] que cubrió una serie de temas, incluso más allá del derecho internacional y las posiciones nacionales, o el Portal Global de cooperación y creación de capacidades en materia de seguridad de las tecnologías de la información y las comunicaciones propuesto.[41] En 2023, la Secretaría de las Naciones Unidas llevó a cabo un ejercicio de mapeo para inventariar los esfuerzos de creación de capacidades en seguridad de las TIC.[42] Los Estados, la academia y actores de la sociedad civil enviaron docenas de presentaciones, muchas de las cuales enumeraban las iniciativas y proyectos relacionados con la creación de capacidades sobre el derecho internacional en el contexto cibernético. Estas están disponibles en la base de datos documental del GTCA sobre seguridad y uso de las tecnologías de la información y la comunicación.[43] Con base en este ejercicio de mapeo, la Secretaría de la ONU compiló un documento que resume las iniciativas de creación de capacidades clave por área temática de enfoque, incluido el derecho internacional.[44]

Algunos ejemplos de dichas iniciativas dedicadas al derecho internacional son:

i. **Cyber Law Toolkit:**[45] El *Cyber Law Toolkit* es un recurso al que se puede acceder a nivel global desarrollado por un consorcio que incluye la Agencia Nacional Checa de Seguridad Cibernética e Información, el Comité Internacional de la Cruz Roja (CICR), el Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN, la Universidad de Exeter, la Escuela de Guerra Naval de los Estados Unidos y la Universidad de Wuhan. Disponible de forma gratuita para todo el mundo, incluidos funcionarios del gobierno y profesionales del derecho, al momento de redactar este documento, el kit de herramientas incluye:

   a. Un número cada vez mayor de escenarios (actualmente 32) que exploran las aplicaciones del derecho internacional a las operaciones cibernéticas.

   b. Una base de datos de las posiciones nacionales sobre la aplicación del derecho internacional en el contexto cibernético existentes.

   c. Un repositorio de ejemplos que actualmente cuenta con 70 incidentes cibernéticos.

40 La Mesa Redonda Mundial 2024 sobre creación de capacidades sobre las TIC llevada cabo en Nueva York el 10 de mayo de 2024, fue el primer evento organizado bajo el auspicio de las Naciones Unidas dedicado al tema de la creación de capacidades. Consulte el informe relacionado: Giacomo Persi Paoli, Samuele Dominioni, Aamna Rafiq y Lenka Filipová, *Acelerar la creación de capacidades en seguridad de las TIC: Puntos clave de la Mesa Redonda Mundial sobre las Capacidades en Seguridad de las TIC*, UNIDIR, Ginebra (2024).

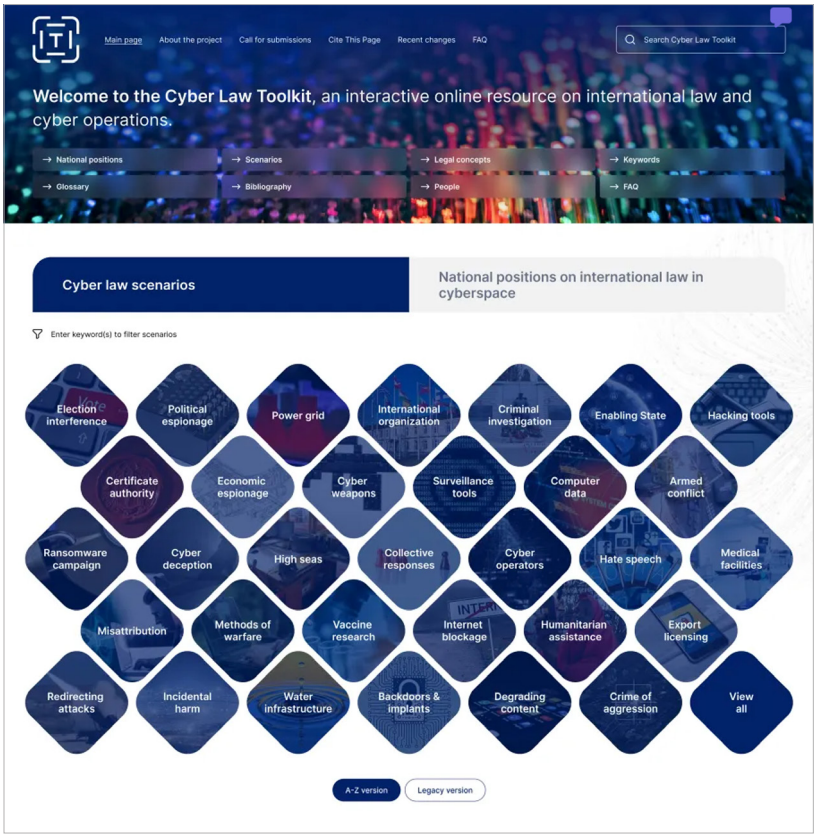
41 Consulte Asamblea General de las Naciones Unidas, *Informe inicial sobre la propuesta para diseñar y poner en funcionamiento un portal mundial de cooperación y creación de capacidad en materia de seguridad de las tecnologías de la información y las comunicaciones I*, A/AC.292/2025/1 (14 de enero de 2025).

42 Secretaría de las Naciones Unidas, *ODA/2023-00042/ICT-Mapping Exercise* (2 de octubre de 2022).

43 GTCA, Grupo de Trabajo de Composición Abierta sobre las tecnologías de la información y comunicación, *documentos*.

44 Asamblea General de la ONU, *Análisis para estudiar el panorama de los programas e iniciativas de creación de capacidad dentro y fuera de las Naciones Unidas y a escala mundial y regional*, A/AC.292/2024/2 (22 de enero de 2024).

45 Consulte https://cyberlaw.ccdcoe.org.



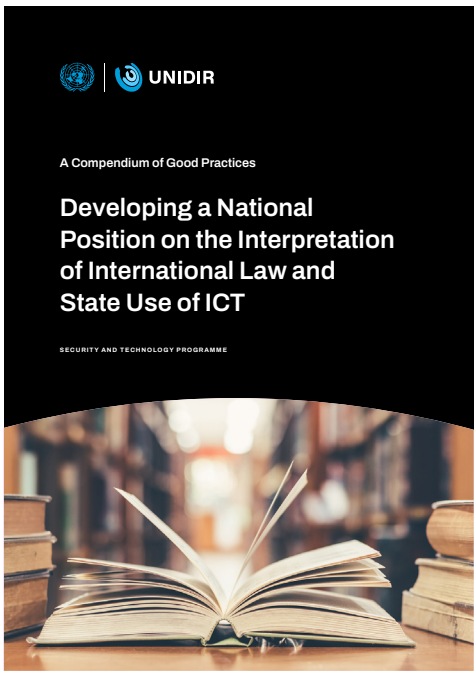
ii. **El Proceso de Oxford sobre las protecciones del derecho internacional en el ciberespacio:** lanzado en 2020 por el Instituto de Ética, Derecho y Conflicto Armado de Oxford en alianza con Microsoft, es una iniciativa que ha producido cinco 'declaraciones de Oxford sobre las protecciones del derecho internacional en el ciberespacio'. Estas declaraciones son el producto de colaboraciones entre expertos jurídicos internacionales de todo el mundo para clarificar qué conductas en el ciberespacio están prohibidas, permitidas o requeridas de conformidad con el derecho internacional en una gama de contextos, incluida la atención en salud, investigación y desarrollo de vacunas, elecciones, regulación de las operaciones de información y ransomware.

iii. **Recursos del CICR sobre el DIH y el ciberespacio:** El CICR brinda recursos y asesoría sobre la aplicación del DIH en el ciberespacio para los desarrolladores de política pública, lo que incluye diálogos bilaterales, talleres y publicaciones.[46] El CICR también puede asesorar a los Estados sobre la parte relacionada con DIH de sus posiciones nacionales. Algunos ejemplos de otras actividades que organiza el CICR son programas de acción humanitaria en coordinación con la academia, mesas redondas y otros esfuerzos colaborativos.

46 CICR, *Derecho internacional humanitario y las operaciones cibernéticas durante los conflictos armados* (2019).

Muchos países y organizaciones internacionales ofrecen capacitación y cursos para funcionarios, entre otras, la Asociación de Naciones del Sudeste Asiático (ASEAN), la Organización para la Seguridad y la Cooperación en Europa (OSCE) y la Organización de Estados Americanos (OEA). Estonia inició los Talleres Tallin basados en escenarios sobre derecho internacional y operaciones cibernéticas. El objetivo principal de estos talleres temáticos es crear un foro para el debate internacional entre aliados y ofrecer oportunidades para estudiar los temas más pertinentes del derecho internacional relacionados con la conducta del Estado en el ciberespacio. Se han llevado a cabo cinco talleres y los informes de los primeros cuatro se publicaron en un compendio.[47]

Además de lo anterior, el *Compendio de buenas prácticas: Desarrollo de una posición nacional sobre la interpretación del derecho internacional y el uso de las TIC por los Estados* de 2024, publicado por el Instituto de las Naciones Unidas para la Investigación sobre el Desarme (UNIDIR)[48] es un recurso conciso, estructurado y orientado a procesos. Ofrece una colección de buenas prácticas y reflexiones útiles, que lo hacen una lectura esencial para las personas responsables de desarrollar una posición nacional. Muchos expertos gubernamentales consultados para este proyecto han destacado la utilidad práctica del compendio.[49]



47 Ministerio de Asuntos Exteriores de Estonia *Talleres Tallin sobre derecho internacional y operaciones cibernéticas, Compendio de informes* (2023).

48 UNIDIR, *Compendio de buenas prácticas: Desarrollo de una posición nacional sobre la interpretación del derecho internacional y el uso de las TIC por los Estados* (2024).

49 Varios comentarios hechos en las tres mesas redondas del proyecto (informe en archivo con autores).

7. Investigación, análisis y redacción

a. Enfoques

En las etapas iniciales del desarrollo de una posición, muchos Estados han contado con experiencia y experticia limitadas en el campo. Solo algunos ya estaban familiarizados, lo que lograron gracias a su participación en iniciativas como el GEG y proceso del Manual de Tallin. Como resultado, el desarrollo de una posición nacional involucra en general investigación, recopilación de información y consultas extensas.

Por lo general, los Estados adoptan uno de los dos principales enfoques para estructurar este proceso: eliminación o inclusión.

- **Enfoque de eliminación:** Este método comienza con la creación de un documento de investigación de antecedentes exhaustivo que identifica los temas comunes y las áreas que necesitan mayor investigación. Luego, este documento se refina, adapta y reduce gradualmente para producir la posición nacional.[50]
- **Enfoque de inclusión:** Este método empieza con un esquema general que luego se expande y revisa a medida que progresa el proyecto, incorporando investigaciones adicionales y retroalimentación en el proceso.[51]

Sin importar cuál enfoque se elija, el proceso por lo general toma de meses a años e incluye varias iteraciones del borrador.[52]

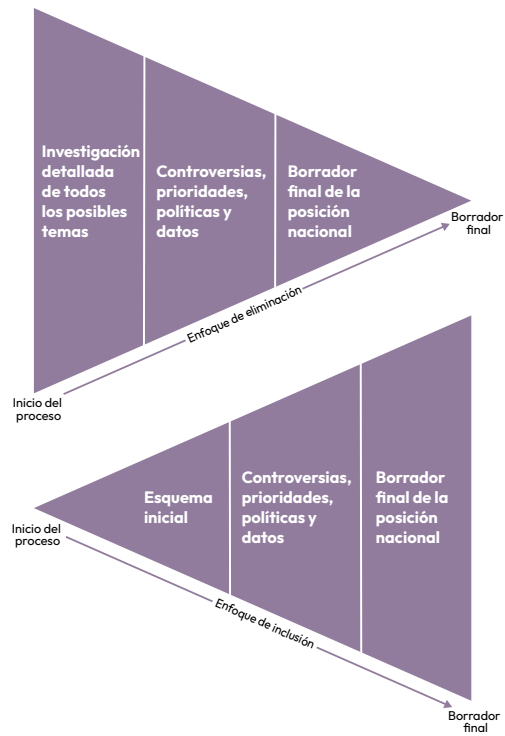


Figura 3: Los dos principales enfoques de redacción.

50 Comentario hecho en el Tercer Simposio Presencial Anual sobre Derecho internacional y cibernético, conflicto futuro: Convergencia del Derecho Internacional Cibernético y de la Información, en el panel sobre 'Perspectivas nacionales sobre el derecho internacional y los potenciales de convergencia', Universidad American, 24 de septiembre de 2024, Washington, DC (informe en archivo con autores)

51 Comentarios hechos en las mesas redondas sobre las perspectivas de Asia, Pacífico, Latinoamérica y el Caribe (informe en el archivo con autores).

52 Los comentarios hechos en las mesas redondas indicaron que la duración es de uno a tres años y al menos ocurren tres iteraciones del borrador.

b. Fuentes de derecho internacional y otras referencias

Desarrollar una posición nacional requiere una investigación extensa para recopilar información pertinente y evaluar las cuestiones jurídicas y políticas asociadas. Gran parte de la información inicial se puede recopilar mediante investigaciones de escritorio, principalmente de fuentes disponibles al público. Estas incluyen documentos jurídicos y de política, informes y publicaciones académicas generales y específicas sobre el ciberespacio. Estos materiales son fundamentales para el proceso de investigación y el contexto de la posición nacional, lo que incluye comprender los debates en curso y sus implicaciones, las políticas nacionales y las posibles áreas prioritarias.

Es importante distinguir estos materiales de referencia de las fuentes formales del derecho internacional definidas en el artículo 38 del Estatuto de la Corte Internacional de Justicia (CIJ). Aunque las fuentes formales, como tratados, derecho internacional consuetudinario y principios generales de derecho, son fundamentales para la preparación de las posiciones nacionales, otros materiales ofrecen antecedentes, contexto y lineamientos esenciales. Las siguientes fuentes diversas pueden consultarse durante el proceso de redacción:

- **Posiciones nacionales:** las posiciones nacionales existentes son un recurso primordial. Se pueden comparar y analizar, lo que ofrece un fundamento para entender e inspirarse en la elección de temas o interpretaciones.[53]
- **Documentos de foros y grupos de expertos especializados de las Naciones Unidas:** en la Primera Comisión de la Asamblea General de la ONU se han estado dando debates especializados y grupos de expertos han estudiado los temas del derecho internacional y el ciberespacio. Los documentos producidos por los seis GGE[54] y dos GTCA (2019 – 2021[55] y 2021 – 2025[56]) están recopilados y disponibles en el sitio web de la Oficina de Asuntos de Desarme de las Naciones Unidas (UNODA). Esto incluye los registros de las declaraciones gubernamentales presentadas ante esos grupos.

53 El Cyber Law Toolkit, en https://cyberlaw.ccdcoe.org tiene una colección de posiciones nacionales y comunes.

54 UNODA, Grupo de Expertos en Desarrollos en el campo de la información y las telecomunicaciones en el contexto de la seguridad internacional.

55 UNODA, Informe del Grupo de Trabajo de Composición Abierta sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional

56 UNODA, Grupo de Trabajo de Composición Abierta sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional.

- **Otras fuentes de la ONU:** varias entidades, órganos, agencias e instituciones de la ONU han abordado diferentes aspectos del derecho internacional que pueden ser relevantes para las TIC. Estos pueden incluir resoluciones de la Asamblea General de la ONU, textos de la Comisión de Derecho Internacional (CDI),[57] informes y publicaciones de UNIDIR,[58] registros de declaraciones en la Sexta Comisión de la Asamblea General de la ONU y otros documentos y publicaciones especializados.
- **Fuentes académicas específicas sobre ciberseguridad:** esta es una categoría muy amplia y hay innumerables libros y artículos de revistas académicas dedicados a los diferentes aspectos del derecho internacional en el contexto cibernético. Algunas posiciones nacionales se refieren a fuentes académicas específicas, por ejemplo, a los *Manuales de Tallin*, el *Cyber Law Toolkit y el Proceso de Oxford*.[59] Publicaciones tales como la *Revista Internacional de la Cruz Roja, los Estudios de Derecho Internacional* o la *Revista sobre política cibernética* también ofrecen artículos de acceso abierto pertinentes para el derecho internacional y las actividades cibernéticas.
- **Documentos de organizaciones internacionales:** varios documentos temáticos publicados por organizaciones internacionales abordan directa o indirectamente el tema. Algunos ejemplos son las publicaciones de la ASEAN,[60] la UA,[61] el Consejo de Europa[62] la UE,[63] el CICR[64] la OEA[65] y la OSCE.[66]
- **Fuentes primarias y secundarias del derecho internacional:** la mayoría de los Estados utilizan fuentes tradicionales del derecho internacional, como está consagrado en el artículo 38 del Estatuto de la CIJ, y se refieren expresamente a los tratados internacionales, el derecho internacional consuetudinario, los principios generales de derecho, la jurisprudencia internacional y las obras académicas. Estos son vitales para redactar declaraciones sobre el derecho bien sustentadas y persuasivas.

57 La principal referencia son los *Artículos sobre la responsabilidad de los Estados por hechos internacionalmente ilícitos con comentarios de la CDI.* (2001).

58 UNIDIR, Ciberseguridad.

59 Consulte, por ejemplo, las posiciones nacionales de Austria (2024), pág. 3, Costa Rica (2023), párr. 6, y República Checa (2024), pág. 1.

60 ASEAN, Ciberseguridad.

61 Posición conjunta de la UA (2024).

62 Sobre los derechos humanos y el estado de derecho, incluida la Convención de Budapest, consulte Consejo de Europa.

63 Consejo de la Unión Europea, *Declaración de la Unión Europea y sus Estados Miembro sobre un Entendimiento común sobre las aplicaciones del derecho internacional al ciberespacio* (2024).

64 Consulte el material del CICR sobre operaciones cibernéticas y de información.

65 OEA, Sección de Ciberseguridad.

66 OSCE, Ciberseguridad.

- **Fuentes nacionales:** algunos Estados hacen referencia a la legislación y las políticas nacionales,[67] así como a declaraciones y documentos de estrategia de organizaciones regionales de las que son miembros.[68] Además, la jurisprudencia nacional, los memorandos internos, las posiciones expresadas en procesos internacionales y muchos otros recursos nacionales pueden ser utilizados por los redactores de la posición nacional para clarificar las declaraciones y entender mejor el contexto, los hechos históricos y los argumentos previos. Las posiciones nacionales no publicadas y compartidas entre socios cercanos también pueden ser fuentes influyentes y útiles.

c. Consultas

Las consultas a expertos técnicos y de política, la academia y otras partes interesadas también pueden fortalecer una posición nacional. Aunque el cronograma de las consultas ha sido variado, como regla general, debería hacerse desde temprano. Sin embargo, depende del cronograma de los esfuerzos de creación de capacidades, al igual que del enfoque general del proceso de redacción (es decir, si tiene un enfoque de inclusión o de eliminación). Los Estados han adoptado uno de dos modelos principales de consulta:

- **Modelo de ruta paralela:** la versión más simple de este modelo es que todos los órganos o partes interesadas (marcados con 'SH' [por sus siglas en inglés] en las Figuras 4 y 6) empiezan a coordinar las diferentes perspectivas desde el principio y siguen haciéndolo durante todo el proceso. Alternativamente, uno o dos órganos pueden tomar el liderazgo desde el principio (marcado como 'SH1' en la Figura 5) y los demás se incorporan a los debates una vez que la posición está desarrollada.[69] El borrador se puede consolidar periódicamente luego de las rondas de consultas (indicadas con flechas en las Figuras 4 y 5).

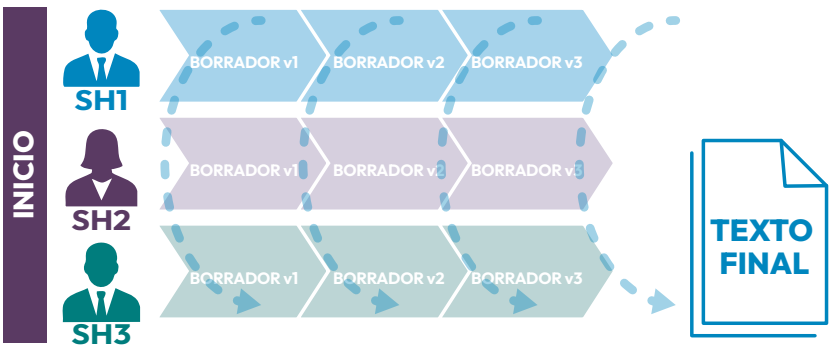


Figura 4: Ruta paralela con coordinación general.

67 Consulte, por ejemplo, las posiciones nacionales de Cuba (2024), párr. 1 a 2 y Kenia (2021) pág. 53 a 54.

68 Consulte, por ejemplo, la posición nacional de Polonia (2022) pág. 1-2.

69 Comentario hecho en la mesa redonda sobre las perspectivas de Asia y el Pacífico (informe en el archivo con autores).

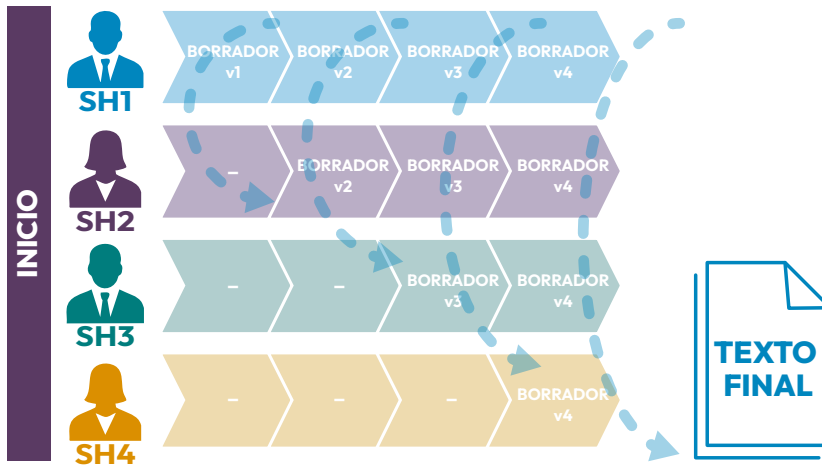


Figura 5: Ruta paralela con coordinación central.

Las partes interesadas relevantes se pueden consultar como un solo grupo o incrementalmente a medida que se refina la posición. Sin embargo, las consultas incrementales corren el riesgo de crear flujos de trabajo paralelos, que pueden requerir mucho tiempo y dificultar la coordinación, resolución de conflictos y consolidación. Uno de los profesionales consultados para este manual sugirió que antes de decidir las áreas que necesitan más trabajo, se debe circular el esquema anotado (en vez del borrador completo) para recibir hasta tres comentarios por tema.[70]

70 Comentario hecho en la mesa redonda sobre las perspectivas de Latinoamérica y el Caribe (informe en el archivo con autores).

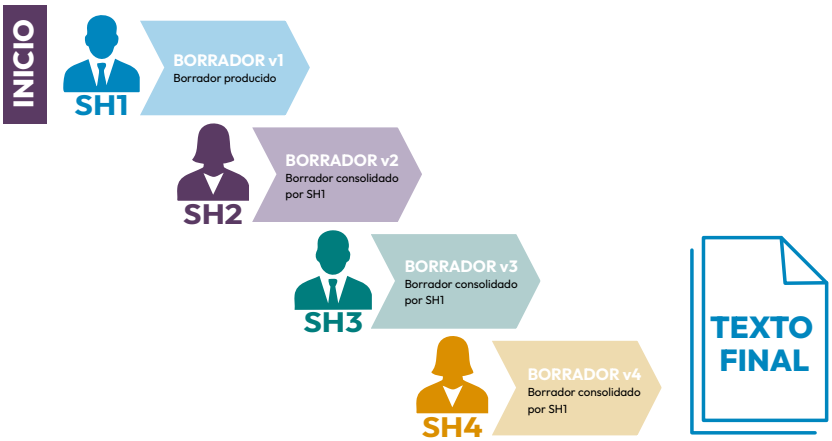


Figura 6: Ruta continua con coordinación central.

- **Modelo de ruta continua:** este enfoque involucra llevar a cabo consultas de manera periódica, y con borradores que se circulan en secuencia a los diferentes grupos de partes interesadas (Vea la Figura 6). Esto podría dar como resultado que algunas partes interesadas solo tengan una oportunidad de hacer comentarios y sugerencias. Sin embargo, este modelo es más simple y fácil de manejar.

Se pueden combinar los dos modelos, y las diversas etapas se pueden repetir.

Las consultas pueden ser internas y externas, como:

- **Colaboraciones interinstitucionales o departamentales:** la colaboración eficaz entre órganos es importante para el desarrollo de una posición nacional coherente e involucra el diálogo regular con los departamentos gubernamentales pertinentes. Algunos de estos pueden ser las agencias nacionales de ciberseguridad, varios ministerios (por ejemplo, de defensa, justicia, interior y comunicaciones), al igual que las fuerzas armadas y órganos de la rama jurídica, como la oficina del fiscal general o entidades judiciales.[71]
- **Consultas con funcionarios de gobiernos extranjeros:** en diferentes etapas del proceso puede ser útil realizar colaboraciones o consultas bilaterales o multilaterales con otros Estados. En particular, los redactores o expertos que participan en el desarrollo de la posición nacional de otro Estado pueden ayudar a diseñar e impulsar el inicio del proceso. De igual manera, las consultas externas pueden servir como un ejercicio de creación de capacidades para el equipo

71 UNIDIR, Compendio de buenas prácticas: Desarrollo de una posición nacional sobre la interpretación del derecho internacional y el uso de las TIC por los Estados (2024).

central del Estado y otras partes que están involucradas en el proceso.[72] Los expertos externos también pueden contribuir durante el proceso de redacción, por ejemplo, brindando asesoría sobre asuntos sustantivos o procedimentales, o facilitando otros debates a nivel regional.

- **Consultas con partes interesadas no estatales:** estas partes interesadas pueden ser asociaciones de profesionales, think tanks, firmas consultoras, representantes de la industria, grupos indígenas, académicos o personas particulares de la sociedad civil, nacionales o internacionales (consulte la **Sección 4** de este capítulo). Como indicó un representante de un Estado durante las mesas redondas del proyecto, en los Estados donde los procesos de política pública son muy inclusivos, también se debe considerar el fenómeno de la 'fatiga de la consulta'. En general, los Estados deben tratar de encontrar un equilibrio entre los aportes y la colaboración útiles y no abrumar a las partes interesadas consultadas.

Las consultas también pueden tener **diferentes formatos**. Pueden ser formales o informales, orales o escritas, presenciales o virtuales (o híbridas) e interactivas o de una sola vía. Las consultas informales pueden evitar las extensas trabas burocráticas. Por esto, organizarlas puede ser más fácil y rápido y permite mayor libertad y flexibilidad en el intercambio de perspectivas. Esto puede fomentar el pensamiento creativo y la construcción de relaciones. Sin embargo, puede que las consultas informales no sean adecuadas en todas las situaciones. Puede ser necesario llevar a cabo reuniones formales para temas complejos que requieren documentación detallada y registros oficiales. En los contextos internos y externos pueden ser útiles las encuestas y cuestionarios, especialmente si hay diferentes órganos participando en los debates.[73] Sin embargo, las partes interesadas relevantes pueden carecer de interés o recursos, o ser renuentes a responder, por ejemplo, porque ciertos temas se pueden considerar delicados o clasificados (como preguntas sobre la atribución o el DIH). Finalmente, las asambleas públicas o conferencias pueden ser especialmente útiles al principio del proceso de redacción.[74] Esto puede implicar reuniones públicas y comunicación básicamente de una vía entre los funcionarios gubernamentales encargados de desarrollar la posición nacional y cualquier miembro del público o de la industria interesada. El principal propósito es recopilar ideas, preocupaciones, comentarios y sugerencias para posiblemente usarlos luego durante el proceso, o identificar las áreas y temas que tienen suficiente apoyo para hacer declaraciones públicas.

72 Comentario hecho en el Tercer Simposio Presencial Anual sobre Derecho internacional y cibernético, conflicto futuro: Convergencia del Derecho Internacional Cibernético y de la Información, en el panel sobre 'Perspectivas nacionales sobre el derecho internacional y los potenciales de convergencia', Universidad American, 24 de septiembre de 2024, Washington, DC (informe en archivo con autores) También considere, por ejemplo, la serie de Talleres Tallin realizada por el Ministerio de Asuntos Exteriores de Estonia.

73 Comentarios hechos en la mesa redonda sobre las perspectivas de Latinoamérica y el Caribe (informe en el archivo con autores).

74 Comentario hecho en la mesa redonda sobre las perspectivas de Asia y el Pacífico (informe en el archivo con autores).

d. Análisis

Con relación a la naturaleza jurídica de las posiciones nacionales y el proceso para desarrollarlas, existe una amplia bibliografía dedicada a determinar la **existencia y el contenido de las reglas**.[75] Ya antes de la histórica conclusión del GEG en 2013 sobre la aplicación del derecho internacional en el contexto cibernético,[76] había un debate cada vez más intenso sobre cómo se aplican las diferentes reglas. La finalidad de las posiciones nacionales es la identificación de las reglas aplicables, especialmente del derecho internacional consuetudinario, al igual que su interpretación con respecto a la conducta cibernética. Para el desarrollo de las posiciones nacionales, los Estados pueden usar lógicas deductivas e inductivas, incluso juntas (consulte también el **Capítulo 5** sobre el formato y estilo).

El **razonamiento deductivo** se refleja en la estrategia de exploración, donde primero se identifican los temas más manejables, como las aplicaciones de la Carta de las Naciones Unidas (consulte la **Sección 5** de este capítulo). Con frecuencia, las posiciones nacionales se refieren a los informes del GTCA, que generalmente hablan de la aplicación del derecho internacional en el contexto cibernético, y luego, la posición nacional pasa a reglas más específicas a partir de esta declaración general. La lógica deductiva se puede verificar buscando ejemplos y escenarios que confirmen la precisión de las conclusiones sobre reglas específicas.

Por otro lado, el **razonamiento inductivo** se refleja en la lógica que comienza por identificar los problemas e incidentes, como el ransomware o la desinformación, seguido por la construcción de la posición alrededor de estos. Como se mencionó en el **Capítulo 5**, muchos Estados se refieren a escenarios en sus documentos de posición[77] e incluso más Estados promueven o han afirmado usar escenarios en el proceso de desarrollo.[78]

75 Consulte, por ejemplo, los *Manuales de Tallin* 1.0 y 2.0.

76 Asamblea General de las Naciones Unidas, *Informe del Grupo de Trabajo de Composición Abierta sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional*, A/68/98 (24 de junio de 2013), párr. 19.

77 Consulte, por ejemplo, las posiciones nacionales de Australia (2021), Austria (2024), Canadá (2022), Costa Rica (2023), República Checa (2024), Italia (2021), Países Bajos (2019), y el Reino Unido (2022).

78 Varios comentarios hechos en las tres mesas redondas del proyecto (informe en archivo con autores).

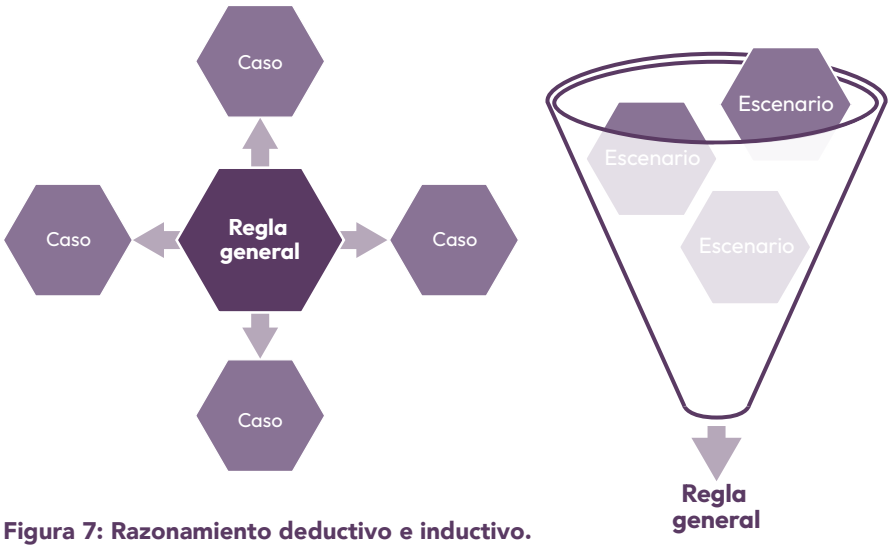


Figura 7: Razonamiento deductivo e inductivo.

Pasar por diferentes formulaciones abstractas de un concepto y 'jugar' el escenario puede arrojar luz sobre las diferencias prácticas significativas en la aplicación en el mundo real y facilita la ejemplificación de una posición en el texto o durante las consultas. Sin embargo, en las mesas redondas del proyecto surgió que, a pesar de sus aplicaciones, algunos Estados pueden ser renuentes a participar en ejercicios basados en escenarios, al menos en foros globales. Por lo menos un experto gubernamental sugirió que estos debates se pueden considerar demasiado reveladores del pensamiento del Estado sobre el caso. Un representante de los Estados dijo que esta renuencia puede deberse a los usos infrecuentes y, por lo tanto, algunos Estados se sienten en desventaja.[79]

Otras orientaciones sobre la identificación de reglas y herramientas interpretativas son:

- Los proyectos de conclusiones de la CDI sobre la identificación del derecho internacional consuetudinario (2018).[80]
- Los proyectos de conclusiones de la CDI sobre la identificación y consecuencias jurídicas de las normas imperativas del derecho internacional general (*jus cogens*) (2022).[81]
- Convención de Viena sobre el Derecho de los Tratados (1969).

79 Comentario hecho en la mesa redonda sobre las perspectivas de Latinoamérica y el Caribe (informe en el archivo con autores).

80 CDI, *Proyecto de conclusiones sobre la identificación del derecho internacional consuetudinario con comentarios*, A/73/10 (2018)

81 CDI, *Proyectos de conclusiones de la CDI sobre la identificación y consecuencias jurídicas de las normas imperativas del derecho internacional general (jus cogens)* (2022).

8. Adopción y difusión

La conclusión y aprobación de una posición nacional requiere una deliberación cuidadosa para garantizar que todas las partes interesadas estén alineadas y que represente con precisión las perspectivas del Estado. El Estado también tiene que determinar qué órganos internos tienen competencia para **adoptar o aprobar formalmente** la posición nacional, de acuerdo con sus marcos jurídicos nacionales. A menudo, esta determinación se toma durante la fase de planeación, como se habló en la **Sección 5** de este capítulo.

La adopción o aprobación oficial de la posición nacional también debe seguir un **proceso institucional** claramente definido. Esto incluye designar la autoridad específica responsable de este respaldo. Es importante tener claridad sobre este asunto desde temprano. Por ejemplo, algunos Estados pueden requerir que la posición se presente ante un cuerpo legislativo para su aprobación, mientras que otros pueden ordenar la adopción mediante un organismo ejecutivo particular, como un ministerio o un consejo de ministros.

Los Estados pueden decidir si publican o mantienen la posición nacional como un documento interno. Las posiciones nacionales incluidas en este manual fueron puestas a disposición del público mediante, por ejemplo, publicación en un boletín oficial o sitio web gubernamental o enviadas a foros internacionales como el GTCA o plataformas similares. Como se discute con más detalle en el **Capítulo 5**, las prácticas de difusión de las posiciones nacionales varían y reflejan la naturaleza y formato diferentes de estos documentos.

9. Seguimiento, reflexión y revisión

Luego de desarrollar una posición nacional, un Estado podría considerar si es necesario tomar otras medidas para **implementar** elementos específicos de esta posición. Si es necesario implementar, se debe preparar un plan de trabajo y presupuesto detallados para apoyar estos esfuerzos. Adicionalmente, si la posición establece ciertas metas, se deben implementar los mecanismos para hacer seguimiento y evaluación del progreso de esta en el tiempo.

Las posiciones nacionales también se pueden revisar, si ciertos temas exigen **mayor evaluación** o las interpretaciones jurídicas **evolucionan**. Puede que esto no involucre cambios de perspectiva drásticos, pero puede construir sobre las perspectivas ya declaradas. Como la tecnología y sus aplicaciones siguen evolucionando, inevitablemente surgirán nuevos temas, que exigirán actualizaciones de la posición nacional.

Un Estado podría considerar si es necesario tomar otras medidas para implementar elementos específicos de esta posición.

No obstante, la revisión de una posición nacional no carece de dificultades. La capacidad del Estado de cambiar su posición puede verse limitada por la necesidad de **justificar** los ajustes con nuevas circunstancias, evidencia o consideraciones que anteriormente no se tomaron en cuenta. Los cambios repentinos o significativos de la posición pueden acarrear altos costos de reputación, y posiblemente socaven la credibilidad del Estado a nivel internacional.[82]

10. Conclusión

El desarrollo de una posición nacional es un **proceso político y también jurídico**, consecuencia de diversas circunstancias. Estas pueden ser desde ataques cibernéticos significativos hasta el cumplimiento de compromisos internacionales o nacionales.

Un paso clave inicial es identificar las partes interesadas relevantes y clarificar sus mandatos y roles. Se debe conformar un equipo base, que con frecuencia incluye a representantes de diferentes órganos y trayectorias profesionales diversas, encargando los redactores de la coordinación y redacción del documento. El equipo debe incluir a expertos en política y técnicos, junto con abogados internacionalistas, para que todos aporten perspectivas diferentes pero esenciales sobre qué conducta es **preferida, permitida y posible** en el ciberespacio.

Las etapas de preparación y planificación deben abordar varios **interrogantes organizacionales**, en particular 'quién hará qué', 'por qué', 'dónde' y 'cómo' (5 preguntas clave). La creación de capacidades debe ser una parte integral del proceso y debe ser relevante en todas las etapas. Para apoyar a los Estados en el desarrollo de la experticia necesaria, hay numerosas iniciativas y recursos.

La fase de **recopilación de datos, investigación y análisis** se puede abordar de maneras diferentes. Un método es empezar con un documento exhaustivo o una lista de temas que luego se refina para limitar el alcance de la posición nacional. Alternativamente, se puede empezar con un esquema corto anotado y gradualmente expandirlo a medida que el proceso evoluciona. Las **consultas** pueden ser una parte importante del proceso y requieren coordinación y gestión cuidadosas para garantizar que se integren eficazmente los aportes de las partes interesadas.

82 Comentario hecho en la mesa redonda sobre las perspectivas de África (informe en el archivo con autores).

La mayoría de las posiciones nacionales adoptan un enfoque deductivo, empezando con reglas establecidas del derecho internacional y luego analizando cómo se aplican en el contexto cibernético. Sin embargo, puede ser valioso un enfoque inductivo, empezando con los desafíos específicos (por ejemplo, ciberataques habilitados por IA o ransomware) y luego estudiando cómo aplica el derecho internacional. Estos **enfoques se pueden combinar** y algunos Estados incorporan escenarios y ejemplos para ilustrar su posición.

Puede que la adopción de una posición nacional deba cumplir ciertos **requisitos institucionales**, como la aprobación del parlamento o de un organismo ejecutivo, dependiendo del Estado. El desarrollo de una posición nacional no es necesariamente un ejercicio único y puede ser objeto de revisiones.

CAPÍTULO 4:

CONTENIDO

DE UN VISTAZO

Este capítulo estudia las principales cuestiones jurídicas que se abordan en las posiciones nacionales, incluidas las reglas y principios fundamentales del derecho internacional (como la soberanía, la diligencia debida y la no intervención), al igual que los regímenes jurídicos especializadas (como el derecho internacional humanitario, el derecho Internacional de los derechos humanos y el derecho penal internacional). Destaca áreas donde hay acuerdos y los debates clave con el fin de ayudar a los Estados a decidir los temas que cubrirán y qué tan profundamente tratarlos.

1. Introducción

Las posiciones nacionales existentes sobre el derecho internacional y las actividades cibernéticas cubren una amplia gama de asuntos sustantivos. Junto con importantes preguntas sobre el derecho internacional, abordan los diferentes aspectos fácticos del actual panorama de las ciber amenazas, como el impacto del ransomware, la desinformación y el espionaje cibernético. También han abordado importantes dificultades políticas, como la necesidad de afrontar las brechas digitales, fomentar el desarrollo internacional, construir capacidades, luchar contra la ciberdelincuencia o desarrollar nuevas reglas para el ciberespacio. La opción de temas a cubrir y las perspectivas que expresan, reflejan la posición del Estado sobre temas políticos, sociales y culturales complejos que surgen del uso generalizado de las tecnologías de la información y comunicación (TIC) a nivel nacional e internacional.

Hoy en día existe consenso con relación a las aplicaciones del derecho internacional al uso de las TIC, y casi todas las posiciones nacionales hasta ahora reflejan esto de manera explícita o implícita. El mero hecho de publicar una posición indica el reconocimiento del Estado de que el derecho internacional es aplicable y pertinente para las actividades cibernéticas. Sin embargo, esto no significa que haya acuerdos sobre cuáles normas exactas del derecho internacional aplican, cómo se aplican en el contexto cibernético ni si son suficientes para abordar los desafíos de este contexto. Las posiciones nacionales han abordado la mayoría de las áreas más controvertidas del derecho internacional en su aplicación a las actividades cibernéticas, y se han hecho evidentes muchas áreas de desacuerdo. Aparte de los debates sustantivos que se tratan en este capítulo, algunos Estados han argumentado que es necesario contar con un nuevo instrumento jurídicamente vinculante para llenar las brechas en la aplicación del derecho internacional existente a las actividades cibernéticas.[1]

1 Consulte, por ejemplo, las posiciones nacionales de China (2021), pág. 3, Cuba (2024), párr. 4, Pakistán (2023), párr. 8, y Rusia (2021), pág. 80.

Este capítulo está estructurado alrededor de tres categorías amplias de temas jurídicos que surgen de las aplicaciones del derecho internacional a las actividades cibernéticas. Comienza con un examen de las reglas y principios fundamentales del derecho internacional, lo que incluye soberanía, no intervención, la prohibición del uso de la fuerza, diligencia debida, arreglo pacífico de controversias y la autodeterminación. Luego, da una mirada a tres regímenes jurídicos especializados, el derecho internacional humanitario, el derecho internacional de los derechos humanos y el derecho penal internacional, y estudia cómo se aplican sus reglas en el contexto cibernético. Por último, analiza el derecho internacional sobre la responsabilidad del Estado, enfocándose en la atribución, las contramedidas y la invocación de necesidad.

Estos debates son vitales para determinar cómo se pueden adaptar los actuales marcos jurídicos a los desafíos especiales que suponen las TIC. Y las posiciones nacionales se han convertido en el principal vehículo mediante el que los Estados han contribuido a estos importantes debates jurídicos. Como se indica en la **Introducción** de este manual, las posiciones nacionales pueden calificar como evidencia de *opinio juris* y más controversialmente, de la práctica del Estado para los fines de la formación del derecho internacional consuetudinario. Por esto, es discreción de los Estados mantener el estatus quo o desarrollar el derecho internacional mediante sus posiciones nacionales.

Este capítulo ofrece un resumen de los asuntos sustantivos del derecho internacional que con más frecuencia se tratan en las posiciones nacionales y conjuntas publicadas hasta la fecha (consulte también la Figura 8 en las páginas 122 y 123), al igual que debates multilaterales pertinentes, incluido en el contexto de los procesos con mandato de la ONU, como el Grupo de Expertos Gubernamentales de la ONU (GEG) y el Grupo de Trabajo de Composición Abierta (GTCA). La selección de los temas también es reflejo de los que presentaron constantemente los participantes de las mesas redondas del proyecto. Además de mapear las diferentes perspectivas sobre cómo estas reglas y principios del derecho internacional se aplican en el contexto cibernético, el capítulo también examina las consideraciones políticas que les dan forma.

Para ayudar a los lectores a explorar estos temas con mayor profundidad, este capítulo incluye códigos QR (que en la versión digital son hipervínculos) que vinculan a las páginas correspondientes del *Cyber Law Toolkit* (Kit de herramientas sobre derecho cibernético). Estas páginas ofrecen contenido actualizado periódicamente, análisis jurídico con mayor profundidad y un resumen comparativo de las posiciones nacionales sobre cada tema.

2. Reglas y principios fundamentales

Esta sección examina seis normas y principios fundamentales del derecho internacional en su aplicación a las actividades cibernéticas. Cuatro de estas, soberanía, la prohibición de intervención, la prohibición del uso de la fuerza y la diligencia debida, están incluidas en una cantidad significativa de posiciones nacionales y están entre los temas más debatidos en esta área. Los otros dos, el arreglo pacífico de controversias y el derecho a la autodeterminación, han atraído menos atención, pero empiezan a surgir con mayor frecuencia en las posiciones nacionales y los debates multilaterales. Aunque la mayoría estaría de acuerdo con que todos los seis aplican a las actividades cibernéticas, los Estados difieren en cuanto a cómo se interpretan y aplican. En general, esta sección describe cómo han abordado estos temas los Estados que han publicado una posición hasta la fecha, destacando las áreas de convergencia y los interrogantes sin resolver.

a. Soberanía

La soberanía es un principio básico del derecho internacional. De acuerdo con la definición clásica, articulada en el laudo arbitral Isla de Palmas[2] en 1928, soberanía significa, 'con relación a una porción del planeta […] el derecho a ejercer sobre ella, con exclusión de cualquier otro Estado, las funciones de un Estado'. Se acepta generalmente que la soberanía aplica al contexto cibernético.[3] Sin embargo, el debate persiste con relación a su naturaleza jurídica precisa: ¿constituye una norma autónoma del derecho internacional o funciona solo como un principio rector?

Existe un consenso amplio de que la soberanía aplica al contexto cibernético, aunque persiste el debate sobre si es una norma autónoma del derecho internacional o es simplemente un principio rector.

2 *Island of Palmas (US v Netherlands)* [Isla de Palmas (Estados Unidos vs Países Bajos] (1928) II RIAA 829, 838 (Trad. libre).

3 Asamblea General de las Naciones Unidas, *Informe del Grupo de Expertos Gubernamentales sobre los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional*, A/76/135 (14 de junio de 2021), párr. 70 y 71(b).

La mayoría de los Estados que han expresado una posición sobre este asunto consideran que la soberanía es una **regla primaria sustantiva del derecho internacional**, cuyo incumplimiento da lugar a responsabilidad del Estado. Es importante destacar que esto puede dar lugar al derecho del Estado víctima de tomar contramedidas contra el Estado responsable de la violación. Esta perspectiva fue adoptada por Estados como Austria, Brasil, Canadá, República Checa, Estonia, Finlandia, Francia, Alemania, Irán, Italia, Japón, Países Bajos, Nueva Zelanda, Noruega, Rumanía y Suecia.[4] También fue respaldada en las posiciones conjuntas de la Unión Africana (UA) y de la Unión Europea (UE).[5]

También existe la perspectiva de que la soberanía es meramente un **principio del derecho internacional** que orienta las interacciones de los Estados, pero no llega a ser una regla primaria autónoma. Hasta ahora, esta posición solo ha sido adoptada por un Estado, el Reino Unido. Bajo este enfoque, las operaciones cibernéticas no pueden violar la soberanía del Estado hacia o contra el cual se dirigen. Sin embargo, dichas operaciones todavía pueden constituir una intervención prohibida, el uso de la fuerza u otro hecho internacionalmente ilícito.

Un **enfoque intermedio** simplemente reconoce que la soberanía se aplica en el contexto cibernético mientras se abstiene de clarificar si constituye una regla del derecho internacional. Algunos Estados que adoptan esta posición, además, hacen notar la complejidad del asunto e indican que siguen estudiándolo. Este enfoque permite a los Estados preservar la flexibilidad operacional y mantener la opción de apoyar una posición más definitiva en el futuro. Los Estados que han adoptado esta posición incluyen a Australia, Israel, Kenia y los Estados Unidos.[6]

La perspectiva prevaleciente de que la soberanía constituye una norma autónoma implica la obligación de todos los Estados de respetar la soberanía de los demás. Sin embargo, en la actualidad no existe consenso sobre los criterios exactos para determinar cuándo las operaciones cibernéticas violan la soberanía, y las posiciones de los Estados varían significativamente. Con relación a este aspecto han surgido dos enfoques principales: basado en el acceso y basado en los efectos.

4 Consulte las posiciones nacionales de Austria (2024), pág. 4, Brasil (2021), pág. 18; Canadá (2022) párr. 10 y 14 ff, República Checa (2024), párr. 1 y 3, Estonia (2021), pág. 24, Finlandia (2020), pág. 1 y 2, Francia (2021), pág. 2 y 3, Alemania (2021), pág. 2 y 3, Irán (2020), art. II.2, Italia (2021), pág. 4, Japón (2021), pág. 2, Países Bajos (2021), pág. 7, Nueva Zelanda (2020), párr. 11 a 15, Noruega (2021), pág. 3, Rumania (2021), pág. 76 y Suecia (2022), pág. 2.

5 Consulte las posiciones nacionales de la UA (2024), párr. 12, y Rusia (2024), pág. 4.

6 Consulte las posiciones nacionales de Australia (2021), pág. 5; Israel (2021), pág. 402; Kenia (2021), pág. 53 y de los Estados Unidos (2021), pág. 139.

- De acuerdo con el **enfoque basado en el acceso** (también referido como basado en penetración o purista), cualquier penetración de sistemas de TIC no autorizada en el interior del territorio de un Estado califica como una violación de su soberanía. Esto incluye operaciones como instalar una puerta trasera en un sistema informático o exfiltrar datos de dicho sistema. Puede que los Estados a favor de este enfoque lo elijan por sus cualidades protectoras.[7] Sin embargo, quienes están contra este destacan su posible incompatibilidad con el diseño y funcionamiento de Internet, particularmente por el hecho de que cualquier comunicación en línea, por definición, involucra entrar en la red del destinatario.[8]
- El **enfoque basado en los efectos** requiere que la operación cibernética produzca algún tipo de efecto o perjuicio al Estado víctima para que califique como una violación de la soberanía. Los posibles efectos o perjuicios proscritos, identificados en la bibliografía, pueden incluir la violación de la integridad territorial del Estado víctima y la interferencia o usurpación de las funciones inherentemente gubernamentales del Estado víctima.[9]
    - Una operación puede **violar la integridad territorial del Estado** de varias maneras. La más obvia es causar daños físicos, destrucción, lesiones o muertes. Los actos que tengan dichos efectos también pueden calificar simultáneamente como violaciones de la no intervención y considerarse uso de fuerza (vea a continuación). En sus posiciones nacionales, algunos Estados extienden esta categoría para incluir la pérdida de funcionalidad de los sistemas ubicados en otro Estado, incluso si dichas pérdidas no resultan en daños físicos.[10]
    - La noción de **funciones inherentemente gubernamentales** cubre actividades que son de exclusiva competencia del Estado y que solo pueden ser ejercidas por actos no estatales mediante delegación del Estado, como defensa nacional, cumplimiento de la ley, prestación de servicios sociales, organización de elecciones o funciones diplomáticas.[11] Interferir con dichas actividades involucra perturbarlas, como la manipulación de resultados electorales por medios cibernéticos. La usurpación ocurre cuando una operación cibernética involucra llevar a cabo una función que solo el Estado afectado está autorizado a realizar, como ejercer fuerza policial en el territorio de otro Estado sin su consentimiento.

---

7 Harriet Moynihan, *The Application of International Law to State Cyberattacks: Sovereignty and Non-Intervention* [Las aplicaciones del derecho internacional a los ataques cibernéticos estatales: Soberanía y no intervención] (Chatham House 2019), párr. 61, que describe este enfoque como de 'máxima protección'.

8 Consulte, por ejemplo, la posición nacional de Estados Unidos (2021), pág. 140, que señala que 'el diseño mismo de Internet puede conducir a cierta injerencia en otras jurisdicciones soberanas'.

9 Michael N Schmitt (editor), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* [Manual de Tallin 2.0 sobre el derecho internacional aplicable a las operaciones cibernéticas]

10 Consulte, por ejemplo, las posiciones nacionales de Austria (2024), pág. 4, Canadá (2022), párr. 16 y 17, Costa Rica (2023), párr. 20, Dinamarca (2023), pág. 449 y Noruega (2021), pág. 3 y 4.

11 *Manual de Tallin 2.0*, comentario sobre la Norma 4.

Un interrogante sin resolver es el relacionado con el **espionaje cibernético**. Aunque el derecho internacional no lo regula como tal, la legalidad del espionaje puede ser difícil de reconciliar con las anteriores perspectivas más amplias de soberanía, particularmente con el enfoque basado en el acceso. Si cualquier recopilación de datos no autorizada en el exterior constituye una violación de la soberanía, esto podría incluir muchas operaciones de espionaje cibernético. En sus posiciones nacionales, Estados como Austria, Costa Rica y Polonia expresan perspectivas que sugieren que ellos consideran que al menos ciertos tipos de espionaje cibernético violan la soberanía. En la posición de Brasil, las intercepciones de telecomunicaciones son ilícitas por definición, porque violan la soberanía del Estado.[12]

En contraste, algunos Estados adoptan una perspectiva expresamente opuesta en sus posiciones nacionales. Por ejemplo, Canadá indica que 'algunas actividades cibernéticas, como el espionaje cibernético, no equivalen a una violación de la soberanía territorial',[13] mientras que Nueva Zelanda dice que 'no considera que la soberanía territorial prohíba cada intrusión no autorizada en un sistema informático extranjero' y que la 'actividad de espionaje pura […] no sería internacionalmente ilícita'.[14] En conclusión, la calificación del espionaje cibernético sigue sin acordarse y probablemente continuará dando forma a las posiciones de los Estados sobre la soberanía en el ciberespacio.

b. No intervención

El principio de no intervención (también llamado la prohibición de intervención) es un corolario de la soberanía del Estado y una norma bien aceptada del derecho internacional consuetudinario. Esta prohíbe a los Estados interferir, directa o indirectamente, en los asuntos internos o externos de los otros Estados por medios coercitivos.[15] No hay duda de que el principio de la no intervención se aplica al contexto cibernético. Para que un acto, incluida una operación cibernética califique como intervención prohibida, debe cumplir dos condiciones clave.

En primer lugar, debe referirse a cuestiones que formen parte de los asuntos internos o externos de un Estado, su domaine réservé: lo que quiere decir, esos asuntos en los que cada Estado tiene permitido decidir libremente, como su elección de sistemas políticos, económicos, sociales y culturales, así como la formulación de su política exterior.[16]

12 Posición nacional de Brasil (2021), pág. 18.

13 Posición nacional de Canadá (2022), párr. 19 (Trad. libre).

14 Posición nacional de Nueva Zelanda (2020), párr. 14 (Trad. libre).

15 CIJ, *Military and Paramilitary Activities in and against Nicaragua (Nicaragua vs. US) [Actividades militares y paramilitares en y contra Nicaragua (Nicaragua vs. Estados Unidos)] (Fondo) [1986] CIJ Rep. 14 (Nicaragua case)* [El caso Nicaragua], párr. 205.

16 CIJ, *Nicaragua case* [El Caso Nicaragua], párr. 205. Consulte también CIJ, *Case Concerning Armed Activities in the Territory of the Congo [Caso relacionado con actividades armadas en el territorio del Congo] (República Democrática del Congo y Uganda)* (Fondo) [2005] CIJ Rep. 168, párr. 162 a 64; *Manual de Tallin 2.0*, comentario sobre la Norma 66., párr. 6 a 8.

Para algunos, el contenido del *domaine réservé* está limitado al alcance y a la naturaleza de las obligaciones jurídicas internacionales de un Estado.[17] En esta perspectiva, entre más normas internacionales haya aceptado un Estado, menos libertad tendrá sobre sus asuntos internos o externos y menos alcance tendrá su *domaine réservé*. Para otros, el alcance del *domaine réservé* de un Estado es fijo y corresponde a una lista normalizada de funciones soberanas inherentes.[18]

En el contexto cibernético, al igual que en otros, adoptar el primer enfoque limitaría las áreas en las cuales la intervención se consideraría ilegal y, por lo tanto, reduce el alcance e importancia del principio de no intervención. Por ejemplo, si un Estado acepta ciertos estándares internacionales de salud, la interferencia con respecto a esos estándares por medios o no cibernéticos no podría considerarse una intervención prohibida. En contraste, el enfoque fijo al *domaine réservé* podría resultar en un alcance más amplio de aplicación del principio de no intervención. Usando el mismo ejemplo de antes, el hecho de que el Estado haya aceptado determinada obligación internacional en el contexto sanitario no elimina por completo su libertad sobre el asunto. Después de todo, los Estados mantienen discreción y autoridad final en asuntos sobre los cuales ejercitan autoridad gubernamental.[19]

La mayoría de las posiciones nacionales y conjuntas emitidas hasta ahora han adoptado el último enfoque y no limitan las áreas que entran dentro del *domaine réservé* del Estado.[20] Este enfoque 'protector' parece surgir de la preocupación de limitar las operaciones cibernéticas intrusivas llevadas a cabo o apoyadas por otros Estados. La perspectiva opuesta parece estar conectada a estrategias cibernéticas 'expansivas' que buscan preservar la capacidad del Estado de llevar a cabo actividades cibernéticas en el extranjero.[21]

17 Consulte, por ejemplo, *Manual de Tallin 2.0*, comentario sobre la Norma 66, párr. 7 y 13; Katja S Ziegler, 'Domaine réservé' (abril de 2013), Enciclopedia del Derecho Internacional Max Planck, Sección C; Marco Roscini, *International Law and the Principle of Non-Intervention* [Derecho internacional y el principio de la no intervención] (OUP 2024) 162 a 164.

18 Consulte, por ejemplo, Harriet Moynihan, *The Application of International Law to State Cyberattacks: Sovereignty and Non-Intervention* [Las aplicaciones del derecho internacional a los ataques cibernéticos estatales: *Soberanía y no intervención]* (Chatham House 2019), párr. 107. Consulte también el debate en Tsvetelina van Benthem, Talita Dias y Duncan B Hollis, 'Operaciones de información bajo el derecho internacional' (2022) 55 *Vanderbilt Journal of Transnational Law* 1217, 1260 a 1261.

19 Harriet Moynihan, *The Application of International Law to State Cyberattacks: Sovereignty and Non-Intervention* [Las aplicaciones del derecho internacional a los ataques cibernéticos estatales: Soberanía y no intervención] (Chatham House 2019), párr. 106.

20 Consulte, por ejemplo, las posiciones nacionales de Costa Rica (2023), párr. 23 a 25, República Checa (2024), párr. 9(a), Dinamarca (2023), pág. 450 e Irlanda (2023), párr. 8 a 10, que incluyen todas áreas no exhaustivas dentro del *domaine réservé*) del Estado, y también la posición nacional de Canadá (2022), párr. 22, que define el alcance de la no intervención sobre las 'funciones inherentemente soberanas'.

21 Consulte, por ejemplo, la posición nacional de los Estados Unidos (2021), pág. 140, que argumenta que 'la no intervención por lo general se considera una regla relativamente estrecha del derecho internacional consuetudinario'.

La coerción es el segundo elemento de una intervención prohibida: el hecho en cuestión debe ser de **naturaleza coercitiva**. De acuerdo con la Corte Internacional de Justicia (CIJ), 'el elemento de la coerción […] define e indudablemente forma la propia esencia de la intervención prohibida'.[22] La coerción puede ser directa, ejercida por órganos de un Estado contra otro, o indirecta, en forma de apoyo a actos de coerción de actores no estatales o hechos dirigidos a la población del Estado víctima (en contraposición a su gobierno).[23] Un ejemplo de intervención directa son las acciones militares en el territorio de otro Estado. Algunos ejemplos de intervención indirecta son el apoyo de un Estado a las acciones subversivas de actores no estatales, u operaciones de influencia para cambiar las actitudes de la población del Estado víctima, como ciertas formas de propaganda y desinformación.

La coerción es un elemento clave de una intervención prohibida: el hecho en cuestión debe ser de naturaleza coercitiva.

La intervención indirecta es particularmente pronunciada en el contexto cibernético, debido a la proliferación de las TIC entre actores no estatales, incluidos perpetradores o víctimas de operaciones cibernéticas maliciosas.

Sin embargo, no hay una definición generalmente aceptada de coerción en el derecho internacional.[24] Existen dos enfoques principales para definir la coerción en el contexto cibernético, que se centran en dos elementos diferentes:

a. El enfoque **basado en la intención**, bajo el cual un acto es coercitivo si está diseñado para obligar al Estado víctima a cambiar su comportamiento con relación a un asunto dentro de su *domaine réservé*.[25]

b. El enfoque **basado en los efectos**, bajo el cual la coerción significa privación real del control, es decir, para ser coercitivo, el hecho debe efectivamente privar al Estado de su capacidad de control o gobierno sobre asuntos en su *domaine réservé*.[26]

22 CIJ, *Nicaragua case* [El Caso Nicaragua], párr. 205 (Trad. libre).

23 CIJ, *Nicaragua case* [El Caso Nicaragua], párr. 205; Asamblea General de las Naciones Unidas, *Declaración sobre la inadmisibilidad de la intervención e interferencia en los asuntos internos de los Estados,* A/RES/36/103 (9 diciembre de 1981), Anexo, Parte II, letras f, g, j, l, m y n.

24 Mohamed Helal, 'On Coercion in International Law' [Sobre la coerción en el derecho internacional] (2019) 52(1) *NYU Journal of International Law and Politics* 1, 3. Consulte también Marco Roscini, *International Law and the Principle of Non-Intervention* [Derecho internacional y el principio de la no intervención] (OUP 2024), 147 a 158.

25 Consulte, por ejemplo, las posiciones nacionales de Austria (2024), pág. 5 y 6, Canadá (2022), párr. 22, República Checa (2024), párr. 9 a 11, Estonia (2021), pág. 25, Alemania (2021), pág. 5, Italia (2021), pág. 4 y 5, Países Bajos (2019), pág. 3, Noruega (2021), pág. 4 y Suiza (2021), pág. 3. Esta también fue la perspectiva respaldada por la mayoría de los expertos del *Manual de Tallin 2.0*: consulte *Manual de Tallin 2.0*, comentario sobre la Norma 66, párr. 19.

26 Consulte, por ejemplo, las posiciones nacionales de Australia (2021), pág. 3, Nueva Zelanda (2020), párr. 9 a 10 y del Reino Unido (2022).

Cada enfoque produce diferentes resultados y tiene bases en diferentes consideraciones políticas. Por ejemplo, en un caso que involucra interferencia electoral, que la mayoría de los Estados han acordado que podría equivaler a una intervención prohibida,[27] el *enfoque basado en la intención requeriría* pruebas de que la operación cibernética en cuestión tenía como fin influir en el proceso electoral del Estado. Probar la intención puede ser difícil de lograr, especialmente en el contexto cibernético, que se destaca por su secretismo. Sin embargo, este requisito asegura que las políticas o acciones del Estado que tienen consecuencias no deseadas en el extranjero no se consideren intervenciones prohibidas.

En cambio, el *enfoque basado en los efectos* requeriría probar que la operación cibernética en cuestión produjo resultados concretos que realmente afectaron la capacidad del Estado de llevar a cabo una elección, como desactivar las máquinas de votación o disuadir a los votantes. La desventaja de este enfoque es que la prueba de una relación causal entre ciertos tipos de operaciones cibernéticas, como las operaciones de influencia, y la privación real de la capacidad del Estado de controlar sus asuntos internos o externos puede ser difícil de producir. Este enfoque parece ser motivado por la necesidad de prevenir y castigar las intervenciones perjudiciales, a pesar de la dificultad para obtener pruebas de la intención coercitiva.

Estos enfoques también tienen variaciones. Por ejemplo, la posición conjunta de la UA respalda una versión más amplia del enfoque basado en la intención, donde la coerción es 'una política […] diseñada para imponer restricciones a la voluntad de un Estado extranjero'.[28] De esta manera, desde la perspectiva de la UA, los efectos coercitivos no son necesarios para que ocurra una violación de la no intervención; siempre que haya un política que imponga restricciones, amenazas o intentos infructuosos de interferir podrían constituir una intervención prohibida.[29] Costa Rica tiene una perspectiva incluso más amplia, indicando que es suficiente que un Estado intente coaccionar a otro, emplee métodos coercitivos o eventualmente los cause en otro Estado' para que se incumpla el principio de no intervención.[30] Desde esta perspectiva, la coerción puede demostrarse por diferentes medios, es decir, la presencia de una intención coercitiva, efectos coercitivos o el uso de métodos coercitivos que tienen el potencial de privar a un Estado de su capacidad para controlar o elegir cómo gobernar sus asuntos internos o externos, cualquiera que sea la intención o los efectos causados.[31]

27 Consulte, por ejemplo, las posiciones nacionales de Australia (2021), pág. 3, Brasil (2021), pág. 19, Canadá (2022), párr. 24, Alemania (2021), pág. 5, Israel (2021), pág. 403, Nueva Zelanda (2020), párr. 10, Noruega (2021), pág. 4, Singapur (2021), pág. 83, el Reino Unido (2018, 2021, párr. 9, y 2022) y los Estados Unidos (2016, pág. 13 y 14, 2020, y 2021, pág. 140).

28 Posición conjunta de AU (2024), párr. 31.

29 Posición conjunta de la UA (2024), párr. 32.

30 Posición nacional de Costa Rica (2023), párr. 24.

31 Consulte Antonio Coco, Talita Dias y Tsvetelina van Benthem, 'Ilegal: The SolarWinds Hack under International Law' [Ilegal: El hack de SolarWinds a la luz del derecho internacional] (2022) 33(4)) *European Journal of International Law* 1275, 1280-1281.

Aunque la prohibición de intervenciones solo aplica entre Estados, un Estado puede incumplir su obligación apoyando actos de coerción de actores no estatales.[32] Las violaciones de la prohibición dan lugar a la responsabilidad del Estado.

c. Uso de la fuerza

La prohibición del uso de la fuerza está consagrada en el Artículo 2(4) de la Carta de las Naciones Unidas, que exige a los Estados que 'en sus relaciones internacionales, se abstendrán de recurrir a la amenaza o al uso de la fuerza contra la integridad territorial o la independencia política de cualquier Estado, o en cualquier otra forma incompatible con los Propósitos de las Naciones Unidas'.[33] Esta regla refleja el derecho internacional consuetudinario,[34] y también se ha considerado una norma imperativa de derecho internacional general (o *jus cogens*).[35] No hay duda de que se aplica al contexto cibernético,[36] y como tal, es una característica de virtualmente todas las posiciones nacionales y conjuntas publicadas.

Como se indica con la frase 'en sus relaciones internacionales', la prohibición del uso de la fuerza se **entiende por lo general que aplica solo entre Estados**.[37] Esto significa que los actores no estatales, como grupos de hackers, pandillas de ransomware o movimientos rebeldes está excluidos de este alcance a menos que su conducta sea atribuible a un Estado.[38] Sin embargo, las operaciones cibernéticas de actores no estatales que no son atribuibles a Estados, pero por lo demás equivaldrían

> No hay duda de que la prohibición del uso de la fuerza aplica al entorno cibernético y como tal, figura en virtualmente todas las posiciones nacionales y conjuntas.

32 Harriet Moynihan, *The Application of International Law to State Cyberattacks: Sovereignty and Non-Intervention* [Las aplicaciones del derecho internacional a los ataques cibernéticos estatales: Soberanía y no intervención] (Chatham House 2019), párr. 79.

33 Carta de las Naciones Unidas (adoptada el 26 de junio 1945, en vigor el 24 de octubre de 1945) 1 UNTS 16 (Carta de las Naciones Unidas) Artículo 2(4) (Trad. libre).

34 CIJ, *Consecuencias jurídicas de la construcción de un muro en el territorio palestino ocupado* (Opinión consultiva) [2004] CIJ Rep. 136 (Opinión consultiva del muro), párr. 87; CIJ, Caso Nicaragua, párr. 187 a 190. Consulte también las posiciones nacionales de Brasil (2021), pág. 19, Israel (2021), pág. 398, Suecia (2022), pág. 8 y los Estados Unidos (2021), pág. 137.

35 Consulte, por ejemplo, Christian Tams, 'Artículo 2(4)' en Bruno Simma et al (editores), *La Carta de las Naciones Unidas: Un comentario*, Vol. I (OUP 2024) 359 a 360, párr. 137. Consulte también las posiciones nacionales de Austria (2024), pág. 6, Brasil (2021), pág. 19, Cuba (2024), párr. 12, República Checa (2024), párr. 24 y la posición conjunta de la UA (2024), párr. 38.

36 Consulte Asamblea General de las Naciones Unidas, *Informe del Grupo de Expertos Gubernamentales sobre los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional*, A/76/135 (14 de junio de 2021), párr. 71(b).

37 Consulte más información en Christian Tams, 'Artículo 2(4)' en Bruno Simma et al (editores), *La Carta de las Naciones Unidas: Un comentario*, Vol. I (OUP 2024) 333 a 338, que argumenta que el alcance de la prohibición también se extiende a los 'regímenes de facto estabilizados' y a las organizaciones internacionales.

38 Marco Roscini, *Cyber Operations and the Use of Force in International Law* [Operaciones cibernéticas y uso de la fuerza en el derecho internacional] (OUP 2014), 44.

a uso de la fuerza, desreguladas por el derecho internacional. Dichas actividades pueden dar lugar a responsabilidad penal individual de las personas involucradas (consulte la sección sobre derecho penal internacional a continuación) o implicar la diligencia debida de los Estados que fallan en prevenir, detener o redirigir dichas operaciones (consulte a continuación la sección sobre diligencia debida).

El término **'fuerza' no está definido en el derecho internacional**, pero existe consenso en que la caracterización de una cierta operación como uso de la fuerza no depende de los medios utilizados. Como observó la CIJ en su opinión consultiva sobre Armas Nucleares, la prohibición se aplica a 'cualquier uso de la fuerza, sin importar las armas empleadas'.[39] Esto significa que, en principio, el uso de capacidades cibernéticas podría calificar como uso de la fuerza tanto como lo hace recurrir a medios cinéticos. La prohibición también se extiende a las amenazas de uso de la fuerza, que en el contexto cibernético pueden incluir operaciones con el potencial de resultar en uso de la fuerza o amenazas verbales transmitidas en línea.[40]

En lugar de centrarse en los medios, el enfoque predominante para determinar si una operación cibernética constituye un uso de la fuerza es referirse a sus efectos o consecuencias (el enfoque basado en los efectos). Sobre esta base, han emergido tres categorías amplias de operaciones cibernéticas:

- Muchos Estados sostienen que una operación cibernética califica como uso de la fuerza si produce **efectos comparables a los de un acto convencional (cinético)** incluido en la prohibición. Esto es claro si la operación cibernética resulta en destrucción física o pérdida de vida. Los ejemplos dados en las posiciones publicadas incluyen daños graves a centrales de energía,[41] causar una colisión de trenes[42] o abrir una represa sobre un área poblada.[43]
- No hay tanto acuerdo con respecto a si las operaciones cibernéticas que dan como resultado la **pérdida de funcionalidad** de infraestructura informática sin causar daños materiales califican como uso de la fuerza. Como se menciona en la posición nacional de Italia, dicha interpretación podría justificarse debido a la dependencia de las sociedades modernas de las tecnologías cibernéticas que han hecho posible interrumpir servicios esenciales sin causar daños físicos.[44] Los ejemplos señalados por los Estados incluyen afectar significativamente infraestructura crítica,[45] desactivar o perturbar el funcionamiento de la

39 CIJ, *Legalidad de la amenaza o uso de armas nucleares* (Opinión consultiva) [1996] CIJ Rep. 226 (Opinión consultiva sobre armas nucleares), párr. 39 (Trad. libre).

40 Consulte Duncan B Hollis y Tsvetelina van Benthem, 'Amenaza de uso de la fuerza en el ciberespacio', en Laura A Dickinson y Edward W Berg (editores), *Grandes datos conflicto armado: Cuestiones jurídicas sobre y bajo el umbral del conflicto armado* (OUP 2024).

41 Consulte las posiciones nacionales de Austria (2024), pág. 7 y Polonia (2022), pág. 5.

42 Consulte la posición nacional de Israel (2021), pág. 399.

43 Consulte la posición nacional de Estados Unidos (2012).

44 Consulte la posición nacional de Italia (2021), pág. 8.

45 Consulte la posición nacional de Irlanda (2023), párr. 18.

infraestructura eléctrica,[46] o desactivar sistemas de defensa antimisiles.[47]

- La calificación de las operaciones cibernéticas que causan **perjuicios puramente económicos** es incluso más controversial. Tradicionalmente, la prohibición del uso de la fuerza se considera como limitante para la fuerza armada, excluyendo otras formas de coerción (como la presión económica), que a lo sumo califican con una violación del principio de no intervención.[48] Sin embargo, debido al potencial de las operaciones cibernéticas de causar perjuicios económicos generalizados y significativos, varios Estados ahora han expresado en sus posiciones nacionales su renuencia a descartar que dichas operaciones cibernéticas puedan calificar como uso de la fuerza. Este es uno de los asuntos sobre los cuales se necesitan las perspectivas de más Estados.[49]

La naturaleza sin acordar de estos interrogantes es evidente por la recurrente afirmación de los Estados de que la evaluación de si una operación cibernética califica como uso de fuerza debe ser hecha caso por caso.[50] De esta manera, los Estados mantienen cierto grado de flexibilidad en esta área en rápida evolución. Para promover la seguridad jurídica, los Estados pueden considerar la identificación de criterios para dichas determinaciones. El *Manual de Tallin 2.0* ofrece orientación útil sobre esto, indicando factores como gravedad, invasividad y naturaleza militar de la operación en cuestión.[51] Algunos Estados ya lo han hecho en sus posiciones nacionales.[52]

El uso de la fuerza se considera ilegal a menos que sea consentido por el Estado territorial,[53] autorizado por el Consejo de Seguridad de la ONU[54] o realizado en legítima defensa.[55] **Si el uso cibernético de la fuerza califica como ataque armado**,[56] **el Estado víctima puede invocar el derecho a la legítima defensa**, y

46 Consulte las posiciones nacionales de Costa Rica (2023), párr. 10, y Noruega (2021), pág. 6.

47 Consulte la posición nacional de Polonia (2022), pág. 5, y también la posición conjunta de la AU (2024), párr. 40.

48 Christian Tams, 'Artículo 2(4)' en Bruno Simma et al (editores), *La Carta de las Naciones Unidas: Un comentario*, Vol. I (OUP 2024) 315, párr. 47. Consulte también la posición nacional de Irlanda (2024), párr. 12.

49 Consulte, por ejemplo, las posiciones nacionales de Dinamarca (2023), pág. 451, Francia (2019), pág. 7, Países Bajos (2019), pág. 4 y Noruega (2021), pág. 6.

50 Consulte, por ejemplo, las posiciones nacionales de Canadá (2022), párr. 45, Costa Rica (2023), párr. 36, República Checa (2024), párr. 27, Dinamarca (2023), págs. 451 a 452, Alemania (2021), pág. 6, Italia (2021), pág. 8, Países Bajos (2019), pág. 4, Noruega (2021), pág. 5, Polonia (2022), pág. 5, Rumania (2021), pág. 77, Suecia (2022), pág. 4 y de los Estados Unidos (2021), pág. 137, y también la posición conjunta de la UA (2024), párr. 41.

51 *Manual de Tallin 2.0*, comentario sobre la Norma 69, párr. 9.

52 Consulte, por ejemplo, las posiciones nacionales de República Checa (2024), párr. 27, Dinamarca (2023), pág. 451, Francia (2021), pág. 7, Alemania (2021), pág. 6, Noruega (2021), pág. 5, Países Bajos (2019), pág. 4, Rumania (2021), pág. 77, Singapur (2021), pág. 84 y de los Estados Unidos (2012 y 2021, pág. 137), y también la posición conjunta de la UA (2024), párr. 41.

53 Consulte, por ejemplo, las posiciones nacionales de Australia (2021), pág. 3, y Rumania (2021), pág. 77.

54 Consulte Carta de las Naciones Unidas, artículos 39 a 42.

55 Consulte Carta de las Naciones Unidas, artículo 51.

56 Consulte CIJ, *Nicaragua case* [El Caso Nicaragua], párr. 191 y 195, que sostiene que solo las 'más graves formas de uso de la fuerza' califican como ataques armados e identifica la 'escala y efectos' como los criterios para evaluar si califican como uso de la fuerza.

terceros Estados pueden usar la fuerza en legítima defensa colectiva a su solicitud[57] La CIJ aclaró que solo las 'más graves formas de uso de la fuerza' califican como ataques armados e identifica la 'escala y efectos' como los criterios para evaluar si califican como uso de la fuerza. Este enfoque se refleja en muchas de las posiciones nacionales y conjuntas,[58] siendo Estados Unidos la excepción al señalar que todos los usos de la fuerza califican como ataques armados.[59]

Al igual que con los usos de la fuerza cinética, **no hay un umbral aceptado universalmente para determinar qué usos de la cibernética califican como ataques armados**. Por lo general, los Estados están de acuerdo en que las operaciones que dan como resultado pérdidas de vida significativas o daños físicos sustanciales cumplen el umbral.[60] Los ejemplos dados en las posiciones nacionales publicadas incluyen causar que un reactor nuclear funcione mal, causar graves daños y pérdidas de vidas,[61] o causar interrupciones graves y prolongadas en la infraestructura crítica nacional.[62] En el contexto cibernético, como en los otros, hay un debate en curso sobre si la conducta de actores no estatales puede constituir un ataque armado y, por lo tanto, activar el derecho del Estado víctima a usar la fuerza en legítima defensa en el territorio del Estado donde se originó el ataque.[63]

Cualquier resorte a la legítima defensa debe cumplir los dos **requisitos de necesidad y proporcionalidad**.[64] Primero, el uso de la fuerza en legítima defensa debe ser necesario para repeler el ataque armado. Entonces, si, por ejemplo, para este fin las defensas cibernéticas sin fuerza son suficientes, el Estado estaría impedido para usar la fuerza.[65] En segundo lugar, la proporcionalidad también requiere que la respuesta no exceda lo necesario para contrarrestar el ataque. Es importante anotar que el Estado víctima no está obligado a responder de igual manera; puede usar medios cibernéticos o cinéticos, siempre que se cumplan los requisitos de necesidad y

57 Consulte la Carta de las Naciones Unidas, artículo 51 y CIJ, *Nicaragua case* [El Caso Nicaragua], párr. 195 y 199.

58 Consulte, por ejemplo, las posiciones nacionales de Austria (2024), pág. 7, Brasil (2021), pág. 20, Costa Rica (2023), párr. 37, Dinamarca (2023), pág. 451 a 452, Cuba (2024) párr. 6, República Checa (2024), párr. 29, Francia (2021), pág. 5, Alemania (2021), pág. 15, Italia (2021), pág. 9, Países Bajos (2019), pág. 8, Noruega (2021), pág. 5, Suecia (2022), pág. 4, Suiza (2021), pág. 4, y también las posiciones conjuntas de la UA (2024), párr. 41 y la UE (2024), pág. 10.

59 Consulte la posición nacional de Estados Unidos (2012).

60 Consulte, por ejemplo, las posiciones nacionales de Austria (2024), pág. 7, Francia (2021), pág. 5, Italia (2021), pág. 8, Nueva Zelanda (2020), párr. 7 y del Reino Unido (2018).

61 Consulte las posiciones nacionales de Nueva Zelanda (2020), párr. 8 y del Reino Unido (2018).

62 Consulte las posiciones nacionales de Francia (2021), pág. 5 y 6, Noruega (2021), pág. 6 y Singapur (2021), pág. 84.

63 Consulte, por ejemplo, las posiciones nacionales de Austria (2024), pág. 7 a 8, Dinamarca (2023), pág. 452, Alemania (2021), pág. 16, Israel (2021), pág. 399, Italia (2021), pág. 9, Países Bajos (2019), pág. 9, Polonia (2022), pág. 6 y de los Estados Unidos (2021), pág. 137, quienes dicen todos que los ataques armados pueden ser perpetrados por actores no estatales, mientras que las posiciones nacionales de Brasil (2021), pág. 20 y Francia (2021), pág. 6, argumentan que solo los Estados pueden cometer ataques armados.

64 Consulte CIJ, *Nicaragua case* [El Caso Nicaragua], párr. 176; CIJ, Opinión consultiva sobre armas nucleares, párr. 41; CIJ, *Caso relacionado con plataformas petroleras (Irán vs. Estados Unidos)* (Sentencia) [2003] CIJ Rep. 161, párr. 74.

65 Por ejemplo, consulte la posición nacional de Estados Unidos (2021), pág. 142.

proporcionalidad.[66] Esta flexibilidad garantiza que el derecho a la legítima defensa permanezca en vigor incluso cuando el Estado perpetrador no depende de capacidades cibernéticas.[67]

d. Diligencia debida

'Diligencia debida' hace referencia a un estándar de conducta encontrado en diferentes obligaciones internacionales, como las obligaciones positivas de derechos humanos que se tratan a continuación. También es un resumen de dos obligaciones de la aplicación general del derecho internacional.

El primero es el principio formulado por la CIJ en el caso del Canal de Corfú, que reconoce 'la **obligación de cada Estado de no permitir a conciencia que su territorio sea usado para actos contrarios a los derechos de otros Estados**'.[68] Esta obligación general de prevención está fundamentada en el derecho internacional consuetudinario y es el corolario de la soberanía del Estado.[69] También se puede violar cuando un Estado sabe o debería saber que un acto contrario a los derechos de otro Estado se origina o perpetra a través de su territorio, y no toma las medidas razonables para detenerlo o prevenirlo, y el daño se materializa.[70]

La segunda obligación general de diligencia debida es el principio de 'no hacer daño' hallado en el derecho internacional consuetudinario[71] y reflejado en el proyecto de Artículos sobre la Prevención del Daño Transfronterizo causado por Actividades Peligrosas de la Comisión de Derecho Internacional (CDI).[72] Esta es la obligación de 'adoptar todas las medidas apropiadas para prevenir un daño transfronterizo sensible o en todo caso minimizar el riesgo de causarlo', donde dichos daños se originan en

66 Consulte, por ejemplo, las posiciones nacionales de Austria (2024), pág. 7, Canadá (2022), párr. 47, Estonia (2021), pág. 30, Finlandia (2020), pág. 7, Francia (2021), pág. 6 a 7, Alemania (2021), pág. 15, Israel (2021), pág. 399, Países Bajos (2019), pág. 8, Nueva Zelanda (2020), párr. 24, Noruega (2021), pág. 9, Polonia (2022), pág. 5, Suecia (2022), pág. 4, el Reino Unido (2021), párr. 6 y de los Estados Unidos (2021), pág. 137.

67 Consulte la posición nacional de Polonia (2022), pág. 5.

68 CIJ, *Caso del Canal de Corfú (Reino Unido vs. Albania)* (Fondo) [1949] CIJ Rep. 4, 22 (Trad. libre).

69 Consulte CIJ, *Caso de las Plantas de Celulosa sobre el Río Uruguay (Argentina vs. Uruguay)* (Sentencia) [2010] CIJ Rep. 14, párr. 101; *Isla de Palmas (Estados Unidos vs. Países Bajos)* (1928) II RIAA 829, 839.

70 Consulte Consejo de la Unión Europea, *Declaración de la Unión Europea y sus Estados Miembro sobre un Entendimiento común sobre las aplicaciones del derecho internacional al ciberespacio* (2024), 5; Talita Dias y Antonio Coco, *Diligencia debida en el derecho internacional* (ELAC 2021) 784–789. Según los expertos del *Manual de Tallin 2.0*, se deben cumplir los siguientes criterios acumulados: existencia de un acto contrario a los derechos del Estado víctima, un acto que deba ser realizado desde o mediante la infraestructura que está bajo el control del Estado responsable, un acto que hubiese sido ilegal si es llevado a cabo por el Estado mismo, un acto que tenga consecuencias adversas graves; el Estado tiene conocimiento real o constructivo, y el Estado no toma las medidas posibles para detener el acto. Consulte el comentario en el *Manual de Tallin 2.0* sobre la Norma 6.

71 Consulte *Caso Trail Smelter (Estados Unidos vs. Canadá)* (1941) 3 RIAA 1911, at 1963; CIJ, *Plantas de Celulosa sobre el Río Uruguay (Argentina vs. Uruguay)* (Sentencia) [2010] CIJ Rep. 14, párr. 101, 187, 197, 204 y 223.

72 CDI, *Proyecto de artículos sobre la prevención de los daños transfronterizos causados por actividades peligrosas, con comentarios*, A/56/10 (2001).

el territorio o jurisdicción del Estado y afectan significativamente a las personas, la propiedad o el medioambiente de otros Estados.[73] Aunque el alcance del proyecto de artículos de la CDI estaba limitado a las actividades que causan daños físicos,[74] el principio de 'no hacer daño' nunca tuvo la intención de estar restringido a asuntos ecológicos.[75] Desde una perspectiva, el principio de 'no hacer daño' también aplica al daño no físico, como el perjuicio financiero o reputacional contra un Estado.[76]

En el contexto cibernético, el GEG reconoció que 'los Estados no deben permitir a sabiendas que su territorio sea utilizado para cometer hechos internacionalmente ilícitos utilizando TIC'.[77] Sin embargo, **sigue siendo controversial si la diligencia debida constituye una obligación vinculante aplicable a las operaciones cibernéticas**.

Para algunos Estados, la diligencia debida es simplemente una norma no vinculante en el contexto cibernético.[78] Han señalado cómo el Grupo de Expertos Gubernamentales (GEG) ha enmarcado la diligencia debida como una norma voluntaria y no vinculante del comportamiento responsable de los Estados y la práctica insuficiente de los Estados para apoyar la existencia de dicha obligación en el contexto cibernético. La renuencia a aceptar que la diligencia debida es aplicable en el contexto cibernético parece surgir de la preocupación de que los Estados no podrían prevenir o detener las operaciones cibernéticas maliciosas, dada su naturaleza frecuentemente encubierta y veloz. Por ejemplo, sería difícil impedir la explotación de funciones ocultas perjudiciales en el software si no se tiene conocimiento de las mismas. También hay preocupación de que aceptar la diligencia debida como una obligación vinculante podría conducir a frecuentes incumplimientos de la obligación, invitando a tomar contramedidas y aumentando el riesgo de escalada del conflicto en el ciberespacio.

Sin embargo, en sus posiciones nacionales, una cantidad significativa de Estados ha aceptado que el principio establecido en el caso del Canal de Corfú es aplicable y por lo tanto, vinculante en el ciberespacio así como en otros contextos.[79] Otros pocos Estados también han apoyado las aplicaciones del principio de 'no hacer daño' en el contexto cibernético.[80] Esta perspectiva está motivada por la necesidad

73 CDI, *Proyecto de artículos sobre la prevención de los daños transfronterizos causados por actividades peligrosas, con comentarios*, A/56/10 (2001), artículos 2 y 3..

74 CDI, *Proyecto de artículos sobre la prevención de los daños transfronterizos causados por actividades peligrosas, con comentarios*, A/56/10 (2001), comentario al artículo 1, párrafos 16 y 17.

75 ONU, *Cuarto informe sobre la responsabilidad internacional por las consecuencias injuriosas que surgen de actos no prohibidos por el derecho internacional, por Robert Q. Quentin-Baxter, Relator especial*, A/ CN.4/373 y Corr.1&.2 (27 de junio de 1983), párr. 17.

76 Consulte, por ejemplo, la posición nacional de República Checa (2024), párr. 18; Talita Dias y Antonio Coco, *Diligencia debida cibernética en el derecho internacional* (ELAC 2021) 790–794.

77 Asamblea General de las Naciones Unidas, *Informe del Grupo de Expertos Gubernamentales sobre los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional*, A/70/174 (22 de julio de 2021), párr. 13(c).

78 Consulte, por ejemplo, las posiciones nacionales de Canadá (2022), párr. 26 a 27, Israel (2021), pág. 404, Nueva Zelanda (2020), párr. 16 y del Reino Unido (2021), párr. 12.

79 Consulte, por ejemplo, las posiciones nacionales de Austria (2024), pág. 10, Colombia (2025), pág. 9, Estonia (2019 y 2021, pág. 26), Finlandia (2020), pág. 4, Francia (2019), pág. 10, Alemania (2021), pág. 3, Italia (2021), pág. 6, Japón (2021), pág. 5, Países Bajos (2019), pág. 4, Suiza (2021), pág. 7, y Suecia (2022), pág. 4, y también las posiciones conjuntas de la UA (2024), párr. 21 y la UE (2024), pág. 5

80 Consulte las posiciones nacionales de Costa Rica (2023), párr. 29, República Checa (2024), párr. 18 y Noruega (2021), pág. 7.

de cerrar el vacío de responsabilidad que podría resultar de la dificultad de atribuir las operaciones cibernéticas a Estados y del uso cada vez mayor de proxis en el contexto cibernético. Después de todo, la diligencia debida podría responsabilizar a los Estados por no prevenir, detener o reparar las operaciones cibernéticas perjudiciales llevadas a cabo por actores no estatales o terceros Estados desde su territorio o infraestructura de TICs. Esto incluye actividades realizadas por ciberdelincuentes, como ransomware y ataques a las cadenas de suministro de TI.

Los Estados que han apoyado la diligencia debida como una obligación vinculante han hecho énfasis en que **la obligación es de conducta, en vez de resultado:** los Estados deben tomar las medidas razonables para prevenir, detener y reparar las operaciones cibernéticas maliciosas llevadas a cabo desde o mediante sus territorio o infraestructura. En sus posiciones nacionales, estos Estados también han destacado que la obligación está sujeta al requisito de tener conocimiento real o constructivo, así como la capacidad de tomar medidas factibles en las circunstancias.[81] Por lo tanto, la diligencia debida no debería suponer una carga imposible para los Estados, especialmente los países en desarrollo, obligándolos, por ejemplo, a monitorear constantemente o a prevenir todas las actividades cibernéticas maliciosas que tienen lugar en el territorio del Estado.

Existe acuerdo en que el tema de la diligencia debida necesita estudiarse más. Este es particularmente el caso de lo que significa la diligencia debida en la práctica, es decir, las diversas medidas que los Estados pueden estar obligados a adoptar para prevenir, detener o reparar las actividades cibernéticas maliciosas. Se pueden encontrar ejemplos de dichas medidas en varias normas sobre el comportamiento responsable de los Estados planteadas por el GEG, como las normas 'g' (sobre la protección de infraestructuras críticas), 'h' (sobre las respuestas a las solicitudes de asistencia de otros Estados) y 'j' (sobre la notificación responsable de las vulnerabilidades de las TIC).[82] Otros ejemplos de comportamiento diligente incluyen la promulgación y cumplimiento de un marco jurídico la conformación de un equipo de respuesta informática de emergencia (CERT), la realización de evaluaciones de riesgos cibernéticos y el desarrollo de alianzas público-privadas para mejorar la ciberseguridad.[83]

Existe acuerdo en que la diligencia debida requiere más estudio, particularmente con relación a las medidas prácticas que los Estados deben tomar para prevenir, detener o reparar las actividades cibernéticas maliciosas.

81 Consulte, por ejemplo, las posiciones nacionales de Austria (2024), pág. 10, República Checa (2020 y 2024, párr. 15), Estonia (2019 y 2021, pág. 26), Irlanda (2023), párr. 13, y Japón (2021), pág. 5 y también las posiciones conjuntas de la UA (2024), párr. 23 y la UE (2024), pág. 5

82 Consulte Asamblea General de las Naciones Unidas, *Informe del Grupo de Expertos Gubernamentales sobre los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional*, A/70/174 (22 de julio de 2021), párr. 13.

83 Consulte Talita Dias y Antonio Coco, *Diligencia debida cibernética en el derecho internacional* (ELAC 2021) 165 a 205.

e. El arreglo pacífico de controversias

El arreglo pacífico de controversias es un principio fundamental del derecho internacional, consagrado en la Carta de las Naciones Unidas[84] y que refleja el derecho internacional consuetudinario.[85] Es un corolario de la prohibición del uso de la fuerza y es una obligación vinculante para que los Estados resuelvan sus controversias internacionales por medios pacíficos.[86] Se reconoce ampliamente que esta obligación aplica en el contexto cibernético[87] conforme con el compromiso a menudo reafirmado de los Estados de promover un 'entorno de TIC abierto, seguro, estable, accesible y pacífico'.[88]

Sin embargo, en las posiciones nacionales hay variaciones sobre cómo se articula esta obligación. Algunas la interpretan ampliamente, cubriendo cualquier controversia internacional,[89] una perspectiva apoyada por la redacción simple del Artículo 2(3) de la Carta de las Naciones Unidas, que no impone otras condiciones.[90] Otros limitan la obligación a controversias que 'cuya continuación sea susceptible de poner en peligro el mantenimiento de la paz y la seguridad internacionales'.[91] Este criterio, encontrado en el Artículo 33(1) de la Carta de las Naciones Unidas, también es el que emplea el Manual de Tallin 2.0 para limitar el alcance de la obligación en su conjunto.[92]

La elección de los medios para el arreglo de controversias depende de las partes,[93] y la Carta de las Naciones Unidas ofrece ejemplos, como la negociación, la

84 Carta de las Naciones Unidas, artículos 2(3) y 33.

85 CIJ, *Nicaragua case [El Caso Nicaragua]*, párr. 290.

86 Alain Pellet, 'Arreglo pacífico de controversias internacionales' en Rüdiger Wolfrum (editor), *Enciclopedia del derecho público Max Planck* (edición en línea, OUP 2013), párr. 2 y 3.

87 Asamblea General de las Naciones Unidas, *Informe del Grupo de Expertos Gubernamentales sobre los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional*, A/70/174 (22 de julio de 2015), párr. 28(b) y Asamblea General de las Naciones Unidas, *Informe del Grupo de Expertos Gubernamentales sobre los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional*, A/76/135 (14 de julio de 2021), párr. 71(a). Consulte también las posiciones nacionales de Austria (2024), pág. 11, Canadá (2022), párr. 41, China (2021), pág. 3, Colombia (2025), pág. 10, Costa Rica (2023), párr. 17, República Checa (2024), párr. 21, Estonia (2021), pág. 29, Francia (2019), pág. 2, Japón (2021), pág. 6, Kenia (2021), pág. 54, Singapur (2021), pág. 85, Suiza (2021), pág. 2 y del Reino Unido (2021, párr. 7, y 2022).

88 Consulte, por ejemplo, las posiciones nacionales de Brasil (2021), pág. 17, Colombia (2025), pág. 4, Estonia (2021), pág. 23, Finlandia (2020), pág. 1, Irlanda (2023), párr. 2, Italia (2021), pág. 3, Kenia (2021), pág. 52, Nueva Zelanda (2020), párr. 1, Noruega (2020), pág. 1, Pakistán (2023), párr. 7, Singapur(2021), pág. 83 y Suecia (2022), pág. 1, Suiza (2021), pág. 1 y del Reino Unido (2021), párr. 1, y también la posición conjunta de la UA (2024), párr. 3. (Énfasis añadido).

89 Consulte, por ejemplo, las posiciones nacionales de Canadá (2022), párr. 41, Costa Rica (2023), párr. 17, República Checa (2024), párr. 21, Japón (2021), pág. 6, and Singapur (2021), pág. 85, y también las posiciones nacionales de la UA (2024), párr. 35 y de la UE (2024), pág. 9.

90 Christian Tomuschat, 'Artículo 2(3)' en Bruno Simma et al (editores), *La Carta de las Naciones Unidas: Un comentario*, Vol. I (OUP 2024), 283, párr. 42.

91 Consulte, por ejemplo, las posiciones nacionales de Austria (2024), pág. 11, Estonia (2021), pág. 29, y Suiza (2021), pág. 2.

92 *Manual de Tallin 2.0*, comentario sobre la Norma 65, párr. 2.

93 CIJ, *Jurisdicción de pesqueras (España vs. Canadá)* (Jurisdicción de la Corte) [1998] CIJ Rep. 432, párr. 56.

investigación, la mediación, la conciliación, el arbitraje, el arreglo judicial, el recurso a organismo s o disposiciones regionales.[94] Esta lista no es exhaustiva, y los Estados también pueden emplear otros medios pacíficos adecuados o combinar varios.[95] Sin embargo, como lo afirma la Declaración de Manila de 1982, deben hacerlo de buena fe y en espíritu de cooperación.[96] De acuerdo con la Carta de las Naciones Unidas, el Consejo de Seguridad de la ONU también puede ser convocado por las partes para conciliar una controversia por medios pacíficos, si es posible que esta ponga en peligro el mantenimiento de la paz y seguridad internacional. [97]

En el contexto cibernético, las controversias entre Estados pueden tener dimensiones fácticas y jurídicas:

- Las **controversias fácticas** en el ciberespacio por lo general están centradas en la atribución técnica, es decir, identificar la máquina que fue usada para llevar a cabo determinada operación cibernética e identificar a las personas o grupos involucrados. Esto también puede involucrar preguntas sobre los efectos de la operación, el momento de su ejecución o si realmente se llevó a cabo. En este sentido, los mecanismos de investigación son importantes.[98] Se concibe que en el futuro se desarrollen mecanismos de atribución formales para abordar estos desafíos.[99]
- Las **controversias jurídicas** por lo general se relacionan con si las actividades cibernéticas que afectan adversamente a un Estado se pueden atribuir a otro, y si esto constituye una violación de cualquier regla aplicable del derecho internacional. Dichas controversias podrán someterse a resolución judicial, incluida la CIJ como principal organismo judicial de las Naciones Unidas. Siempre que se cumplan los requisitos de jurisdicción y admisibilidad, la CIJ tiene competencia para adjudicar cualquier disputa sobre asuntos del derecho internacional, incluida la aplicación del derecho internacional a las actividades cibernéticas.

94 Carta de las Naciones Unidas, artículo 33(1).

95 Alain Pellet, *'Arreglo pacífico de controversias internacionales'* en Rüdiger Wolfrum (editor), Enciclopedia del derecho público Max Planck (edición en línea, OUP 2013), párr. 31.

96 Asamblea General de la ONU, *Declaración de Manila sobre el Arreglo Pacífico de Controversias Internacionales*, A/ RES/37/10 (15 de noviembre de 1982), sección I, párr. 5.

97 Carta de las Naciones Unidas, artículo 33(2).

98 Nicholas Tsagourias, 'Controversias cibernéticas como controversias del derecho internacional', en Nicholas Tsagourias, Russell Buchan y Daniel Franchini (editores), *Arreglo pacífico de controversias cibernéticas entre Estados* (Hart 2024), 20.

99 Consulte, por ejemplo, Yuval Shany y Michael N Schmitt, 'Un mecanismo de atribución internacional para las operaciones cibernéticas hostiles' (2020) 96 *International Law Studies* 196.

Puede que los Estados quieran usar sus posiciones nacionales para articular perspectivas sobre cómo se deben resolver las controversias fácticas y jurídicas que involucran las TIC. Esto podría incluir la expresión de perspectivas sobre la posible creación de mecanismos de atribución o investigación de hechos,[100] animando a otros Estados a aceptar la jurisdicción obligatoria de la CIJ o abstenerse de hacerlo,[101] y explorar cómo se pueden usar las TIC para ayudar a conciliar pacíficamente controversias cibernéticas y de otra índole.[102]

Durante los debates multilaterales sobre el uso de las TICs por los Estados y la seguridad internacional, algunos Estados plantearon preocupaciones relacionadas con que las características del ciberespacio podrían animar medidas unilaterales sobre el arreglo pacífico de controversias.[103] Por un lado, es cierto que la obligación de buscar el arreglo pacífico de controversias no limita los demás derechos de los Estados conforme con el derecho internacional, como tomar contramedidas legales y usar la fuerza en legítima defensa para responder a un ataque armado.[104] Por otro lado, como se explicó anteriormente, cualquier uso de esas medidas unilaterales solo está disponible bajo estrictas condiciones. Si esos criterios no se cumplen, los Estados deben llevar a cabo esfuerzos de buena fe para resolver las controversias por medios pacíficos. En cualquier caso, deben abstenerse de tomar medidas que puedan poner en riesgo la paz y seguridad internacional.[105]

En el contexto cibernético, las controversias entre Estados pueden estar relacionadas tanto con los hechos (como atribución técnica) como con el derecho (atribución jurídica o calificación de operaciones que violan el derecho internacional).

100 Consulte, por ejemplo, la posición nacional de Cuba (2024), párr. 23 y 24.

101 Consulte, por ejemplo, las posiciones nacionales de Suiza (2021), pág. 2 y del Reino Unido (2022).

102 Por ejemplo, consulte la posición conjunta de la UA (2024), párr. 37.

103 Asamblea General de las Naciones Unidas, *Resumen del presidente sobre el Grupo de Trabajo de Composición Abierta sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional,* A/ AC.290/2021/ CRP.3 (10 de marzo de 2021), párr. 7.

104 Consulte, por ejemplo, las posiciones nacionales de Canadá (2022), párr. 42, República Checa (2024), párr. 23, Estonia (2021), pág. 29, Singapur (2021), pág. 85.

105 Carta de las Naciones Unidas, artículo 2(3). Consulte también *Manual de Tallin 2.0,* comentario sobre la Norma 65, párr. 12.

f. Autodeterminación

El derecho a la autodeterminación fue reconocido por la Asamblea General de las Naciones Unidas como uno de los 'principios fundamentales del derecho internacional',[106] Está consagrado en la Carta de las Naciones Unidas,[107] el Pacto Internacional de Derechos Civiles y Políticos (PIDCP)[108] y el Pacto Internacional de Derechos Económicos, Sociales y Culturales (PIDESC).[109] Además, se considera ampliamente que refleja el derecho internacional consuetudinario.[110] La obligación correspondiente a respetar este derecho se considera una obligación debida a la comunidad internacional en su conjunto,[111] y posiblemente es una norma imperativa del derecho internacional general (jus cogens).[112]

Aunque el derecho a la autodeterminación es un derecho humano fundamental,[113] difiere de otros derechos debatidos en la sección de derecho internacional de los derechos humanos a continuación, porque es un derecho **colectivo**. El titular del derecho no es una persona, sino un grupo definido, comúnmente denominado 'un pueblo'. Aunque el derecho internacional no define formalmente 'un pueblo', por lo general se entiende que el término se refiere a un grupo con una herencia histórica, cultural o lingüística común y una conexión con un territorio específico, que también se identifica a sí mismo como tal.[114]

La autodeterminación se puede dividir en dimensiones internas y externas. La autodeterminación interna se refiere al derecho de un pueblo a buscar libremente su desarrollo político, económico, social y cultural dentro del marco de un Estado existente.[115] La autodeterminación externa se relaciona con el derecho de un pueblo

106 Asamblea General de la ONU, *Declaración sobre los principios de derecho internacional referentes a las relaciones de amistad y a la cooperación entre los Estados de conformidad con la Carta de las Naciones Unidas*, A/RES/2625.

107 Carta de las Naciones Unidas, artículo 1(2).

108 PIDCP, artículo 1.

109 PIDESC, artículo 1.

110 CIJ, *Consecuencias jurídicas de la separación del Archipiélago Chagos de Mauricio en 1965 (Opinión consultiva) [2019] CIJ Rep. 95 (Opinión consultiva sobre Chagos), párr. 155.*

111 CIJ, *Timor del Este (Portugal v Australia)* (Sentencia) [1995] CIJ Rep. 90, párr. 29; CIJ, Opinión consultiva Wall, párr. 88.

112 Consulte, por ejemplo, CIJ, *Proyecto de artículos sobre la responsabilidad del Estado por hechos internacionalmente ilícitos, con comentarios* (2001) (ARSIWA), comentario del artículo 26, párr. 5; CIJ, Opinión consultiva sobre Chagos, Opinión separada del juez Robinson, párr. 77; CIJ, *Consecuencias jurídicas que surgen de las políticas y prácticas de Israel en el territorio palestino ocupado, incluido el este de Jerusalén* (Opinión consultiva) (19 de julio de 2024), párr. 233 (limitando este hallazgo a las situaciones de ocupación extranjera).

113 CIJ, *Opinión consultiva sobre Chagos*, párr. 144.

114 Milena Sterio, *El derecho a la autodeterminación conforme con el derecho internacional* (Routledge 2013), 16; Tom Sparks, *Autodeterminación en el sistema jurídico internacional* (Bloomsbury 2023), 24.

115 Asamblea General de las Naciones Unidas, *Declaración sobre la concesión de la independencia a los países y pueblos coloniales*, Res 1514 (XV) (14 de diciembre de 1960) 2; CIJ, *Consecuencias jurídicas que surgen de las políticas y prácticas de Israel en el territorio palestino ocupado, incluido el este de Jerusalén* (Opinión consultiva) (19 de julio de 2024), párr. 241.

a determinar su estado internacional, como lograr su independencia como Estado soberano o elegir integrarse a otro Estado.[116] Se acepta generalmente que el derecho a la autodeterminación externa solo surge en circunstancias excepcionales, como cuando un pueblo es objeto de opresión o dominación colonial.[117]

Al momento de escribir esta obra, solo tres posiciones nacionales abordan el derecho a la autodeterminación. Italia se refiere al derecho a la autodeterminación interna como una 'norma auxiliar' del principio de la soberanía.[118] De manera similar, Irán indica que la soberanía se debe 'interpretar conforme a otros principios jurídicos fundamentales', incluida la autodeterminación.[119] Rusia también reconoce las aplicaciones de la autodeterminación de los pueblos en el contexto cibernético, aunque no elabora sobre el tema.[120]

Puede que los Estados quieran clarificar varios aspectos del derecho a la autodeterminación en el contexto cibernético en sus posiciones nacionales o conjuntas.

Primero, se ha argumentado que la **interferencia cibernética en los procesos electorales de otro Estado** puede ser inconsistente con la dimensión interna del derecho a la autodeterminación.[121] Aunque dicha interferencia puede calificar simultáneamente como una violación de los principios de soberanía y/o no intervención, puede que los Estados deseen clarificar las líneas divisorias entre estos conceptos y cómo reconciliarlos en caso de conflictos de normas. Por ejemplo, la interferencia exterior en apoyo del gobierno autónomo y democrático en un Estado con un régimen autoritario puede entrar en tensión con el principio de soberanía, pero ser consistente con el principio de la autodeterminación.[122]

Al momento de escribir esta obra, pocas posiciones nacionales abordan el derecho a la autodeterminación. Sin embargo, varias de sus dimensiones pueden estar implicadas por operaciones cibernéticas y podría ser útil abordarlas en futuras posiciones.

116 Karen Knop, *Diversidad y autodeterminación en el derecho internacional* (CUP 2009), 18.

117 Consulte, por ejemplo, *Referencia de la secesión de Quebec* [1998] 2 SCR 217, párr. 112.

118 Posición nacional de Italia (2021), pág. 4.

119 Posición nacional de Irán (2020), párr. II.5 (Trad. libre).

120 Posición nacional de Rusia (2021), pág. 79.

121 Consulte, por ejemplo, Nicholas Tsagourias, 'Interferencia electoral cibernética, autodeterminación y el principio de la no intervención en el ciberespacio', en Dennis Broeders y Bibi van den Berg (editores), *Gobernar el ciberespacio: Behavior, Power, and Diplomacy* [Comportamiento, poder y diplomacia] (Rowman y Littlefield 2020); Marco Roscini, *International Law and the Principle of Non-Intervention* [Derecho internacional y el principio de la no intervención] (OUP 2024) 399–400.

122 Jens D Ohlin, "¿La interferencia cibernética de Rusia en las elecciones de 2016 violó el derecho internacional?' (2017) 95 *Texas Law Review* 1579, 1597.

En segundo lugar, por lo general se acepta que la autodeterminación incluye el **derecho a ejercer soberanía permanente sobre los recursos naturales**.[123] Como señaló el Secretario General de las Naciones Unidas, António Guterres, 'Hoy en día, las tecnologías digitales son similares a recursos naturales como el aire y el agua'.[124] Al mismo tiempo, los Estados han reconocido, en el Pacto Digital Global, que algunas tecnologías, incluido el software de código abierto y los datos abiertos, se consideran 'bienes públicos digitales' o infraestructura pública digital.[125] Por lo tanto, los Estados deben evaluar cuáles tecnologías o elementos del espacio digital, como el acceso a las redes de comunicación mundial o la asignación equitativa de las direcciones IP, constituyen recursos que son objeto de soberanía permanente o son bienes públicos digitales. Una consecuencia de considerar que dichas tecnologías son objeto de soberanía es que la denegación de dicho acceso podría, en determinados casos, constituir una violación de la autodeterminación.

Tercero, el derecho a la autodeterminación **protege a los pueblos contra actos diseñados para dispersar a la población y socavar su integridad como pueblo**.[126] En el contexto cibernético, esto podría incluir campañas de desinformación a gran escala diseñadas para obligar al movimiento de la población y alterar la composición demográfica de un territorio. Otro ejemplo posible es la imposición de cortes de Internet a las personas por parte del Estado que las controla, privando a las comunidades de acceso a servicios vitales y perturbando la cohesión social. Puede que los Estados deseen articular el alcance hasta el cual los hechos cibernéticos caen dentro del alcance del derecho a la autodeterminación.

123 CIJ, *Caso relativo a las actividades armadas en el territorio del Congo (República Democrática del Congo vs. Uganda)* (Fondo) [2005] CIJ Rep. 168, párr. 244; CIJ, *Consecuencias jurídicas que surgen de las políticas y prácticas de Israel en el territorio ocupado de Palestina, incluido el este de Jerusalén* (Opinión consultiva) (19 de julio de 2024), párr. 240.

124 Asamblea General de la ONU, *Nuestra Agenda Común. Informe de políticas núm. 5: un Pacto Digital Global – un futuro digital abierto, libre y seguro para todas las personas*, A/77/CRP.1/Add.4 (25 de abril de 2023), párr. 31.

125 Asamblea General de la ONU, *Pacto Digital Global*, A/79/L.2 (2024), párr. 14 (Trad. libre).

126 CIJ, *Consecuencias jurídicas que surgen de las políticas y prácticas de Israel en el territorio ocupado de Palestina incluido el este de Jerusalén* (Opinión consultiva) (19 de julio 2024), párr. 239.

3. Regímenes especializados

Esta sección explora cómo tres regímenes especializados del derecho internacional, el derecho internacional humanitario (DIH), el derecho internacional de los derechos (DIDH) y el derecho penal internacional (DPI) se aplican a las actividades cibernéticas. Estos fueron seleccionados porque se abordaron a menudo en las posiciones nacionales emitidas hasta la fecha, aunque otros regímenes también han sido incluidos en las posiciones.[127] Cada régimen proporciona un marco jurídico distinto que rige las actividades cibernéticas que entran dentro de su ámbito de aplicación. Lo que las une es su enfoque común en la protección de las personas frente a daños, incluidos los derivados del uso de tecnologías modernas, como las capacidades cibernéticas.

a. Derecho internacional humanitario

El DIH es un conjunto de reglas que tiene como fin limitar los efectos de los conflictos armados por razones humanitarias. Establece los límites de las conductas de las partes del conflicto y de los Estados más ampliamente, protegiendo así a las víctimas de los conflictos armados, incluyendo a los civiles y la población civil. En la década de 2010, hubo cierto debate entre los Estados con respecto a **si el DIH resultaba aplicable a las operaciones cibernéticas**.[128] Sin embargo, luego del respaldo al informe del GEG en 2021 y su subsecuente adopción por parte de la Asamblea General de la ONU y el GTCA, en la actualidad existe un amplio consenso en que así es, y que afirmar esta aplicabilidad no legitima el conflicto ni fomenta la militarización.[129] Todas las posiciones nacionales que abordan el DIH, incluidas las emitidas por Estados anteriormente escépticos,[130] han apoyado esta perspectiva como un punto de

127 Consulte, por ejemplo, la posición nacional de Austria (2024), pág. 14, que incluye una sección sobre el derecho diplomático y consular.

128 Anders Henriksen, 'El final del camino para el proceso del Grupo de Expertos Gubernamentales (GEG) de la ONU: El futuro de la regulación del ciberespacio' (2019) 5(1) *Journal of Cybersecurity* 1; Eneken Tikk y Mika Kerttunen, *La supuesta desaparición del Grupo de Expertos Gubernamentales (GEG) de la ONU: Una autopsia y apología*, Cyber Policy Institute (2017).

129 Consulte Asamblea General de las Naciones Unidas, *Informe del Grupo de Expertos Gubernamentales sobre los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional*, A/76/135 (14 de julio de 2015), párr. 71(f); Asamblea General de las Naciones Unidas, *Informe del Grupo de Trabajo de Composición Abierta sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional*, A/79/214 (22 de julio de 2024), párr. 36(b)(ii). Consulte también la 34ª Conferencia Internacional de la Cruz Roja y de la Media Luna Roja, *Resolución 2: Protección de la población civil y de otras personas y bienes protegidos ante el posible costo humano de las actividades relacionadas con las tecnologías de la información y las comunicaciones durante conflictos armados*, 34IC/24/R2 (octubre de 2024).

130 Consulte, por ejemplo, la Oficina del representante exterior del Cuba, *'71 AGNU: Cuba en la sesión final 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 2017).

partida.[131] De este modo, el enfoque de los debates internacionales ha cambiado a cómo aplica el DIH en el contexto cibernético.

Existe un amplio consenso entre los estados con relación a que el DIH aplica a las operaciones cibernéticas durante los conflictos armados y que afirmar esta aplicabilidad no legitimiza el conflicto ni promueve la militarización.

Aunque la mayoría de las normas del DIH aplican durante un conflicto armado, **ciertas obligaciones también deben ser observadas durante tiempos de paz**. Entre estos están el deber de respetar y garantizar el respeto del DIH;[132] la obligación de difundir el DIH lo más ampliamente posible, incluso mediante instrucción a las fuerzas armadas;[133] la obligación de llevar a cabo revisiones jurídicas de las nuevas armas, medios y métodos de guerra;[134] y el deber de prevenir y reprimir el uso ilícito de emblemas protectores como la cruz roja, media luna roja y el cristal rojo.[135] Aunque la mayoría de las posiciones publicadas ofrecen poco o ningún detalle sobre estas obligaciones en tiempo de paz, destacar su relevancia en el contexto cibernético ofrece una oportunidad para que los Estados que no prevén participar en conflictos armados enfaticen la importancia del DIH.

La **relación entre las operaciones cibernéticas y los conflictos armados** puede adoptar una de dos formas. Por un lado, las operaciones cibernéticas pueden ser llevadas a cabo como parte de un conflicto armado existente. Siempre que estas operaciones tengan un nexo con el conflicto, están regidas y por lo tanto, limitadas por el DIH. Por otro lado, las operaciones cibernéticas pueden dar lugar a un conflicto armado, donde previamente no lo había. En dichos casos, el surgimiento del conflicto armado activa la aplicación del DIH a todas las conductas conexas a este. El DIH distingue entre los conflictos armados internacionales y no internacionales.

131 Consulte las posiciones nacionales de Australia (2021), pág. 3, Austria (2024), pág. 16, Brasil (2021), pág. 22, Canadá (2022), párr. 48, Costa Rica (2023), párr. 38, Cuba (2024) párr. 16, República Checa (2020 and 2024, párr. 37), Dinamarca (2023), pág. 454, Estonia (2021), pág. 26, Finlandia (2020), pág. 7, Francia (2019), pág. 13, Alemania (2021), pág. 7, Irlanda (2023), párr. 29, Israel (2021), pág. 399, Italia (2021), pág. 9, Japón (2021), pág. 6, Kenia (2021), pág. 54, Países Bajos (2019), pág. 5, Nueva Zelanda (2019), párr. 25, Noruega (2021), pág. 9, Pakistán (2023), párr. 9, Polonia (2022), pág. 7, Rumania (2021), pág. 77, Singapur (2021), pág. 85, Suecia (2022), pág. 6, Suiza (2021), pág. 8, el Reino Unido (2018 y 2021, párr. 22), y de los Estados Unidos (2012, 2016, pág. 8, 2020, and 2021, pág. 138), y también las posiciones conjuntas de la UA (2024), párr. 47 y de la UE (2024), pág. 2.

132 Artículo común 1 de los Convenios de Ginebra de 1949, protocolo adicional I, artículo 1(1); Jean-Marie Henckaerts y Louise Doswald-Beck (editores, *Derecho internacional humanitario consuetudinario: Volumen I, Normas* (CICR y CUP 2005) (Estudio de DIH consuetudinario del CICR) Normas 139 y 144; 26a Conferencia Internacional de la Cruz Roja y de la Media Luna Roja, *Resolución 1: Derecho internacional humanitario: de la ley a la acción*, 26IC/95/R1 (3 de diciembre de 1995), párr. 2.

133 Convenios de Ginebra I/II/III/IV, artículos 47/48/127/144; Protocolo adicional I, artículo 83; Protocolo adicional II, artículo 19.

134 Protocolo adicional I, artículo 36.

135 Consulte Convenio de Ginebra I, artículos 53 a 54.

- Un **conflicto armado internacional** surge cuando se utiliza fuerza armada entre dos o más Estados.[136] En general, se entiende que este criterio no exige un nivel específico de intensidad.[137] Por lo tanto, es de amplio consenso que las operaciones cibernéticas con efectos comparables a los cinéticos pueden dar lugar a un conflicto armado internacional.[138]

- Un **conflicto armado no internacional** se caracteriza por la lucha entre un Estado y un grupo armado organizado no estatal o entre dichos grupos. La identificación de un conflicto armado no internacional puede ser más compleja, ya que debe tener un mayor umbral de intensidad.[139] Aún no se ha determinado si las operaciones cibernéticas, en particular aquellas sin efectos cinéticos, pueden cumplir este requisito.[140] Sin embargo, algunas posiciones nacionales, así como la posición conjunta de la UA, afirman que las operaciones cibernéticas pueden desencadenar un conflicto armado no internacional.[141] Este tema sigue siendo uno de los que necesitan más perspectivas de los Estados.

Otros interrogantes clave que requieren atención de los Estados son los relacionados con el alcance de la **prohibición de ataques contra los civiles y objetos civiles**. Esta prohibición, codificada en el Protocolo adicional a los Convenios de Ginebra y que refleja el derecho internacional consuetudinario,[142] aplica, como el resto del DIH, a las operaciones cibernéticas durante los conflictos armados. Sin embargo, la interpretación de los términos 'ataques' y 'objetos' en el contexto cibernético permanece en discusión.

136 TPIY, *Fiscalía vs. Tadić* (Decisión de la moción de defensa de apelación interlocutoria sobre la jurisdicción) ICTY-94-1-A (2 de octubre de 1995) párr. 70.

137 CICR, *¿Cómo se define el término 'conflicto armado' en el derecho internacional humanitario?*, Documento de Opinión (2024) 9.

138 CICR (editor), *Comentario sobre el Tercer Convenio de Ginebra* (CUP 2021), comentario sobre el artículo 2, párr. 288.

139 Consulte, por ejemplo, TPIY, *Fiscalía vs. Lima* (Sentencia del juicio) ICTY-03-66-T (30 de noviembre de 2005) párr. 84; TPIY, *Fiscalía vs. Boškoski y Tarčulovski* (Sentencia del juicio) ICTY-04-82-T (10 de julio de 2008) párr. 175.

140 CICR (editorial), *Comentario sobre el Tercer Convenio de Ginebra* (CUP 2021), comentario sobre el artículo 3 común, párr. 471; Misión permanente de Liechtenstein ante las Naciones Unidas, *El informe sobre la aplicación del Estatuto de Roma a la guerra cibernética del Consejo de Asesores* (Agosto de 2021), 33 a 36.

141 Consulte, en particular, las posiciones nacionales de Austria (2024), pág. 17, Costa Rica (2023), párr. 43, Francia (2019), pág. 12, Alemania (2021), pág. 7 e Irlanda(2023), párr. 30, y también la posición conjunta de la UA (2024), párr. 49.

142 Protocolo adicional I, artículo 52(1); *Estudio del DIH consuetudinario del CICR*, Normas 1 y 7.

- Primero, un asunto central es determinar **si las operaciones cibernéticas califican como 'ataques'** conforme con el DIH, lo que es un punto de referencia clave para muchas reglas que rigen la conducción de las hostilidades. Además de la prohibición de ataques contra los civiles y objetos civiles, estas incluyen la prohibición de ataques indiscriminados,[143] la de ataques desproporcionados,[144] y la obligación de tomar todas las precauciones posibles para evitar, o al menos reducir, los daños incidentales a personas y objetos civiles al llevar a cabo un ataque.[145] El artículo 49 del Protocolo adicional I define 'ataques' como 'actos de violencia contra el adversario, sean ofensivos o defensivos'. Asumiendo que un ataque se puede definir por sus efectos,[146] las operaciones cibernéticas que causan efectos violentos como muertes, lesiones o daños deberían constituir ataques.[147] Sin embargo, persiste el debate sobre si también califican como tales las operaciones cibernéticas que ocasionan pérdidas de funcionalidad, sin daños físicos a los sistemas objeto de ataque. Un creciente número de Estados apoya una interpretación que incluye la pérdida de funcionalidad,[148] mientras que otros limitan la calificación de ataque a las operaciones que se espera que causen daños físicos.[149] No obstante, parece haber acuerdo en que una operación cibernética puede constituir un ataque cuando se espera que la pérdida de funcionalidad cause daños físicos, lesiones o muertes.[150] Este podría ser el caso de una operación cibernética con la intención de cortar la electricidad en un aeropuerto militar, con el fin de ocasionar la colisión de aeronaves militares.[151] Dado el posible impacto grave de las operaciones cibernéticas sobre los servicios esenciales, incluso sin daño físico, clarificar los límites entre ataques y otras operaciones cibernéticas es fundamental.

- En segundo lugar, también existe un debate sobre la protección de los datos civiles, como las bases de datos de seguridad social, fiscales o electorales, como 'objetos' civiles. Conforme con el DIH, todos los objetos están protegidos de los ataques, incluidos los llevados a cabo por medios cibernéticos, a menos

143 Protocolo adicional I, artículo 51(4); *Estudio del DIH consuetudinario del CICR*, Normas 11 y 12.

144 Protocolo adicional I, artículos 51(5)(b) y 57; *Estudio del DIH consuetudinario del CICR*, Norma 14.

145 Protocolo adicional I, artículo 57; *Estudio del DIH consuetudinario del CICR*, Norma 15

146 Cordula Droege, 'Fuera de mi nube: Guerra cibernética, derecho internacional humanitario y la protección de los civiles' (2012) 94(886) *Revista internacional de la Cruz Roja* 533, 557.

147 Consulte *Manual de Tallin 2.0*, Norma 92.

148 Consulte, por ejemplo, las posiciones nacionales de Austria (2024), pág. 17, Colombia (2025), pág. 13, Costa Rica (2023), párr. 20, Francia (2019), pág. 13, Alemania (2021), pág. 8, Japón (2021), pág. 7 y Nueva Zelanda (2020), párr. 20.

149 Consulte, por ejemplo, las posiciones nacionales de Dinamarca (2023), pág. 455, y Israel (2021), pág. 400-401.

150 *Manual de Tallin 2.0*, comentario sobre la Norma 92, párr. 15.

151 Posición nacional de Israel (2021), pág. 400 a 401.

que califiquen como I.[152] Esto presenta el interrogante **de si los datos civiles califican como objeto civil** y por lo tanto, se benefician de las protecciones del DIH. Algunos Estados adoptan la perspectiva de que los datos, como supuestamente son inmateriales, invisibles e intangibles, no se pueden considerar objetos conforme al DIH.[153] Sin embargo, esta interpretación ha sido criticada por dejar las operaciones cibernéticas dirigidas a los datos civiles por fuera del ámbito de las reglas de conducción de las hostilidades que se relacionan únicamente con objetos civiles, creando así un vacío significativo en la protección.[154] Una perspectiva alternativa promueve una interpretación más amplia del término 'objeto', alineándolo con el propósito humanitario general del DIH.[155] Esto se debe a que las operaciones cibernéticas que interfieren con datos civiles pueden interrumpir los servicios gubernamentales, perjudicar a las empresas privadas y afectar a las personas, lo que subraya la necesidad de ampliar las protecciones del DIH a dichos datos.[156] En consecuencia, un creciente número de Estados adoptan la perspectiva de que los objetos civiles incluyen los datos civiles.[157]

Incluso si ciertas **operaciones cibernéticas caen por fuera del alcance de la prohibición de ataques contra personas y objetos civiles**, estas no dejan de estar reguladas por el DIH. Las reglas pertinentes incluyen la obligación de ejercer cuidado constante para preservar a la población y a los bienes de carácter civil durante las operaciones militares.[158] Otras restricciones prohíben las operaciones dirigidas contra objetos específicamente protegidos, como instalaciones médicas[159] y objetos utilizados para operaciones de asistencia humanitaria, [160] y prohíben las operaciones diseñadas para desactivar objetos que son indispensables para la supervivencia de la población civil, como los sistemas de suministro de agua o la infraestructura agrícola.[161]

152 Consulte Protocolo adicional I, artículo 52(52): 'En lo que respecta a los bienes, los objetivos militares se limitan a aquellos objetos que por su naturaleza, ubicación, finalidad o utilización contribuyan eficazmente a la acción militar o cuya destrucción total o parcial, captura o neutralización ofrezca en las circunstancias del caso una ventaja militar definida'.

153 Consulte, por ejemplo, las posiciones nacionales de Dinamarca (2023), pág. 455, y Israel (2021), pág. 401. Consulte también *Manual de Tallin 2.0*, comentario sobre la Norma 100, párr. 5.

154 Kubo Mačák y Laurent Gisel, 'Las restricciones jurídicas de las operaciones cibernéticas en los conflictos armados', en Rajeswari Pillai Rajagopalan (editor) *Futuro de la guerra y la tecnología: Problemas y estrategias* (Wiley 2022) 148.

155 Consulte, por ejemplo, Robert McLaughlin, 'Los datos como objetivo militar', Instituto Australiano de Asuntos Internacionales (20 de septiembre de 2018).

156 Consulte también Kubo Mačák, 'Objetivos militares 2.0: El caso de la interpretación de los datos informáticos como objetivos conforme al derecho internacional humanitario' (2015) 48 *Israel Law Review* 55.

157 Consulte, por ejemplo, las posiciones nacionales de Austria (2024), pág. 18, Colombia (2025), pág. 18, Costa Rica (2023), párr. 50, Finlandia (2020), pág. 7, Alemania (2021), pág. 8 y Rumania (2021), pág. 78.

158 La aplicación de esta regla a las operaciones cibernéticas ha sido confirmada en la posición nacional de los Estados, incluidos Austria (2024), pág. 18, República Checa (2024), párr. 42, Costa Rica (2023), párr. 52, Dinamarca (2023), pág. 455, Finlandia (2020), pág. 7, Francia (2019), pág. 15 y Alemania (2021), pág. 9.

159 Consulte Convenio de Ginebra I, artículo 19; Convenio de Ginebra IV, artículo 18; Protocolo adicional I, artículo 12; Protocolo adicional II, artículo 11(1); *Estudio del DIH consuetudinario del CICR*, Norma 28.

160 Convenio de Ginebra IV, artículo 59(3), Protocolo adicional I, artículo 70(4); Estudio del DIH consuetudinario del CICR, Norma 32.

161 Protocolo adicional I, artículo 54: Protocolo adicional II, artículo 14; *Estudio del DIH consuetudinario del CICR*, regla 54. Consulte también Consejo de Seguridad de la ONU, res. 2573 (2021) S/RES/2573 (27 de abril de 2021).

Por lo tanto, el DIH sigue imponiendo límites significativos a cómo se pueden realizar operaciones cibernéticas, incluso si no califican como un ataque o si el objetivo al que se dirigen no se considera un objeto civil. Aclarar estas limitaciones ofrece una oportunidad para que los Estados que están desarrollando sus posiciones nacionales o conjuntas fortalezcan aún más la protección de los civiles contra el daño causado por las operaciones cibernéticas durante los conflictos armados.

b. Derecho internacional de los derechos humanos

Existe hoy en día consenso en que los derechos humanos aplican tanto en línea como fuera de ella.[162] Esto significa que los Estados deben respetar, proteger y garantizar los derechos humanos en el ciberespacio de conformidad con sus obligaciones que surgen de los tratados de derechos humanos y el derecho internacional consuetudinario.[163] Los tratados de derechos humanos incluyen el PIDCP y el PIDESC, junto con tratados regionales como el Convenio Europeo de Derechos Humanos (CEDH), la Convención Americana sobre Derechos Humanos (CADH) y la Carta Africana de Derechos Humanos y de los Pueblos (CADHP).[164] Todos ellos prevén órganos judiciales o cuasi judiciales de supervisión de los derechos humanos, entre otros, el Comité de Derechos Humanos (para el PIDCP); el Comité de Derechos Económicos, Sociales y Culturales (para el PIDESC); el Tribunal Europeo de Derechos Humanos (para el CEDH); la Corte Interamericana de Derechos Humanos (para la CADH); y la Corte Africana de Derechos Humanos y de los Pueblos (para la CADHP).

Los tratados internacionales y el derecho internacional consuetudinario [165] reconocen una amplia gama de **derechos humanos que son particularmente relevantes en la era digital**, incluidas las libertades de opinión, expresión y asociación, al igual que los derechos a la privacidad y a la no discriminación. Dada la creciente digitalización de los servicios públicos, los derechos a la vida, educación y salud, además de las condiciones laborales justas y favorables, también pueden verse afectados en el ciberespacio. Por ejemplo, durante la pandemia del COVID-19, las operaciones

162 Consulte, por ejemplo, UNCDH, *Promoción, protección y disfrute de los derechos humanos en Internet*, A/CDH/RES/32/13 (1 julio de 2016), párr. 1; Asamblea General de las Naciones Unidas, *Informe del Grupo de Expertos Gubernamentales sobre los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional*, A/70/174 (22 de julio de 2015), párr. 28(b).

163 CDH, *Observación general núm. 31[31]: La naturaleza de la obligación jurídica general impuesta a los Estados Partes del Pacto*, CCPR/C/21/Rev.1/Add.13 (26 de mayo de 2004) (Observación general 31), párr. 6 a 8.

164 Pacto Internacional de Derechos Civiles y Políticos (16 de diciembre de 1966) 999 UNTS 171; Convención Internacional sobre la Eliminación de todas las Formas de Discriminación Racial (21 de diciembre de 1965) 660 UNTS 195; Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, según enmiendas núm. 11 y 14, ETS 5, (4 de noviembre de 1950); Convención Americana sobre Derechos Humanos, Serie de tratados, núm. 36 (1969); Carta Africana de Derechos Humanos y de los Pueblos, CAB/LEG/67/3 ver. 5, 21 ILM 58 (1982) (27 de junio de 1981).

165 Por ejemplo, los derechos humanos reconocidos en la Declaración Universal de los Derechos Humanos (Resolución de la Asamblea General de la ONU217 A (III) del 10 de diciembre de 1948) se consideran un reflejo del derecho internacional consuetudinario. Consulte ONU, *Proclamación de Teherán, Acto final de la conferencia internacional sobre derechos humanos*, Teherán, 22 de abril a 13 de mayo de 1968, A/CONF.32/41, 3. Consulte también, en general, William A Schabas, *El derecho internacional consuetudinario de los derechos humanos* (OUP 2021).

cibernéticas y de influencia se dirigieron al sector sanitario, arriesgando los esfuerzos para salvaguardar las vidas y la salud de los pacientes.[166] Del mismo modo, la difusión de discursos de odio en línea, además de que puede constituir discriminación ilegal contra las personas, también alimenta la violencia, especialmente en entornos frágiles.[167] Además, la moderación en línea de dicho contenido ha sido realizada por personas que trabajan en condiciones lamentables.[168]

Sin embargo, las obligaciones consagradas en la mayoría de los tratados de derechos humanos aplican solo dentro de la **jurisdicción del Estado**; es decir, dentro del alcance de aplicación de cada tratado.[169] No hay duda de que los Estados tienen jurisdicción sobre los derechos humanos en su territorio: la jurisdicción es principalmente territorial. Pero el alcance de la jurisdicción extraterritorial es controvertido. Esta pregunta es fundamental en el contexto cibernético, porque una cantidad significativa de las operaciones cibernéticas se llevan a cabo desde una infraestructura de TIC ubicada en diferentes Estados y puede afectar remotamente los derechos humanos de personas en los Estados de origen, tránsito y destino. Por ejemplo, la vigilancia electrónica se puede llevar a cabo usando cables y servidores ubicados en varios territorios, y puede socavar la privacidad de personas más allá de las fronteras internacionales. Aunque algunos Estados refutan la aplicación extraterritorial de los derechos humanos,[170] la perspectiva prevaleciente es que dichas obligaciones pueden, al menos en algunas circunstancias, extenderse a las acciones del Estado por fuera de sus fronteras.[171] Diferentes modelos o enfoques de la jurisdicción extraterritorial en materia de derechos humanos han sido apoyados por diferentes Estados y órganos de derechos humanos,[172] como:

a. El **modelo espacial**, por el cual las obligaciones de derechos humanos aplican en áreas que están bajo el control efectivo de un Estado.[173]

b. El **modelo personal**, bajo el cual las obligaciones de derechos humanos surgen cuando un Estado ejerce control o autoridad efectivos sobre las personas.[174]

166 Consulte, por ejemplo, Agencia de ciberseguridad y seguridad de la infraestructura de los Estados Unidos, 'El COVID-19 explotado por actores cibernéticos maliciosos' (8 de abril de 2020); Marko Milanovic y Michael Schmitt, 'Ataques cibernéticos y operaciones de información (desinformación) informática durante una pandemia' (2020) 11(1) *Journal of National Security Law and Policy* 247.

167 Talita Dias, 'Encontrado bases comunes: El derecho a estar libres de incitación a la discriminación, hostilidad y violencia en la era digital' (2024) 16(4) *Responsabilidad global de proteger* 391, 392.

168 Andrew Arsht y Daniel Etcovitch, 'El costo humano de la moderación de contenido en línea', *Jolt Digest* (2 de marzo de 2018).

169 Consulte, por ejemplo, PIDCP, Artículo 2(1), que utiliza la formulación 'todos los individuos que se encuentren en su territorio y estén sujetos a su jurisdicción los derechos reconocidos en el presente Pacto'.

170 Consulte, por ejemplo, las perspectivas de los Estados Unidos expresadas en su posición nacional (2021) y en el Comité de Derechos Humanos de la ONU, *Consideración de los informes presentados por los Estados partes de conformidad con el artículo 40 de la Convención, Tercer informe periódico de los Estados parte para el 2003: Estados Unidos de América*, CCPR/C/USA/3 (2005), 109 a 110.

171 Consulte, por ejemplo, CIJ, *Consecuencias jurídicas que surgen de las políticas y prácticas de Israel en el territorio ocupado de Palestina incluido el este de Jerusalén* (Opinión consultiva) (19 de julio 2024), párr. 99.

172 Para ver un resumen, consulte Marko Milanovic, *Aplicación extraterritorial de los tratados de derechos humanos: derecho, principios y política* (OUP 2011); Priya Urs, Talita Dias, Antonio Coco, y Dapo Akande, *Las protecciones del derecho internacional contra las operaciones cibernéticas que tienen como objetivo el sector sanitario* (ELAC 2023), 170 a 173.

173 TEDH, *Banković y otros vs. Bélgica y otros (Ap. núm. 52207/99)* (12 de diciembre de 2001), párr. 80.

174 TEDH, *Al-Skeini y otros vs. Reino Unido (ap. núm. 55721/07)* (7 de julio de 2011), párr. 136 y 137.

c. El **modelo funcional**, bajo el cual se define la jurisdicción como el control efectivo sobre el disfrute de los derechos humanos, incluso si dicho control se ejerce remotamente, como en el caso de la vigilancia exterior.[175]

El modelo espacial es el más limitante. Surge de la preocupación de que los Estados no pueden respetar, proteger o garantizar los derechos humanos sin control territorial efectivo. En el contexto cibernético, adoptar este enfoque significaría que el Estado no tendría jurisdicción sobre la conducta que tiene lugar en su territorio, sin embargo, afecta los derechos de las personas en otros Estados, como con vigilancia electrónica o interferencia electoral exterior. El modelo personal va un paso más allá al expandir el concepto de jurisdicción a situaciones donde el Estado tiene control físico sobre las personas. Fue concebido originalmente para cubrir situaciones de detención durante un conflicto armado, donde el Estado responsable no tiene control territorial, pero tiene capacidad para violar físicamente los derechos humanos. Sin embargo, este modelo excluiría la mayoría de la actividad remota que afecta los derechos humanos en otros Estados por la ausencia de proximidad física entre los perpetradores y las víctimas. El modelo funcional es el más expansivo, ya que se centra en el disfrute de los derechos humanos, sean físicos o no. Por lo tanto, cubre una amplia gama de actividades en línea, sin importar la proximidad física entre los perpetradores y las víctimas. Este modelo está fundamentado en la idea de que a los Estados no se les permite violar los derechos humanos en otros Estados si no pueden hacerlo en casa. También se ajusta al ritmo acelerado del desarrollo tecnológico y a las nuevas maneras en que la tecnología se puede usar para violar los derechos humanos.

Bajo el derecho internacional consuetudinario, la jurisdicción no es una precondición de las obligaciones de derechos humanos. No obstante, hay un debate sobre el alcance extraterritorial de las obligaciones de derechos humanos consuetudinarias, al igual que sobre la capacidad del Estado para cumplirlas.[176]

175 CDH, *Observación general núm. 36: artículo 6: Derecho a la vida*, CCPR/C/GC/36 (3 de septiembre de 2019) *(Observación general 36)*, párr. 21 y 63. Consulte también Sarah H Cleveland, 'Derecho internacional incorporado y la constitución exterior' (2010) 110 *Columbia Law Review* 225; Yuval Shany, 'Asumir la universalidad con seriedad: Un enfoque funcional a la extraterritorialidad en el derecho internacional de los derechos humanos' (2013) 7 *The Law and Ethics of Human Rights* 47

176 Ryan Fisher (editor), *Manual jurídico operativo* (Departamento de Seguridad Jurídica Nacional, Escuela del Juez Defensor General, Ejército de los Estados Unidos, 2022), 96.

Los Estados tienen obligaciones positivas y negativas de derechos humanos en línea y fuera de línea.

Las obligaciones negativas requieren que los estados respeten los derechos humanos sin interferir ilegalmente en ellos.[177] Las obligaciones positivas requieren que los Estados protejan los derechos humanos de interferencias ilícitas de otros Estados y actores no estatales, y que garanticen las condiciones para la realización progresiva de los derechos humanos tomando medidas activas,[178] Las obligaciones positivas de derechos humanos son obligaciones de conducta medidas por un estándar de diligencia debida: Los Estados deben hacer su mejor esfuerzo para proteger y garantizar los derechos humanos hasta el alcance de su jurisdicción y capacidad de acción.[179] En la era digital, es particularmente importante proteger los derechos humanos de la conducta de actores no estatales, incluidos empresas de tecnología y ciberdelincuentes. Las obligaciones positivas de derechos humanos son independientes de otras obligaciones de diligencia debida, incluidas las de aplicación general que se trataron anteriormente.

La perspectiva prevalente en el momento es que las **corporaciones** no tienen obligaciones de derechos humanos *vinculantes* de conformidad con el derecho internacional.[180] Sin embargo, en su posición nacional, Austria plantea la perspectiva de que 'también se *requiere* que las empresas comerciales, sin importar su tamaño, sector, contexto operativo o estructura, respeten los derechos humanos'.[181] En cualquier caso, de acuerdo con los Principios Rectores sobre las Empresas y los Derechos Humanos de las Naciones Unidas, las empresas tienen la *responsabilidad* de respetar los derechos humanos, lo que incluye ejercer la diligencia debida para identificar, prevenir, mitigar y responsabilizarse por su impacto sobre los derechos humanos en línea y fuera de línea.[182]

Nunca se debe interferir con los **derechos absolutos**, como la libertad de opinión y la prohibición de la tortura, incluyendo por medios cibernéticos. Los **derechos calificados**, como la privacidad y la libertad de expresión, pueden ser objeto de interferencia legal. Las condiciones para dicha interferencia están definidas por las disposiciones de los tratados pertinentes y las normas consuetudinarias. Sin embargo, por lo general, la interferencia legal con los derechos humanos está sujeta a los siguientes requisitos:

177 Consulte, por ejemplo, CDH, *Observación general 31*, párr. 6.

178 CDH, *Observación general 31*, párr. 8; Corte IDH, *Velásquez Rodríguez vs. Honduras*, (Fondo) (Serie C) No 4 (29 de julio de 1988), párr. 177.

179 Consulte Antonio Coco y Talita de Souza Dias, 'Diligencia debida cibernética: Un entramado de obligaciones de protección en el derecho internacional' (2021) 32 *European Journal of International Law* 795.

180 Por ejemplo, consulte la posición conjunta de la UA (2024), párr. 56.

181 Consulte la posición nacional de Austria (2024), pág. 13 (Trad. libre). (Énfasis añadido).

182 Consulte ACNUDH, *'Principios Rectores sobre las empresas y los derechos humanos: puesta en práctica del marco de las Naciones Unidas para 'proteger, respetar y remediar'*, (2011), principios 11 a 15.

a. **Legitimidad:** las limitaciones deben hacerse con un fin legítimo de política pública, como seguridad nacional o protección de los derechos de otras personas.

b. **Legalidad:** las limitaciones deben estar fundamentadas en leyes accesibles y están sujetas a revisión judicial.

c. **Necesidad:** las limitaciones deben ser los medios menos restrictivos para lograr el fin legítimo.

d. **Proporcionalidad:** la limitación en cuestión debe ser conmensurable con la importancia del fin perseguido.[183]

Los Estados deben observar estas condiciones al llevar a cabo operaciones cibernéticas y otras medidas en línea para proteger los fines legítimos, como la vigilancia dirigida a posibles delincuentes y las normas de seguridad en línea.

A la vez que se aumenta la militarización del ciberespacio, también es importante tener en cuenta que el **DIDH sigue aplicando durante los conflictos armados junto con el DIH**.[184] Cuando los dos regímenes ofrecen distintos niveles de protección a los civiles, como en el contexto de ataques específicos, solo se puede determinar cuál es el más adecuado para cada situación analizando cada caso individualmente.[185] Como regla general, cuanto más se aproxime la conducta al campo de batalla, más adecuado será el DIH para regularla, y viceversa.

El incumplimiento de las obligaciones de respetar, proteger o garantizar los derechos humanos puede dar lugar a responsabilidad del Estado. Debido a que los derechos humanos son obligaciones *erga omnes* – obligaciones contraídas con todos los Estados partes de un tratado o con la comunidad internacional en su conjunto – las violaciones de derechos humanos pueden ser invocadas por cualquier Estado parte del tratado pertinente o cualquier Estado en el caso de las obligaciones de derechos humanos consuetudinarias.[186] Como se discute a continuación, sigue la controversia sobre si los Estados no víctimas pueden tomar contramedidas en respuesta a dichas violaciones.

183 CDH, *Observación general 31*, párr. 6; CDH, Observación general núm. 34: artículo 19: Libertad de opinión y libertad de expresión, CCPR/C/GC/34 (12 de septiembre de 2011), párr. 21 a 36.

184 CDH, *Observación general 31*, párr. 11; CIJ, *Opinión consultiva sobre armas nucleares*, párr. 25; CIJ, *Wall Opinión consultiva*, párr. 105 a 106; CIJ, *Caso relacionado con las actividades armadas en el territorio del Congo (República Democrática del Congo vs. Uganda)* (Fondo) [2005] CIJ Rep. 168, párr. 216.

185 Cordula Droege, "¿Afinidades electivas? Derechos humanos y derecho humanitario' (2008) 90 *Revista Internacional de la Cruz Roja* 501.

186 Consulte CDI, *ARSIWA*, artículo 48.

c. Derecho penal internacional

Las personas pueden cometer o facilitar crímenes internacionales (incluidos los crímenes básicos internacionales de agresión, crímenes de guerra, genocidio y crímenes de lesa humanidad) por medios cibernéticos o no cibernéticos. El que una operación cibernética sea o no un crimen internacional dependerá de la interpretación del crimen y de los elementos de cada caso, incluidos la conducta (*actus reus*) y los elementos mentales (*mens rea*), así como los modos de participación. Los crímenes internacionales básicos son punibles conforme al derecho internacional consuetudinario y a ciertos tratados, como el Estatuto de Roma de la Corte Penal Internacional (CPI).[187] Las operaciones cibernéticas que constituyen crímenes internacionales pueden ser juzgadas ante tribunales penales internacionales y nacionales con jurisdicción sobre los presuntos delitos.[188] Esto incluye la CPI, que tiene jurisdicción, por regla general, cuando un elemento del crimen es cometido en un territorio o por un nacional de un Estado parte del Estatuto de la CPI o de un Estado que haya aceptado su jurisdicción.[189]

La operaciones cibernéticas que constituyen crímenes internacionales pueden ser juzgadas ante cortes internacionales o domésticas que tengan jurisdicción sobre los presuntos delitos.

El uso de las TIC para perpetrar o permitir crímenes internacionales está lejos de ser una cuestión meramente teórica. Por ejemplo, en el contexto de la guerra en Ucrania, algunas operaciones cibernéticas dirigidas a personas e infraestructuras civiles pueden, además de ser violaciones del DIH, ser crímenes de guerra.[190] En 2023, el fiscal de la CPI anunció el desarrollo de una política sobre el procesamiento de los 'crímenes cometidos por medios cibernéticos', incluidos los cometidos por medios completamente cibernéticos y casos donde las operaciones cibernéticas han permitido o habilitado conductas no cibernéticas que equivalen a crímenes internacionales.[191] Al momento de escribir este manual, el borrador de política está abierto a comentarios del público.[192] No obstante, hasta la fecha, solo la posición

187 Consulte el Estatuto de Roma de la Corte Penal Internacional (adoptado el 17 de julio de 1998, en vigor desde el 1 de julio de 2002) 2187 UNTS 90 (y sus enmiendas) ("Estatuto de la CPI').

188 Consulte Robert Cryer, Darryl Robinson y Sergey Vasiliev, *Introducción al derecho y procedimiento penal internacional* (CUP 2019), partes II y III.

189 Estatuto de la CPI, artículo 12(12)-(3).

190 Consulte Lindsay Freeman, 'Simposio Ucrania – Responsabilidad por los crímenes cibernéticos', *Articles of War* (14 de abril de 2023); Andy Greenberg, 'El caso de los crímenes de guerra contra los hackers Sandworm de Rusia', *Wired* (12 de mayo de 2022).

191 CPI, 'Declaración del fiscal Karim A.A. Khan KC de la CPI en la conferencia que aborda los crímenes habilitados por la cibernética en el sistema del Estatuto de Roma' (22 de enero de 2024).

192 CPI, 'La oficina del fiscal de la CPI lanza una consulta pública sobre los delitos cometidos mediante medios informáticos bajo el Estatuto de Roma' (7 de marzo de 2025).

nacional de Austria cubre las aplicaciones del DPI en el ciberespacio.[193]

Muchos interrogantes que surgen de la aplicación del DPI en el contexto cibernético surgirán en otros contextos. Por ejemplo, probar la intención necesaria para condenar a alguien por genocidio (la intención de destruir, completa o parcialmente, un grupo nacional, religioso, étnico o racial como tal)[194] puede ser difícil, ya sea que la conducta se lleve a cabo en línea o no. De igual modo, la pregunta sobre si la conducta tiene suficiente gravedad para ser admisible ante la CPI no es exclusiva de la conducta llevada a cabo por medios cibernéticos.[195] Sin embargo, surgen algunos desafíos específicamente de aplicar el DPI a las actividades cibernéticas.

Al interpretar las normas del DPI para evaluar si las actividades cibernéticas constituyen o facilitan crímenes internacionales, se debe respetar el **principio de legalidad y sus corolarios** (no retroactividad, interpretación estricta, prohibición de analogía e in dubio pro reo).[196] Esto significa que las definiciones de crímenes, el elemento mental y los modos de participación no se pueden ampliar más allá de lo que permite razonablemente el texto para condenar a personas por conductas realizadas en el ciberespacio.[197] El principio de legalidad protege a las personas de castigos penales sin aviso justo y es un derecho humano fundamental reconocido en los tratados y el derecho internacional consuetudinario.[198]

La interpretación de **crímenes de guerra** en el contexto cibernético también puede presentar desafíos específicos. Los crímenes de guerra son violaciones graves de los Convenios de Ginebra y otras violaciones graves del DIH.[199] Dirigir ataques contra personas u objetos civiles es un crimen de guerra. Sin embargo, en la jurisprudencia de la CPI, han emergido desacuerdos sobre si la conducta se puede caracterizar como un ataque debido a sus consecuencias,[200] un tema que es particularmente relevante en el contexto cibernético.

193 Consulte la posición nacional de Austria (2024), pág. 20.

194 Convención para la prevención y la sanción del crimen de genocidio (firmada el 9 de diciembre de 1948, en vigor desde el 12 de enero 1951) 78 UNTS 277 (Convención del Genocidio), artículo 2.

195 Consulte Estatuto de la CPI, artículo 17(12)(d). Consulte también Marco Roscini, 'Gravity in the Statute of the International Criminal Court and Cyber Conduct that Constitutes, Instigates or Facilitates International Crimes' [Gravedad en el Estatuto de la Corte Penal Internacional y la conducta cibernética que constituye, instiga o facilita los crímenes internacionales] (2019) 30 *Criminal Law Forum* 247.

196 Consulte, por ejemplo, Estatuto de la CPI, artículos 22 a 24.

197 Consulte Dapo Akande, 'Fuentes del derecho penal internacional', en Antonio Cassese (editor), *Compendio de Oxford sobre derecho penal internacional* (OUP 2009), 44 y 45.

198 Consulte, por ejemplo, PIDCP, artículo 15(1). Consulte también Talita Dias, *Más allá de la justicia imperfecta: Los principios de legalidad y clasificación justa en el derecho penal internacional* (Brill 2022); Kenneth S Gallant, *El principio de legalidad en el derecho internacional y penal comparativo* (CUP 2010).

199 Consulte Estatuto de la CPI, artículo 8(12).

200 En el contexto de la CPI, consulte *Fiscalía vs. Ntaganda, Sentencia de apelaciones sobre las apelaciones de Bosco Ntaganda y el Fiscalía contra la decisión de la Cámara del tribunal VI del 8 de julio de 2019 titulada 'Sentencia'* (30 de marzo de 2021), ICC-01/04-02/06-2666-Red 30-03-2021, párr. 1164 a 1166 y anexo I, Opinión separada de los jueces Morrison y Hofmanski, ICC-01/04-02/06-2666-Anx1.

Como se señala anteriormente, tampoco es claro si las operaciones cibernéticas que causan daños funcionales no físicos pueden considerarse como ataques,[201] y hasta qué punto sus efectos indirectos pueden tenerse en cuenta.[202] De igual manera, la controversia sobre si los datos civiles constituyen un objeto civil es pertinente a la interpretación de los crímenes de guerra, como se discutió anteriormente.[203]

El **genocidio** es la perpetración de actos potencialmente destructivos con la intención de destruir total o parcialmente a un grupo nacional, étnico, racial o religioso como tal.[204] Solo en casos raros se puede cometer un genocidio completamente por medios cibernéticos. Sin embargo, el discurso en línea puede constituir una incitación al genocidio o el delito independiente de incitación directa y pública al genocidio.[205] Sin embargo, no es claro si y hasta qué punto las nuevas formas de expresión en línea, como compartir y dar 'me gusta' a las publicaciones pueden equivaler a participación en genocidio o incitación a este.

Los **crímenes de lesa humanidad** son violaciones graves de los derechos humanos cometidas como parte de un ataque generalizado o sistemático contra una población civil.[206] Pueden llevarse a cabo o facilitarse por medios cibernéticos, como la tecnología de vigilancia.[207] Aunque la mayoría de los actos que equivalen a crímenes de lesa humanidad requieren cierta conducta física (por ejemplo, asesinato, exterminación y tortura), los crímenes de persecución y otros 'actos inhumanos' pueden ser cometidos completamente por medios cibernéticos.

201 Compare, por ejemplo, las posiciones nacionales de Dinamarca (2023), pág. 455 e Israel (2021), pág. 400 que consideran que solo el daño físico puede constituir un ataque, con las posiciones nacionales de Austria (2024), pág. 17, Colombia (2025), pág. 13, Costa Rica (2023), párr. 49, Francia (2019), pág. 13, Alemania (2021), pág. 8, Japón (2021), pág. 7 y Nueva Zelanda (2020), párr. 25, que consideran que las operaciones cibernéticas pueden calificar como 'ataque' sin causar daños físicos si desactivan la funcionalidad del objetivo. Consulte también Misión Permanente de Liechtenstein ante las Naciones Unidas, *El informe del Consejo Asesor sobre la aplicación del Estatuto de Roma a la guerra cibernética* (Agosto de 2021), párr. 12, en el contexto de los crímenes de guerra bajo el Estatuto de la CPI.

202 Compare, por ejemplo, la posición nacional del Reino Unido (2021), párr. 24, con CICI, *DIH y los desafíos de los conflictos armados* (Octubre de 2015), 41

203 Compare, por ejemplo, las posiciones nacionales de Austria (2024), pág. 18, Colombia (2025), pág. 18, Costa Rica (2023), párr. 50, Finlandia (2020), pág. 7, Alemania (2021), pág. 8 y Rumania (2021), pág. 78, que consideran que la protección de los objetos civiles se extiende a los datos civiles, con las posiciones nacionales de Dinamarca (2023), pág. 455 e Israel (2021), pág. 401, que indican que los datos no se pueden considerar un objecto bajo el DIH.

204 Consulte Convención para la prevención y la sanción del crimen de genocidio, artículo 2 y el Estatuto de la CPI, artículo 6.

205 Consulte Convención para la prevención y la sanción del crimen de genocidio, artículo 3(c) y el Estatuto de la CPI, artículo 25(3)(b) y (e).

206 Consulte, por ejemplo, Estatuto de la CPI, artículo 7 y CDI, *Proyecto de artículos sobre la prevención y el castigo de los crímenes de lesa humanidad* (2019), artículo 1.

207 Por ejemplo, Centro Europeo por los Derechos Constitucionales y Humanos, 'Vigilancia en Siria: Empresas europeas pueden estar ayudando y permitiendo crímenes de lesa humanidad'.

El **crimen de agresión** es una violación grave de la prohibición del uso de la fuerza cometida por una persona en posición de liderazgo. En el estatuto de la CPI, un acto de agresión debe también, por su carácter, gravedad y escala, constituir una violación *manifiesta* de la Carta de las Naciones Unidas.[208] Como se discutió anteriormente, algunas operaciones cibernéticas pueden equipararse al uso prohibido de la fuerza si su escala y efectos son comparables al uso de fuerza armada, como cuando dan como resultado pérdidas de vidas o destrucción física. Sin embargo, dada la definición más restrictiva del crimen de agresión y la aplicación del principio de legalidad, solo las operaciones cibernéticas más graves y claramente ilícitas equivaldrían a este crimen.

Los crímenes internacionales se pueden cometer mediante diferentes **formas de participación**.[209] La perpetración conjunta, la complicidad e incitación y la responsabilidad de los jefes y otros superiores, son especialmente relevantes en el ciberespacio porque es más posible que la conducta cibernética *contribuya* a la comisión de un crimen internacional por medios no cibernéticos, en contraposición a que por sí misma constituya dicho crimen. Un interrogante importante que surge en el contexto cibernético es el relacionado con la causalidad; ¿en qué medida los efectos indirectos o reverberantes de las operaciones cibernéticas pueden atribuirse a la conducta en cuestión de la persona? La responsabilidad penal individual probablemente surja si dichos efectos son intencionales. Pero la causalidad se hace crucial cuando la persona puede ser condenada sobre la base de un comportamiento imprudente o negligente. Muchas operaciones cibernéticas que podrían tener consecuencias catastróficas se evitarán gracias a los avances en ciberseguridad, y en esos casos la operación cibernética puede constituir una tentativa de crimen internacional cuando la conducta sea intencional.[210]

208 Consulte Estatuto de la CPI, artículo 8 bis.
209 Consulte Estatuto de la CPI, artículos 25 y 28.
210 Consulte Estatuto de la CPI, artículo 25(12)(f).

4. Responsabilidad del Estado

Esta sección examina cómo se aplica el derecho de la responsabilidad del Estado a las actividades cibernéticas. En términos generales, este régimen jurídico regula la responsabilidad de los Estados por hechos internacionalmente ilícitos y las consecuencias jurídicas que se derivan de dichos actos. Aunque no se han codificado en un tratado vinculante, los *Artículos sobre la responsabilidad del Estado por hechos internacionalmente ilícitos* (2001) de la CDI se consideran ampliamente como reflejo del derecho internacional consuetudinario. Existe un consenso amplio de que estas reglas aplican en el contexto cibernético,[211] pero algunos Estados han notado que su aplicación no siempre es directa, debido a las características particulares de las TIC.[212] Esta sección examina tres temas clave que más llaman la atención en el contexto cibernético: atribución, contramedidas y la invocación de necesidad. Destaca áreas donde hay acuerdos generales, al igual que los aspectos que siguen sin acordarse o son refutados.

a. Atribución

La atribución es uno de los elementos constitutivos de la responsabilidad del Estado, en lo referente a la relación jurídicamente definida entre una acción (u omisión) dada y un Estado.[213] Cuando se cumplen los criterios relevantes, la conducta en cuestión se considera atribuible al Estado, lo que significa que el derecho la trata como la conducta propia del Estado. Si dicha conducta atribuible incumple una obligación jurídica aplicable vinculante para el Estado, constituye un hecho internacionalmente ilícito por el cual el Estado es responsable jurídicamente.[214]

Como norma, la conducta de los órganos del Estado es atribuible al Estado,[215] mientras que las acciones de los actores no estatales no lo son, excepto bajo condiciones específicas.[216]

211 Consulte, por ejemplo, las posiciones nacionales de Australia (2021), pág. 5, Austria (2024), pág. 8, Canadá (2022), párr. 32, Colombia (2025), pág. 14, República Checa (2024), párr. 52, Dinamarca (2023), pág. 452, Estonia (2019 y 2021, pág. 28), Finlandia (2020), pág. 5, Italia (2021), pág. 5 y 6, Noruega (2021), pág. 6, Suecia (2022), pág. 5, Suiza (2021), pág. 5, y también las posiciones conjuntas de la UA (2024), párr. 61 y de la UE (2024), pág. 8. *Consulte también Manual de Tallin 2.0*, 80, párr. 4.

212 Consulte, por ejemplo, la posición nacional de Italia (2021), pág. 6; China (2021), Declaración de las aplicaciones del derecho internacional en el GTCA (16 de diciembre de 2021).

213 CDI, *ARSIWA*, comentario sobre el artículo 2, párr. 12.

214 CDI, *ARSIWA*, artículo 2

215 CDI, *ARSIWA*, artículo 4.

216 Consulte, en particular, CDI, *ARSIWA*, artículo 8.

- **Los órganos estatales** incluyen entidades como las unidades militares cibernéticas, las agencias de inteligencia civil, los funcionarios policiales y cualquier otra entidad o individuo que haga parte de la organización del Estado. El concepto también cubre los órganos que un Estado pone a disposición de otro,[217] como los miembros de los CERT puestos en comisión de servicio a otro Estado y operando bajo la autoridad exclusiva del Estado receptor.[218] Es importante tener en cuenta que la conducta de un organismo del Estado es atribuible al Estado correspondiente incluso si el organismo se extralimita en la competencia o contraviene las instrucciones que recibe (es decir, actúa *ultra vires*).[219]

- Las actividades de los **actores no estatales**, como las operaciones cibernéticas realizadas por hacktivistas individuales, grupos de hackers o pandillas de ransomware pueden ser atribuibles al Estado bajo ciertas condiciones. Esto ocurre cuando actúan con completa dependencia del Estado[220] o bajo sus instrucciones, dirección o control.[221] El grado de control requerido sigue siendo objeto de debate: la CIJ ha afirmado que es necesario el ejercicio de 'control efectivo',[222] mientras que la Corte Penal Internacional para la antigua Yugoslavia desarrolló una prueba de 'control general' menos exigente, aplicable a los grupos organizados con el fin de clasificar un conflicto armado.[223] Solo algunos Estados han adoptado una perspectiva sobre este asunto, y todos los que lo han hecho, han apoyado la prueba de control efectivo. [224] Parece que esto se debe a la preocupación de que una prueba menos exigente de la atribución podría conducir a su abuso. Finalmente, la conducta de un actor no estatal también es atribuible al Estado si el actor estaba facultado por el derecho de ese Estado para ejercer atribuciones del poder público,[225] o si posteriormente el Estado reconoce y adopta la conducta como propia.[226]

Las actividades cibernéticas de actores no estatales pueden atribuirse al Estado cuando se llevan a cabo bajo su control, pero sigue en disputa el umbral de control necesario.

217 CDI, *ARSIWA*, artículo 6.

218 *Manual de Tallin 2.0*, comentario sobre la Norma 16, párr. 4.

219 CDI, *ARSIWA*, artículo 7.

220 CIJ, *Nicaragua case* [El Caso Nicaragua], párr. 110; CIJ, *Caso relacionado con la aplicación de la Convención para la prevención y la sanción del crimen de Genocidio (Bosnia y Herzegovina vs. Serbia y Montenegro)* (Sentencia) [2007] CIJ Rep. 43 (Caso del genocidio bosnio), párr. 392.

221 CDI, *ARSIWA*, artículo 8.

222 CIJ, N*icaragua case* [El Caso Nicaragua], párr. 115; CIJ, *Caso del genocidio bosnio*, párr. 400.

223 TPIY, *Fiscalía vs. Tadić* (Sentencia de apelación) IT-94-1-A (15 de julio de 1999), párr. 116 y ff.

224 Consulte las posiciones nacionales de Brasil (2021), pág. 21, Irlanda (2023), párr. 22, Países Bajos (2019), pág. 6 y Noruega (2021), pág. 6.

225 CDI, *ARSIWA*, artículo 5.

226 CDI, *ARSIWA*, artículo 11.

Cuando un Estado víctima invoca la responsabilidad internacional de otro Estado por una actividad cibernética, implica que considera que la actividad es atribuible a dicho Estado. Aunque el derecho internacional no regula los pasos procedimentales para hacer dichas determinaciones, generalmente se acepta que cualquier acusación de acto ilícito debe estar razonablemente fundamentada.[227] Sin embargo, los Estados no están obligados en virtud del derecho internacional a divulgar públicamente la evidencia sobre la que basan su atribución. Esta interpretación también ha sido afirmada en varias posiciones nacionales.[228]

Incluso si una actividad cibernética no es atribuible a un Estado, de todas maneras el Estado puede ser responsable bajo ciertas circunstancias excepcionales por no haber adoptado las medidas razonables para prevenir, detener o reparar la actividad. Dicha responsabilidad no surge de la actividad misma, sino de la omisión de acción del Estado conforme con sus obligaciones de diligencia debida, que anteriormente se expusieron con mayor detalle.

b. Contramedidas

Las contramedidas son respuestas a hechos internacionalmente ilícitos que, de lo contrario, serían ilícitos, pero se permiten para inducir al Estado responsable de la conducta ilícita a cumplir sus obligaciones conforme con el derecho internacional.[229] Son una circunstancia que excluye la ilicitud y están bien fundamentadas en el derecho internacional consuetudinario.[230] Las contramedidas deben distinguirse de las medidas de retorsión, que son hostiles, pero legales por parte de la víctima contra el Estado responsable (como suspender las relaciones diplomáticas). [231]

227 Asamblea General de las Naciones Unidas, *Informe del Grupo de Expertos Gubernamentales sobre los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional*, A/70/174 (22 de julio de 2015), párr. 28(f) y Asamblea General de las Naciones Unidas, *Observación general No. 31 [80], Naturaleza de la obligación jurídica general impuesta a los Estados Partes en el Pacto*, A/76/135 (14 de julio de 2021), párr. 71(g). Consulte también, por ejemplo, las posiciones nacionales de Brasil (2021), pág. 21, Alemania (2021), pág. 12, Rusia (2021), pág. 80 y Suiza (2021), pág. 6.

228 Consulte, por ejemplo, las posiciones nacionales de Australia (2021), pág. 5, Canadá (2022), párr. 33, República Checa (2024), párr. 58, Dinamarca (2023), pág. 452, Finlandia (2020), pág. 6, Francia (2019), pág. 11, Alemania (2021), pág. 12, Israel (2021), págs. 404-405, Italia (2021), pág. 5, Países Bajos (2019), pág. 6, Nueva Zelanda (2020), párr. 20, Suecia (2022), pág. 5, Suiza (2021), pág. 6, el Reino Unido (2018 y 2021, párr. 15), y de los Estados Unidos (2016, pág. 19 y 2021, pág. 141), y también la posición conjunta de la UE (2024), pág. 8.

229 CDI, *ARSIWA*, comentario sobre la parte 3 del capítulo 3, párrafo 1.

230 CDI, *ARSIWA*, artículo 22, párr. 1 y 2, y comentario sobre el capítulo II de la parte tres, párr. 1.

231 Elizabeth Zoller, *Reparaciones unilaterales en tiempos de paz: Un análisis de las contramedidas* (Transnational 1984) 5.

La mayoría de los Estados acepta las aplicaciones de las contramedidas a las operaciones cibernéticas.[232] Esto se debe a que las contramedidas son uno de los pocos caminos que tienen los Estados para hacer cumplir el derecho internacional en ausencia de un cuerpo de policía global.[233]

Con el aumento y sofisticación de las operaciones cibernéticas ilícitas, las contramedidas son una herramienta importante para la responsabilidad en el ciberespacio.

Sin embargo, al menos un Estado, Brasil, ha cuestionado su estado consuetudinario en general.[234] Esta perspectiva parece basarse en las objeciones planteadas por varios países en desarrollo a la inclusión de contramedidas en los artículos de la CDI sobre responsabilidad del Estado a principios de los 2000.[235] Otros han condenado el recurso a contramedidas en el contexto cibernético por temor a una escalada del conflicto y a la militarización del ciberespacio.[236] El tema es controversial, y por esto, por ejemplo, está excluido expresamente de la posición conjunta de la UA.[237]

Para garantizar que no se abuse de las contramedidas, conforme con el derecho internacional general, les aplican **condiciones sustantivas y procedimentales** estrictas. Es de destacar que las contramedidas deben estar dirigidas únicamente a inducir el cumplimiento, dirigidas al Estado responsable, ser proporcionales al perjuicio sufrido, con efectos temporales y reversibles tanto como sea posible y coherentes con ciertas obligaciones internacionales, como la prohibición del uso de la fuerza y el respeto por los derechos humanos fundamentales.[238] Pero las contramedidas no tienen que ser iguales o del mismo tipo; en otras palabras, el derecho internacional no precluye el uso de contramedidas cibernéticas para responder a un hecho internacionalmente ilícito, y viceversa. Además, antes de tomar contramedidas, el Estado víctima debe primero llamar al Estado responsable a que cumpla con sus obligaciones internacionales. Como regla general, el Estado

232 Consulte, por ejemplo, las posiciones nacionales de Australia (2021), pág. 5, Austria (2024), pág. 8, Canadá (2022), párr. 34, Costa Rica (2023), párr. 13, Dinamarca (2023), pág. 453, Estonia (2019 y 2021, pág. 28), Finlandia (2020), pág. 5, Francia (2019), pág. 8, Alemania (2021), pág. 13, Irlanda (2023), párr. 25, Israel (2021), pág. 405, Italia (2021), pág. 7, Japón (2021), pág. 4, Países Bajos (2019), pág. 7, Nueva Zelanda (2020), párr. 21, Noruega (2021), pág. 8, Polonia (2022), pág. 7, Rumania (2021), pág. 79, Rusia (2021), pág. 80, Singapur (2021), pág. 84, Suecia (2022), pág. 6, Suiza (2021), pág. 6, el Reino Unido (2018, 2021, párr. 17, y 2022), y de los Estados Unidos (2016, pág. 20, 2020, 2021, pág. 142), y también la posición conjunta de la UE (2024), pág. 9.

233 CDI, *ARSIWA*, comentario, capítulo II de la parte tres, párr. 1.

234 Consulte la posición nacional de Brasil (2021), pág. 21.

235 Consulte, por ejemplo, Asamblea General de las Naciones Unidas, *Informe de la Comisión de Derecho Internacional sobre la labor realizada en su 52° período de sesiones*, A/CN.4/513 (15 febrero de 2001), párr. 149, que refleja las contramedidas que 'prefieren los Estados más poderosos' en detrimento de los más 'pequeños y débiles'.

236 Consulte las posiciones nacionales de China (2021), pág. 1 y Cuba (2024) párr. 8.

237 Consulte la posición conjunta de la UA (2024), párr. 10.

238 CDI, *ARSIWA*, artículos 49 a 51.

víctima también debe notificar al Estado responsable y ofrecerse a negociar con este antes de recurrir a contramedidas, a menos que la urgencia exija medidas inmediatas, por ejemplo, para preservar sus derechos.[239] Las contramedidas se pueden tomar mientras las negociaciones están en curso, o si hay una controversia pendiente ante un organismo de solución de controversias. Pero, deben suspenderse si el organismo de solución de controversias tiene el poder para emitir decisiones vinculantes ordenando medidas equivalentes y si la anterior violación ha cesado.[240]

Hay cierto debate sobre cómo se aplican estas condiciones generales en el contexto cibernético. Por ejemplo, en sus posiciones nacionales, algunos Estados han argumentado que el requisito de exigencia previa puede ser dispensado en casos urgentes.[241] Subyacente a esta perspectiva está la preocupación de que, al hacer una exigencia previa, el Estado víctima puede perder el elemento sorpresa o revelar capacidades cibernéticas sensibles.[242]

La noción de **contramedidas colectivas**, las tomadas por los Estados diferentes del Estado víctima, sigue siendo controvertida, especialmente en el ciberespacio.[243] El uso inconsistente del término añade incertidumbre al asunto. El debate sobre si las contramedidas colectivas son legales ha ganado impulso particular dada la formación de alianzas cibernéticas y respuestas conjuntas a las operaciones cibernéticas maliciosas.[244] Algunos Estados han expresado su apoyo a la toma de contramedidas para el interés general; es decir, en respuesta a violaciones de las obligaciones erga omnes, como las que protegen los derechos humanos.[245] Una cantidad menor de Estados también apoya tomar contramedidas en nombre de terceros Estados víctimas, sin importar el tipo de obligación violada.[246] El apoyo a las contramedidas colectivas está fundamentado en la idea de la solidaridad internacional y en la protección de los derechos humanos y otros valores colectivos. Las contramedidas colectivas también podrían abordar las asimetrías en capacidades cibernéticas, permitiendo que los Estados más capaces las tomen en nombre de los más pequeños. Sin embargo, otros Estados han rechazado la permisibilidad

239 CDI, *ARSIWA*, artículo 52(1)-(2).

240 CDI, *ARSIWA*, artículo 52(3).

241 Consulte las posiciones nacionales de Costa Rica (2023), párr. 14, Italia (2021), pág. 7, Suiza (2021), pág. 6, el Reino Unido (2018 y 2021, párr. 19), y de los Estados Unidos (2016, pág. 22, 2020 y 2021, pág. 142).

242 Consulte Henning Lahmann, Reparaciones unilaterales para las operaciones cibernéticas: Legítima defensa, contramedidas, necesidad y el interrogante de la atribución (CUP 2020), 138.

243 Consulte Talita Dias, Contramedidas en el derecho internacional y su rol en el ciberespacio (Chatham House 2024) 33 a 54.

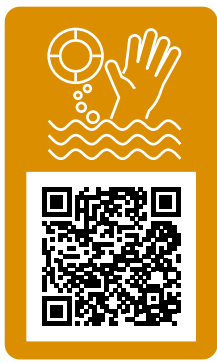
244 Consulte, por ejemplo, Ashley Deeks, 'Defensa preventiva y contramedidas cibernéticas', Hoover Working Group on National Security, Technology, and Law (2020), 8–9; Michael N Schmitt and Sean Watts, "¿Contramedidas cibernéticas colectivas?' (2021) 12 *Harvard National Security Journal* 373.

245 Consulte, por ejemplo, las posiciones nacionales de Austria (2024), pág. 9, Colombia (2025), pág. 17, Irlanda (2023), párr. 25 a 26, y Polonia (2022), pág. 8

246 Consulte, por ejemplo, las posiciones nacionales de Costa Rica (2023), párr. 15, y Estonia (2019).

de las contramedidas colectivas conforme con el derecho internacional.[247] Las preocupaciones sobre una carrera armamentística cibernética, efectos desproporcionados, escalada de conflictos y la desestabilización de las relaciones de los tratados parecen fundamentar estas perspectivas.[248] La posición de que los Estados han tomado contramedidas colectivas en otros contextos, como la guerra en Ucrania, también determina sus perspectivas en el contexto cibernético.[249]

Finalmente, algunos Estados han sugerido que terceros Estados pueden ayudar o asistir al Estado víctima en la toma de sus contramedidas, incluso en el contexto cibernético.[250] Esta perspectiva se basa en la comprensión de que el Estado víctima actúa jurídicamente y, de igual manera, el que asista no incurre en responsabilidad internacional, siempre que su asistencia, que puede incluir medidas como la provisión de fondos, inteligencia, entrenamiento o equipo, sea legal en sí misma a la luz del derecho internacional.[251]



c. Necesidad

Como las contramedidas, invocar el estado de necesidad es una circunstancia que precluye la ilicitud de la conducta que de otra manera sería inconsistente con las obligaciones internacionales del Estado. La mayoría de los Estados están de acuerdo con que la necesidad está fundamentada en el derecho internacional consuetudinario y la CIJ así lo reconoce.[252] Pero esta es una defensa excepcional porque solo está disponible cuando hay un **peligro grave e inminente contra intereses esenciales** del Estado, su pueblo o la comunidad internacional.[253] Incluso bajo esas circunstancias, la acción del Estado no debe afectar gravemente los intereses esenciales de los Estados afectados la comunidad internacional.[254] Esto significa que el impacto de los actos justificados

247 Consulte, por ejemplo, las posiciones nacionales de Canadá (2022), párr. 37, y Francia (2021), pág. 4

248 Consulte, por ejemplo, Asamblea General de las Naciones Unidas, *Sexta Comisión, Registro resumido de la reunión 15,* A/C.6/55/SR.15 (13 de noviembre de 2000), párr. 25 (Israel); Asamblea General de las Naciones Unidas, *Sexta Comisión, Registro resumido de la reunión 14,* A/C.6/55/SR.14 (10 de noviembre de 2000), párr. 31 (Reino Unido); y China, 'Declaración de la delegación china en el debate temático de la Primera Comisión del AGNU 27' (2017).

249 Consulte, por ejemplo, Consejo de la UE (2023), 'Sanciones de la UE – Nuevo recital en la decisión del Consejo', (CFSP) 2023/191 del 27 de enero de 2023 – Contramedidas, WK 5169/2023 INIT, párr. 4; Italia, Tribunal administrativo regional de Lazio (Segunda sesión), núm. 08669/2022 REG.PROV. COLL, núm. 04902/2022 REG.RIC., Sentencia (2022).

250 Consulte, por ejemplo, las posiciones nacionales de Canadá (2022), párr. 37 y Dinamarca (2023), pág. 454.

251 CDI, *ARSIWA*, comentario sobre el artículo 16, párr. 5 y 6; Talita Dias, *Contramedidas en el derecho internacional y su rol en el ciberespacio* (Chatham House 2024) 50 a 54; Miles Jackson y Federica Paddeu, 'Las contramedidas de los demás' (2024) 118(2) American Journal of International Law 231, 254–255.

252 Consulte CDI, ARSIWA, comentario sobre el artículo 25, párr. 14; CIJ, Proyecto Gabčíkovo-Nagymaros (Hungría/Eslovaquia (Sentencia) [1997] CIJ Rep. 7, párr. 51.

253 CDI, *ARSIWA*, artículo 25(1)(a) y comentario, párr. 15.

254 CDI, *ARSIWA*, artículo 25(1)(b).

por la invocación del estado de necesidad no debe ser mayor que el daño que se evita.[255] Es más, la invocación del estado de necesidad no está disponible para Estados que han contribuido sustancialmente a la situación en la cual se hallan o cuando la obligación internacional en cuestión excluye la defensa.[256] Por ejemplo, la necesidad no puede justificar violaciones de la prohibición del uso de fuerza, que tiene sus propias excepciones.[257]

En sus posiciones nacionales, varios Estados han reconocido la aplicabilidad del estado de necesidad en el contexto cibernético.[258] La necesidad también se ha sugerido como posible justificación para las operaciones cibernéticas defensivas contra perjuicios en curso o inminentes, lo que frecuentemente se denomina 'defensa cibernética activa' o 'defensa avanzada'.[259]

Al contrario de las contramedidas, **invocar el estado de necesidad puede hacerse incluso cuando no hay una violación del derecho internacional por parte de un Estado**. Esto significa que la defensa no depende de la atribución y está disponible como respuesta a los actos de actores no estatales. Además, el estado de necesidad puede justificar acciones que de otro modo violarían los derechos de Estados no responsables, si las anteriores condiciones se cumplen. Es más, la necesidad no depende del daño real y puede invocarse preventivamente contra amenazas inminentes. Como lo indican los Países Bajos en su posición nacional, la necesidad 'está principalmente dirigida a otorgar al Estado la oportunidad de proteger sus propios intereses y minimizar el daño que sufre'.[260]

Estas características hacen que la invocación del estado de necesidad sea particularmente atractiva en el contexto cibernético, dados los desafíos de atribución que se trataron anteriormente. Sin embargo, los Estados han hecho énfasis en la naturaleza excepcional de la defensa y las condiciones muy estrictas a las cuales está sujeta. Esto es para evitar el abuso y el riesgo de escalada del conflicto, lo que podría ser especialmente alto en el entorno de ritmo rápido e interconectado del ciberespacio.

Al contrario de las contramedidas, invocar el estado de necesidad puede hacerse sin que otro Estado haya actuado ilícitamente, lo que la hace atractiva en el contexto cibernético donde la atribución a menudo es incierta.

255 CDI, *ARSIWA*, comentario sobre el artículo 25, párr. 1 y 17.

256 CDI, *ARSIWA*, artículo 25(2).

257 CDI, *ARSIWA*, comentario sobre el artículo 25, párr. 21.

258 Consulte las posiciones nacionales de Costa Rica (2023), párr. 16, República Checa (2024), párr.61, Francia (2019), pág. 8, Alemania (2021), pág. 14, Japón (2021), pág. 5, Países Bajos (2019), pág. 7-8, Noruega (2021), pág. 9, Suecia (2022), pág. 6, Suiza (2021), pág. 7 y también la posición conjunta de la UE (2024), pág. 9.

259 Consulte 'Aplicar la invocación de necesidad a las operaciones cibernéticas', resumen de reunión, Chatham House, Programa de Derecho Internacional (27 de septiembre de 2023); Henning Lahmann, 'la invocación de necesidad en las emergencias cibernéticas' (2023) 92 *Nordic Journal of International Law* 422.

260 Posición nacional de Países Bajos (2019), pág. 8 (Trad. libre).

Se ha notado que la necesidad está **disponible como respuesta a daños físicos y no físicos**.[261] En sus posiciones nacionales, algunos Estados han propuesto los siguientes ejemplos de operaciones cibernéticas que podrían equivaler a un 'peligro grave e inminente' a un 'interés esencial' y, por lo tanto, activar la invocación de necesidad: un corte de Internet[262] y una operación cibernética dirigida a infraestructura crítica,[263] como una central nuclear.[264] En este contexto, inminencia no solo significa peligros próximos en el tiempo, sino también los que son ciertos o inevitables.[265]

5. Conclusión

Este capítulo ofrece un resumen de los temas jurídicos sustantivos claves para la preparación de posiciones nacionales sobre la aplicación del derecho internacional a las actividades cibernéticas. Su selección fue orientada por las posiciones publicadas hasta ahora, debates multilaterales en curso en el GTCA y consultas a puerta cerrada organizadas en el contexto de este proyecto.

El capítulo se estructuró alrededor de tres categorías amplias. Primero, comienza con los principios fundamentales del derecho internacional, lo que incluye soberanía, no intervención, prohibición del uso de la fuerza, diligencia debida, arreglo pacífico de controversias y autodeterminación. Segundo, se evalúan las aplicaciones e interpretación de tres regímenes especializados del derecho internacional: DIH, DIDH y DPI. En tercer lugar, se analizó el derecho de la responsabilidad del Estado, con un enfoque en la atribución, las contramedidas y la invocación del estado de necesidad.

En todas estas áreas, el análisis reveló importantes puntos de convergencia y divergencia entre los Estados. Los Estados están de acuerdo en que el derecho internacional es aplicable al uso de las TIC en general y con relación a los regímenes específicos explorados en este capítulo. También, a menudo están de acuerdo sobre los elementos de las reglas aplicables (por ejemplo, que un acto debe referirse a asuntos que formen parte de los asuntos internos o externos de un Estado y ser de naturaleza coercitiva para constituir una intervención prohibida). Y, en ocasiones hay acuerdo en que un tema, como la diligencia debida, debe estudiarse más.

261 Consulte, por ejemplo, las posiciones nacionales de República Checa (2024), párr. 68, Alemania (2021), pág. 15 y Países Bajos (2019), pág. 8.

262 Posición nacional de Países Bajos (2019), pág. 8.

263 Posición nacional de Alemania (2021), pág. 14 y 15.

264 Consulte 'Aplicar la invocación de necesidad a las operaciones cibernéticas', resumen de reunión, Chatham House, Programa de Derecho Internacional (27 de septiembre de 2023), párr. 5.

265 CIJ, Proyecto Gabčíkovo-Nagymaros (Hungría/Eslovaquia) (Sentencia) [1997] CIJ Rep. 7, párr. 54.

Al mismo tiempo, subsisten diferencias importantes. Estas incluyen interrogantes sobre si cierto estándar jurídico constituye una regla autónoma en el contexto cibernético (como el caso de la soberanía y la diligencia debida), cuál es el umbral en el cual una operación cibernética califica como violación de una regla en cuestión (por ejemplo, la soberanía y las prohibiciones de uso de la fuerza e intervención), y cómo calificar una categoría de conducta realizada por medios cibernéticos (como el espionaje cibernético). Estas divergencias sirven como incentivo para que los Estados continúen desarrollando sus perspectivas y contribuyan a los debates en curso.

Para los Estados que están desarrollando posiciones nacionales, el resumen de este capítulo ofrece una hoja de ruta para seleccionar qué temas o asuntos incluir (o evitar), navegar los puntos de controversia, formar sus perspectivas sobre los diversos asuntos y, en última instancia, lograr entendimientos comunes sobre cómo aplica el derecho internacional en el contexto cibernético. Una vez que estos interrogantes sustantivos hayan sido abordados, el paso a seguir es decidir cómo se debe presentar la posición nacional, incluidos el formato, estilo, lenguaje y las estrategias de difusión. Es sobre esto que trata el siguiente capítulo.

		Posiciones conjuntas													
		AU	EU	AU	AT	BR	CA	CN	CO	CR	CU	CZ	DK	EE	FI
Reglas y principios fundamentales y principios	Soberanía	●	●	●	●	●	●	●	●	●	●	●	●	●	●
	No intervención	●	●	●	●	●	●	●	●	●	●	●	●	●	●
	Uso de la fuerza	●	●	●	●	●	●	●	●	●	●	●	●	●	●
	Diligencia debida	●	●	●	●	●	●	●	●	●		●	●	●	●
	Arreglo pacífico de controversias	●	●	●	●	●	●	●	●	●	●	●		●	
	Autodeterminación														
Regímenes especializados	DIH	●	●	●	●	●	●		●	●	●	●	●	●	●
	DIDH	●	●	●	●	●	●		●	●		●	●	●	●
	DPI				●										
Responsabilidad del Estado	Atribución	●	●	●	●	●	●		●	●	●	●	●	●	●
	Contramedidas		●	●	●	●	●		●	●		●	●	●	●
	Necesidad		●		●					●		●			●

Figura 8: Resumen de posiciones nacionales y conjuntas por temas cubiertos.

Posiciones nacionales

	FR	DE	IR	IE	IL	IT	JP	KZ	KE	NL	NZ	NO	PK	PL	RO	RU	SG	SE	CH	UK	US
	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
	●	●	●	●	●	●	●			●	●	●	●	●	●	●	●	●	●	●	●
	●	●	●	●	●	●	●			●	●	●	●	●	●	●	●	●	●	●	●
	●	●		●	●	●	●			●	●	●		●	●			●	●	●	●
	●						●		●		●	●	●			●	●		●	●	
			●			●										●					
	●	●		●	●	●	●		●	●	●	●	●	●	●		●	●	●	●	●
				●		●	●	●	●	●	●	●		●	●		●	●	●	●	●
	●	●		●	●	●	●			●	●	●		●	●	●		●	●	●	●
	●	●		●	●	●	●			●	●	●		●	●	●	●	●	●	●	●
	●	●					●			●		●						●	●		

CAPÍTULO 5:

PRESENTACIÓN

DE UN VISTAZO

Este capítulo explora cómo pueden presentar y difundir los Estados sus posiciones nacionales. Compara los formatos orales y escritos, habla sobre la extensión, estructura, lenguaje y uso de ejemplos, y describe opciones para su difusión. Cada elección afecta la claridad, alcance e impacto de la posición. El capítulo anima a los Estados a equilibrar la autoridad jurídica con la accesibilidad y a ajustar su enfoque de acuerdo con sus objetivos, públicos y los recursos disponibles.

1. INTRODUCCIÓN

Aunque las posiciones nacionales emitidas hasta ahora cubren una lista de temas bastante uniforme, como se habla en el **Capítulo 4**, estas han sido presentadas de diferentes maneras. Las primeras fueron presentadas como discursos gubernamentales, pero la tendencia ha cambiado gradualmente hacia documentos escritos autónomos. Igualmente, las posiciones nacionales varían significativamente en extensión, desde documentos concisos de solo un par de páginas, hasta más detallados con más de 20 páginas. Algunos son muy generales, mientras que otros profundizan más en preguntas difíciles del derecho internacional y/o desafíos específicos que surgen en el ciberespacio, incluyendo escenarios o ejemplos de operaciones cibernéticas maliciosas. La estructura de las posiciones también varía, algunas utilizan títulos claros, párrafos numerados y/o resúmenes. La mayoría de las posiciones nacionales han sido publicadas en inglés, mientras que otras están publicadas o traducidas en otros idiomas. Las posiciones nacionales han sido difundidas a varios públicos usando diferentes estrategias, incluidas comunicados de prensa, publicaciones en revistas o blogs académicos, anuncios en redes sociales y eventos para debatir su contenido.

La presentación de una posición nacional no es solo el reflejo de las idiosincrasias nacionales o regionales, también determina en gran medida cuál será su impacto. La finalidad de este capítulo es desglosar las diferentes tendencias en cuanto a formato, estilo, idioma y difusión de las posiciones nacionales. Este capítulo también toma en cuenta por qué estas elecciones importan y sus implicaciones para el estatus, contenido e impacto de las posiciones nacionales.

Como se discutió en la **introducción** de este manual, consideramos que una posición nacional es una declaración pública, publicada por escrito, que describe las perspectivas del Estado sobre uno o más interrogantes sustantivos de la aplicación del derecho internacional en el contexto cibernético.

Esto no quiere decir que los Estados no hayan expresado sus opiniones sobre diversos aspectos de la aplicación del derecho internacional en el contexto cibernético en otros formatos. Por ejemplo, muchos Estados han hecho comentarios verbales y/o presentado declaraciones escritas al Grupo de Trabajo de Composición Abierta (GTCA) sobre interrogantes del derecho internacional que creen que deberían incluirse en sus informes anuales.[1] Entre ellos hay varios países del Sur Global que todavía no han publicado una posición nacional, como Chile,[2] Sudáfrica[3] y ciertos Estados miembros del Foro de las Islas del Pacífico.[4] Estas declaraciones pueden, de hecho, servir como estructura o punto de partida para una posición nacional completa. Sin embargo, como hasta ahora no han articulado las perspectivas sustantivas del Estado sobre cómo las diferentes reglas y principios del derecho internacional aplican a las actividades cibernéticas, están por fuera del alcance de este manual; como se discute a continuación, solo tres Estados han usado sus declaraciones ante el GTCA para presentar sus posiciones nacionales.

Algunas elecciones políticas dan forma al formato, estilo, lenguaje y estrategias de difusión de las posiciones nacionales.

Esto incluye, sobre todo, la elección del estatus jurídico de la posición nacional; es decir, si constituye evidencia de la práctica y/o opinio juris del Estado, es una ayuda para la interpretación, o es una simple declaración política. Segundo, como se discute en el **Capítulo 3**, es importante considerar si la posición seguirá un enfoque deductivo del derecho internacional (al plantear las normas relevantes en abstracto y luego explicar cómo se aplican en el contexto cibernético) o el enfoque inductivo (empezando desde ciertos desafíos fácticos del contexto cibernético y luego desglosando las normas que le aplican). Tercero, las funciones, fines y/o motivaciones de la posición nacional también informan las elecciones de formato, estilo, idioma y difusión. Como se vio en el **Capítulo 2**, las funciones generales de una posición nacional pueden incluir la comunicación o interacción con diferentes partes interesadas para transformar o adaptar el derecho internacional en su aplicación a las actividades cibernéticas y para prevenir el comportamiento ilegal. Esto se puede traducir en objetivos y motivaciones específicos, que incluyen prevenir los errores de cálculo y las escaladas aumentando la previsibilidad y estabilidad a escala, mejorando el cumplimiento y la rendición de cuentas, y orientando la evolución del derecho internacional al abordar la inseguridad jurídica.

1 Consulte, por ejemplo, Austria, *Preproyecto del informe del GTCA – TIC: Comentarios de Austria* (31 de marzo de 2020).

2 Ministerio de Relaciones Exteriores de Chile, *Derecho Internacional,* ONU, Nueva York, GTCA, Sexta sesión sustantiva (11 a 15 de diciembre de 2023).

3 Consulte, Sudáfrica, *Declaración de Sudáfrica en la novena sesión del Grupo de Trabajo de Composición Abierta sobre seguridad y uso de las TIC (2021 – 2025) – Derecho internacional,* ONU, Nueva York (4 de diciembre de 2024).

4 Foro de las Islas del Pacífico, *Declaración del Presidente del PIF en nombre del Foro de las Islas del Pacífico,* ONU (Nueva York, 4 de diciembre de 2024).

2. Formato y estilo

Para los fines de este capítulo, el formato y estilo de una posición nacional hacen referencia a su forma (oral o escrita), su extensión (larga o concisa) y otros elementos estructurales como el uso de ejemplos, casos de estudio, resúmenes, encabezados, referencias, apartados numerados y ayudas visuales.

a. Forma oral vs. escrita

i. Discursos

El concepto de posición nacional surgió cuando Harold Hongju Koh, asesor jurídico del Departamento de Estado de los Estados Unidos, articuló las perspectivas del país sobre el derecho internacional en el ciberespacio en un discurso en la Conferencia Jurídica Interinstitucional del Comando Cibernético en 2012. El discurso fue publicado y se convirtió en un referente sobre cómo los Estados Unidos se posicionó con relación a la aplicación de diferentes reglas y principios del derecho internacional a las tecnologías de la información y la comunicación (TIC).[5] Fue presentado en el contexto de debates seminales sobre este tema que tuvieron lugar en los Grupos de Expertos Gubernamentales (GEG) de la ONU en 2009-2010 y 2011-2013[6] al igual que durante el proceso que condujo a la publicación de la primera edición del Manual de Tallin en 2013.[7] En dos discursos posteriores en 2016[8] y 2020,[9] los Estados Unidos cubrieron temas o áreas más específicos del derecho internacional que fueron debatidos en el GEG de 2014 a 2015, como soberanía, derecho internacional humanitario (DIH), no intervención y derecho Internacional de los derechos humanos (DIDH).[10]

5 Posición nacional de Estonia (2012).

6 Consulte Asamblea General de las Naciones Unidas, *Informe del Grupo de Expertos Gubernamentales sobre los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional*, A/65/201 (30 de julio de 2010), párr. 14 y 16; Asamblea General de las Naciones Unidas, *Desarrollos en el campo de la información y las telecomunicaciones en el contexto de la seguridad internacional. Informe de la Secretaría General, A/66/152*, A/66/152 (15 de julio de 2011), 6, 18 y 19; Asamblea General de las Naciones Unidas, *Informe del Grupo de</104194> expertos gubernamentales sobre los desarrollos en el campo de la información y las telecomunicaciones en el contexto de la seguridad internacional*, A/68/98 (24 de junio de 2013), párr. 11, 16 y 19. Consulte también Eneken Tikk-Ringas, *Desarrollos en el campo de la información y las telecomunicaciones en el contexto de la seguridad internacional. Trabajo del Primera Comisión de la ONU, 1998 a 2012*, ICT4Peace (2012), 9-10; Camino Kavanagh, *Naciones Unidas, Ciberespacio y paz y seguridad internacional. Responder a la complejidad del siglo XXI*, UNIDIR (2017), pág. 16 a 19.

7 Consulte CCDCOE, I; Wikipedia, 'Manual de Tallin'.

8 Posición nacional de Estonia (2016).

9 Posición nacional de Estonia (2020).

10 Asamblea General de las Naciones Unidas, *Informe del Grupo de Expertos Gubernamentales sobre los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional*, A/70/174 (22 de junio de 2013), párr. 28.

En 2016, Norbert Riedel, comisionado de la policía cibernética internacional del Ministerio Federal de Asuntos Exteriores de Alemania, pronunció un discurso sobre 'Ciberseguridad como una dimensión de la política de seguridad' en Chatham House.[11] Aunque no estaba centrado en el derecho internacional, el discurso abordó brevemente cómo, desde la perspectiva de Alemania, la soberanía, la prohibición del uso de la fuerza y el DIH deben entenderse en el contexto cibernético. El discurso no estaba enmarcado como posición nacional de Alemania, que luego fue publicada como un documento autónomo en 2021, pero ofreció una base para esta.[12]

En 2018, también en Chatham House, Jeremy Wright, el fiscal general del Reino Unido, pronunció la primera posición nacional del país en forma de un discurso titulado 'El ciberespacio y el derecho internacional en el siglo XXI'.[13] Este fue repetido para la primera posición nacional del Reino Unido en 2022.[14] En 2019, el presidente Kersti Kaljulaid develó la primera posición nacional de Estonia en la apertura de la conferencia principal de la OTAN sobre conflicto cibernético, 'CyCon'.[15] Israel le siguió en 2020 con el discurso pronunciado por su fiscal general adjunto, Roy Schöndorf, en la Escuela de Guerra Naval de Estados Unidos. El discurso fue publicado como un artículo académico[16] y en un blog.[17]

11 Ministerio Federal de Asuntos Exteriores de Alemania, 'Ciberseguridad como dimensión de la política de seguridad' (Trad. libre) Discurso del embajador Norbert Riedel, Comisionado para Política Cibernética Internacional, Ministerio Federal de Asuntos Exteriores, Berlín, en Chatham House, Londres (18 de mayo de 2015) (Trad. libre).

12 Posición nacional de Alemania (2021).

13 Posición nacional de Estonia (2018) (Trad. libre).

14 Posición nacional de Estonia (2022).

15 Posición nacional de Estonia (2019), pág. 23 a 30.

16 Roy Schöndorf, 'La perspectiva de Israel sobre las cuestiones jurídicas y prácticas relacionados con la aplicación del derecho internacional a las operaciones cibernéticas' (2021) *Estudios de Derecho Internacional*, 97, pág. 395 a 406.

17 Roy Schöndorf, 'La perspectiva de Israel sobre las cuestiones jurídicas y prácticas relacionados con la aplicación del derecho internacional a las operaciones cibernéticas', EJIL. *Talk!* (9 de diciembre de 2020).

Lanzar una posición nacional como un discurso oficial del gobierno puede ser una manera efectiva de llamar la atención de grandes públicos y publicitar más el documento. Por lo general, hay cierto grado de ceremonia que rodea el pronunciamiento de un discurso oficial, especialmente de un representante de Estado de alto perfil, como un presidente o fiscal general. Debido a que un discurso gubernamental puede reunir a varias partes interesadas, también puede ser una buena oportunidad para responder preguntas y recibir retroalimentación. Los discursos tienden a ser menos formales y más concisos, accesibles y recordables, y ofrecen mayor conexión con el público. De este modo, pueden mejorar el alcance e impacto de la posición nacional entre las diferentes partes interesadas. Por otro lado, su formato menos estructurado puede ser más difícil de seguir, especialmente para quienes no son abogados. Existe también el riesgo de crear una expectativa de que se pronunciarán discursos nuevos o de seguimiento sobre el derecho internacional en el ciberespacio. También, por su naturaleza, el formato oral limita el alcance y la profundidad de la posición nacional: en un solo discurso únicamente se puede tratar una cantidad limitada de temas o asuntos, y como máximo, a nivel muy general.

ii. Declaraciones en la ONU

Algunos Estados, Brasil,[18] República Checa,[19] y Finlandia[20] compartieron sus perspectivas sobre el derecho internacional y las actividades cibernéticas en declaraciones orales ante la segunda sesión sustantiva del GTCA en 2020. En el caso de Finlandia, aunque la declaración oral nunca se publicó, fue seguida de una presentación más larga que se convirtió en la posición nacional escrita y autónoma del país.[21] Los Estados tienen tiempo limitado para leer sus declaraciones durante las sesiones del GTCA (generalmente de 3 a 5 minutos). Por lo tanto, estas declaraciones cubren una gama menor de temas, son más concisas y tienen un estilo general. Sin embargo, el entorno de la ONU requiere un tono más formal que otros entornos institucionales, como en conferencias o universidades.

Al igual que los discursos, las **declaraciones en la ONU son una buena manera de llamar la atención de los Estados miembros de la ONU y de las partes interesadas asistentes o que siguen la sesión correspondiente del GTCA**. Sin embargo, si no se publican las transcripciones y se facilita su acceso, se arriesga que los públicos que no asisten o siguen la reunión correspondiente, incluidos otros Estados, no las conozcan o no tengan acceso fácil al contenido de las declaraciones. Por este motivo, este manual no tiene en cuenta las declaraciones sin publicar o inaccesibles como posiciones nacionales.

18 Posición nacional de Brasil (2020).

19 Posición nacional de República Checa (2020).

20 Consulte Marja Lehto, 'Perspectivas de Finlandia sobre el derecho internacional y el ciberespacio' (2023), *Nordic Journal of International Law* 92(3), 456–469, y Michael Schmitt, 'Finlandia define posiciones clave sobre el derecho internacional cibernético', *Just Security* (27 de octubre de 2020).

21 Posición nacional de Finlandia (2020).

iii. Documentos escritos autónomos

A medida que se debatían más áreas o temas del derecho internacional en el ciberespacio en diferentes foros, incluidos la ONU y el mundo académico, los Estados comenzaron a considerar la posibilidad de publicar posiciones nacionales en forma de documentos escritos independientes. El primero en hacerlo fue Australia en 2017, que publicó su posición nacional como anexo a su Estrategia de Interacción Cibernética Internacional.[22] Luego siguieron Francia[23] y los Países Bajos en 2019.[24] La posición nacional de Francia fue publicada por su Ministerio de Fuerzas Armadas, mientras que la de los Países Bajos fue una carta a su parlamento. En 2020, Irán, Finlandia y Nueva Zelanda publicaron sus posiciones nacionales autónomas.[25]

En este trasfondo de la publicación de cada vez más posiciones nacionales, el GEG invitó en 2019 a los Estados a enviar 'contribuciones nacionales voluntarias sobre el tema de cómo aplica el derecho internacional al uso de las tecnologías de la información y comunicación'.[26] La idea era que más Estados emitieran posiciones nacionales escritas que consolidaran sus perspectivas sobre cómo aplica el derecho internacional a las actividades cibernéticas en un solo documento. El objetivo era mejorar la transparencia, previsibilidad y entendimiento mutuo sobre el asunto. Quince Estados respondieron al llamado del GEG y sus posiciones nacionales se publicaron en un Compendio Oficial del GEG en 2021.[27] Fueron Australia, Brasil, Estonia, Alemania, Japón, Kazajistán, Kenia, Países Bajos (que presentaron una copia de su posición nacional de 2019), Noruega, Rumanía, Rusia, Singapur, Suiza, el Reino Unido y los Estados Unidos.

Luego de la publicación del Compendio Oficial del GEG, otros varios Estados publicaron su posición nacional como un documento autónomo. Italia lo hizo en 2021,[28] y el mismo año Francia publicó una versión en inglés de su posición de 2019.[29] También en 2021, China publicó dos documentos de posición; uno más general sobre 'La creación de reglas internacionales en el ciberespacio'[30] y otro sobre la 'Aplicación del principio de soberanía en el ciberespacio'.[31] Canadá, Polonia

22 Posición nacional de Australia (2017).

23 Posición nacional de Francia (2019).

24 Posición nacional de Países Bajos (2019).

25 Posiciones nacionales de Irán (2020), Finlandia (2020) y Nueva Zelanda (2020).

26 Asamblea General de las Naciones Unidas, *Resolución adoptada por la Asamblea General el 22 de diciembre de 2018 [sobre el informe del Primera Comisión (A/73/505)] 73/266 (Trad. libre). Avanzar el comportamiento responsable de los Estados en el ciberespacio en el contexto de la seguridad internacional,* A/RES/73/266 (2 de enero de 2019), párr. 3.

27 Asamblea General de las Naciones Unidas, *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,* A /76/136* (13 de julio de 2021).

28 Posición nacional de Italia (2021).

29 Posición nacional de Francia (versión en inglés) (2021).

30 Posición nacional de China (general) (2021) (Trad. libre).

31 Posición nacional de China (soberanía) (2021) (Trad. libre).

y Suecia publicaron sus posiciones nacionales en 2022;[32] Costa Rica, Dinamarca, Irlanda y Pakistán en 2023;[33] Austria, Cuba y República Checa en 2024;[34] y Colombia en 2025.[35] La UA y la UE publicaron posiciones conjuntas en 2024.[36]

Los documentos escritos autónomos se han convertido en el formato más popular para publicar posiciones nacionales. Estos permiten lograr una mayor cobertura y detalle, lo que las hace ideales para los Estados que quieren emitir posiciones más exhaustivas e influyentes. El proceso de publicar una posición escrita autónoma también tiende a ser más formal que pronunciar discursos o declaraciones o publicar artículos académicos. También existe la expectativa de que las posiciones escritas autónomas se conviertan en el referente de las perspectivas del Estado sobre el derecho internacional en el ciberespacio, lo que significa que, por lo general, hay más en juego con este formato. Todo esto significa que la redacción de una posición escrita autónoma puede tomar más tiempo e involucrar a más partes interesadas del gobierno que redactar un discurso, declaración o artículo académico. Por un lado, esto permite crear una posición nacional más refinada y representativa. Por otro, puede producir documentos más complejos, lo que podría reducir su accesibilidad para los públicos no especializados.

iv. Artículos académicos

Como se indicó anteriormente, la posición nacional de 2016 de los Estados Unidos fue originalmente pronunciada en un discurso y emitida el año siguiente como un artículo académico en el *Berkeley Journal of International Law*.[37] Israel hizo lo mismo, publicando el discurso pronunciado por su fiscal general adjunto como artículo académico en *International Law Studies* en 2021.[38] En 2023, el *Nordic Journal of International Law* publicó una edición especial que contenía las posiciones nacionales anteriormente publicadas de Finlandia, Noruega y Suecia, mientras develaba la posición nacional de Dinamarca, todas con introducciones escritas por los asesores jurídicos responsables.[39]

32 Posiciones nacionales de Canadá (2022), Polonia (2022) y Suecia (2022).

33 Posiciones nacionales de Costa Rica (2023), Dinamarca (2023), Irlanda (2023) y Pakistán (2023).

34 Posiciones nacionales de Austria (2024), Cuba (2024) y República Checa(2024).

35 Posición nacional de Colombia (2025).

36 Posiciones conjuntas de la UA (2024) y la UE (2024).

37 Brian J. Egan, *'Derecho internacional y estabilidad en el ciberespacio'* (2017) 35 Berkeley Journal of International Law 35, 169 a 180.

38 Roy Schöndorf, 'La perspectiva de Israel sobre las cuestiones jurídicas y prácticas relacionados con la aplicación del derecho internacional a las operaciones cibernéticas' (2021) Estudios de Derecho Internacional, 97, pág. 395 a 406.

39 Jeppe Mejer Kjelgaard y Ulf Melgaard, 'Posición de Dinamarca sobre la aplicación del derecho internacional en el ciberespacio' (2023) *Nordic Journal of International Law*, 92(3), 446 a 455; Marja Lehto, 'Perspectivas de Finlandia sobre el derecho internacional y el ciberespacio' (2023), *Nordic Journal of International Law* 92(3), 456 a 469; Vibeke Musæus, 'Documento de posición de Noruega sobre el derecho internacional y el ciberespacio' (2023) Nordic Journal of International Law 92(3), 470 a 488; Ola Engdahl, 'Documento de posición de Suecia sobre la aplicación del derecho internacional en el ciberespacio' (2023) Nordic Journal of International Law 92(3), 489 a 497.

Publicar las posiciones nacionales como artículos académicos puede aportar rigor y autoridad jurídica a la publicación, dados los altos estándares de las revisiones de pares y/o editoriales a las que por lo general se someten los artículos académicos. Los artículos académicos también pueden ser una manera eficaz de comunicarse e influenciar a audiencias de especialistas jurídicos, especialmente académicos. Por otro lado, puede que no sean tan accesibles para las personas no especializadas. Esto se debe al lenguaje complejo que normalmente se emplea en los artículos académicos, así como al hecho de que no muchas personas no especialistas tienen conocimiento de las publicaciones académicas.

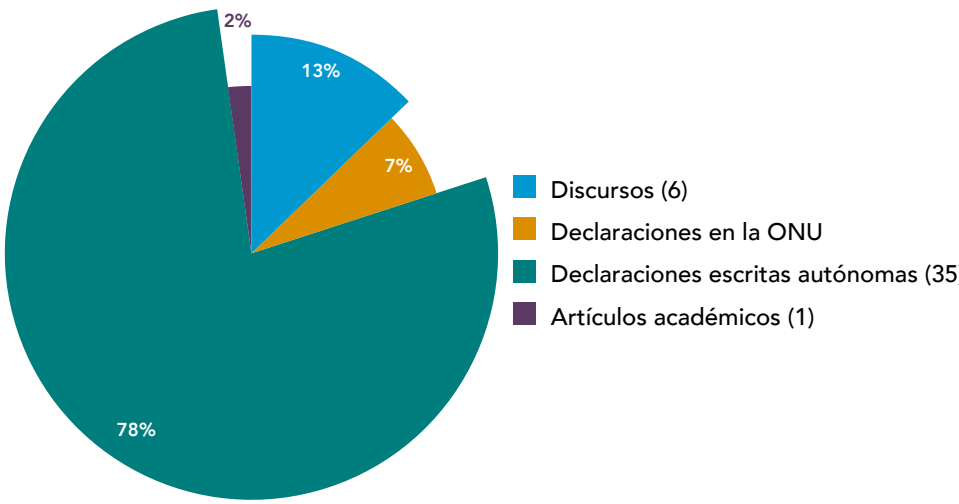
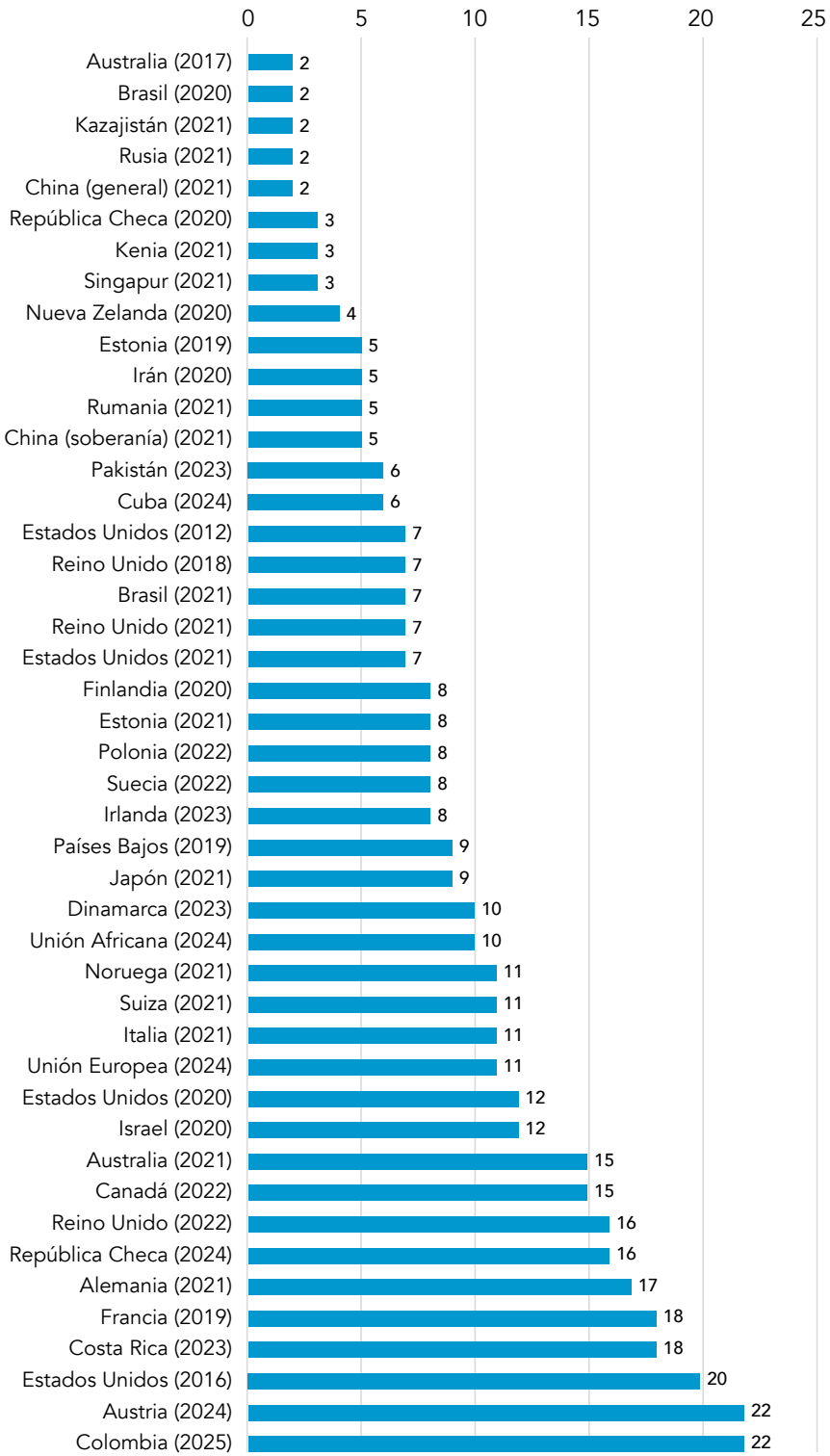


Figura 9: Relación de las posiciones nacionales y conjuntas orales vs. escritas.

b. Extensión

La extensión de las posiciones nacionales publicadas hasta la fecha varía significativamente: las más cortas tienen dos páginas (como las de Australia [2017], Kenia, Kazajistán y Rusia), mientras que las más largas tienen 22 páginas (Austria y Colombia). Sin embargo, como lo indica el cuadro de abajo, **existe una preferencia por documentos más detallados y extensos, con nueve páginas en promedio**, la mayoría de los cuales fueron publicados originalmente de forma escrita.

Figura 10: Posiciones nacionales y conjuntas por extensión (en páginas).



La preferencia por documentos más extensos se puede explicar por la amplitud y profundidad del análisis que permite el formato autónomo. Por ejemplo, las posiciones nacionales de Austria y Costa Rica (22 y 18 páginas, respectivamente) han sido bien recibidas por los académicos, algunos apreciando su sofisticación, detalle, alcance y matiz.[40] Como se trató en el **Capítulo 4**, en el ciberespacio puede ser relevante una diversidad de reglas, principios y regímenes, y cada uno presenta interrogantes complejos de interpretación e implementación jurídica. Por lo tanto, la amplitud y profundidad del análisis son particularmente importantes si la posición nacional pretende desarrollar o clarificar el derecho internacional existente en lo relacionado con su aplicación al contexto cibernético o influenciar el cuerpo académico. La amplitud y profundidad también conducen a mayor transparencia y rendición de cuentas. Pero, al mismo tiempo, demasiado detalle y exceso de formalismo o terminología jurídica pueden afectar la claridad y accesibilidad de la posición nacional, particularmente para públicos sin conocimientos jurídicos.

Esto no quiere decir que las posiciones nacionales breves sean menos valiosas. Estas pueden ser útiles cuando el Estado pretende centrarse en algunas áreas o temas clave de la aplicación del derecho internacional al contexto cibernético.[41] La posiciones nacionales concisas también son adecuadas si el objetivo es simplemente reconocer la aplicación general del derecho internacional y/o ciertas reglas, principios o regímenes en el ciberespacio, sin profundizar en los detalles o complejidades de cómo se aplican en ese contexto.[42] Del mismo modo, si la finalidad de la posición nacional es destacar áreas de incertidumbre o vacíos, será más adecuado un documento más conciso. Las declaraciones de política sobre asuntos como el panorama de las ciber amenazas, la creación de capacidades o de fomento de la confianza, tampoco necesitan el mismo nivel de detalle como los análisis jurídicos, y se pueden realizar de modo más conciso e informal.[43] Por lo tanto, las posiciones concisas pueden ser de utilidad para los debates diplomáticos de alto nivel sobre los temas de política más amplios que rodean las aplicaciones del derecho internacional en el contexto cibernético. Con relación a esto, los profesionales tienden a preferir documentos más cortos, dado el poco tiempo que tienen para estudiar posiciones nacionales en su totalidad. Por ejemplo, durante las mesas redondas del proyecto, el formato conciso de la posición nacional de Nueva Zelanda (cuatro páginas) fue elogiada por un representante estatal debido a su 'elegancia' y como modelo a seguir.[44] El modelo conciso también es adecuado si el objetivo de la posición nacional es informar a un público más amplio de personas no expertas en derecho internacional, incluidos los responsables de políticas públicas, la industria y la sociedad civil.

40 Consulte Chris Carpenter y Duncan B. Hollis, 'La perspectiva de una víctima sobre el derecho internacional en el ciberespacio', *Lawfare* (28 de agosto de 2023); Przemysław Roguski, 'La posición progresiva de Austria sobre las operaciones cibernéticas y el derecho internacional,' *Just Security* (25 de junio de 2024).

41 Consulte, por ejemplo, la posición nacional de Estonia (2019).

42 Consulte, por ejemplo, las posiciones nacionales de Brasil (2020), China (2021) (general) y Kenia (2021).

43 Consulte, por ejemplo, las posiciones nacionales de China (2021) (general) y Rusia (2021).

44 Comentario hecho en la mesa redonda sobre las perspectivas de Latinoamérica y el Caribe (informe en el archivo con autores).

c. Escenarios y ejemplos

Varias posiciones nacionales incluyen ejemplos de operaciones cibernéticas maliciosas para ilustrar las posibles violaciones o destacar la importancia del derecho internacional en el contexto cibernético. Ha habido ejemplos que van desde tipos generales de operaciones cibernéticas maliciosas (como espionaje cibernético, interferencia electoral y ransomware)[45] hasta incidentes del mundo real (por ejemplo, el ataque cibernético NotPetya).[46] Dos posiciones nacionales van un paso más allá e incluyen escenarios hipotéticos más detallados sobre operaciones cibernéticas que posiblemente violen el derecho internacional.[47] La inclusión de ejemplos o escenarios puede mejorar la claridad y la precisión. En particular, puede clarificar los resultados o implicaciones jurídicas de la adopción de determinada interpretación o promover una nueva regla del derecho internacional en el contexto cibernético. También pueden garantizar que las posiciones nacionales sean relevantes y prácticas en el contexto cibernético y no constituyan meras reafirmaciones abstractas del derecho internacional. En particular, los ejemplos de incidentes cibernéticos del mundo real pueden poner en contexto e ilustrar la motivación para la emisión de una posición nacional. Los ejemplos o escenarios son cruciales si el Estado decide seguir el enfoque inductivo en su posición, es decir, partir de ciertos datos y luego explicar cómo les aplica el derecho.

45 Consulte, por ejemplo, las posiciones nacionales de Costa Rica (2023), el Reino Unido (2022) y los Estados Unidos (2016).

46 Consulte, por ejemplo, las posiciones nacionales del Reino Unido (2018 y 2022).

47 Consulte, por ejemplo, las posiciones nacionales de Australia (2021) y Austria (2024).

d. Referencias

La mayoría de las posiciones nacionales publicadas hasta la fecha incluyen referencias a decisiones relevantes de cortes y tribunales internacionales y tratados internacionales, documentos de la ONU (particularmente el trabajo de la Comisión de Derecho Internacional) y fuentes académicas (más notoriamente los Manuales de Tallin). Estas referencias toman forma de notas al pie de página,[48] citas[49] y/o bibliografía.[50] **Las referencias pueden dar mayor autoridad jurídica a la posición nacional, haciéndola más persuasiva para los diferentes públicos, incluidos otros Estados y la academia**. Sin embargo, usar demasiadas referencias puede hacer que la posición sea visualmente abarrotada y difícil de leer, especialmente si las referencias están al pie de página. Por lo tanto, referenciar con eficacia requiere lograr un equilibrio entre la autoridad jurídica y la accesibilidad. Los hipervínculos a los materiales citados en las notas al pie de página también pueden mejorar la accesibilidad, facilitando que los lectores encuentren los documentos correspondientes. Para que las posiciones nacionales sean más concisas e informales, como las emitidas como declaraciones en la ONU o discursos que luego se publican como artículos en blogs, una opción es incluir hipervínculos a las obras referenciadas en el cuerpo del texto, en vez de escribirlas completamente en las notas al pie de página.

e. Encabezados, resúmenes y apartados numerados

La gran mayoría de las posiciones nacionales publicadas emplean encabezados. Estos pueden ayudar a estructurar la posición alrededor de áreas, temas o preguntas claves del derecho internacional en el contexto cibernético, a menudo de lo más general a lo más específico. **Esto puede mejorar significativamente la claridad y legibilidad de la posición nacional**.

Los resúmenes también son importantes para la claridad y accesibilidad, especialmente en los documentos más extensos, ya que pueden destacar los mensajes clave que comunica la posición nacional. Los resúmenes son particularmente útiles para los profesionales, como los abogados y diplomáticos del gobierno, que tienen poco tiempo para leer las posiciones por completo. No obstante, solo seis posiciones nacionales publicadas hasta la fecha tienen resúmenes (Australia [2017], Austria, Estonia [2021], Francia, Noruega y Polonia). En las posiciones nacionales de Austria, Estonia (2021), Francia y Noruega, los resúmenes están contenidos en recuadros de texto, lo que mejora más la legibilidad. En las posiciones nacionales de Australia (2017) y Polonia, los resúmenes aparecen en forma de encabezados con frases cortas que capturan los puntos principales de las secciones relevantes. Esto ayuda al lector a identificar rápidamente los asuntos que cubre la posición y cuáles son las conclusiones principales de estos.

48 Consulte, por ejemplo, las posiciones nacionales de Austria (2024), Costa Rica (2023), Cuba (2024), República Checa (2024) e Irlanda (2023).

49 Consulte, por ejemplo, las posiciones nacionales de Canadá (2022) y Colombia (2025).

50 Consulte, por ejemplo, la posición nacional de Colombia (2025).

Los apartados numerados también ayudan a referenciar los puntos específicos que se plantean en el documento, permitiendo a otros citar la posición fácilmente. Si el objetivo de la posición es influenciar a las audiencias, particularmente a otros Estados o a la academia, esto se debe considerar. Sin embargo, solo unas pocas posiciones nacionales y una conjunta publicadas hasta la fecha contienen apartados numerados.[51]

f. Ayudas visuales

Algunas posiciones nacionales han sido publicadas en documentos con diseño especial, como las de Australia (2017 y 2021), Colombia, Francia (2019) y Nueva Zelanda. Sin embargo, ninguna cuenta con apoyos visuales, como tablas, cuadros o infografías. Estos recursos han sido utilizados exitosamente en otros documentos de políticas cibernéticas, como la Estrategia de Interacción Cibernética Internacional de Australia (que, como se indicó, contiene su posición nacional del 2017 como anexo),[52] y explicaciones [53] sobre las 11 normas del GEG de comportamiento responsable de los Estados.[54] **Las ayudas visuales se pueden incorporar para aumentar la accesibilidad de las posiciones nacionales**, ya sea en el mismo documento o en estrategias de difusión separadas, como se discute a continuación.

51 Posiciones nacionales de Canadá (2022), Costa Rica (2023), Cuba (2024), República Checa (2024), Irlanda (2023), Nueva Zelanda (2020), Pakistán (2023), y del Reino Unido (2021), y también la posición conjunta de la UA (2024).

52 Commonwealth de Australia, Departamento de Asuntos Exteriores y Comercio Exterior, *La estrategia de Interacción Cibernética Internacional de Australia'* (octubre de 2017), 8 a 9, y 16 y 85.

53 Consulte, por ejemplo, Instituto Australiano de Política Estratégica. Centro de Política Cibernética Internacional, *Las normas de las Naciones Unidas sobre el comportamiento responsable de los Estados, Orientación sobre la implementación para los Estados miembro de ASEAN* (Marzo de 2022).

54 Asamblea General de las Naciones Unidas, *Informe del Grupo de Expertos Gubernamentales sobre los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional,* A/70/174 (22 de julio de 2021), párr. 13(c).

3. Lenguaje

Para los fines de este capítulo, 'lenguaje' se refiere al uso de terminología jurídica y la lengua o lenguas de publicación.

a. Terminología jurídica

Todas las posiciones nacionales emitidas hasta la fecha han empleado la terminología tradicional del derecho internacional en su análisis de las reglas, principios y regímenes internacionales con relación a su aplicación en el contexto cibernético. Esto es fundamental si la finalidad de la posición es desarrollar o clarificar cómo aplica el derecho internacional en el contexto cibernético. **Pero los Estados deben ser precisos y coherentes al utilizar términos jurídicos**, como 'soberanía', 'jurisdicción', 'ataque' y 'coerción'. Estas y otras palabras, además de tener un significado especial en el derecho internacional, también están sujetas a debates significativos. Por lo tanto, en la posición nacional es importante clarificar lo que quiere decir el Estado al emplear dichos términos. Esto, además de proporcionar una definición jurídica, sitúa cada concepto dentro de los debates existentes, así como indica la perspectiva, si la hay, que el Estado promueve sobre el tema.

Por ejemplo, al hablar de soberanía en su aplicación a las actividades cibernéticas en la posición nacional, es útil especificar si el Estado se refiere al debate entre soberanía como principio y soberanía como norma,[55] o a los corolarios de la soberanía del Estado, como la jurisdicción y la no intervención.[56] De igual manera, si el objetivo de la posición nacional es adoptar una posición sobre estos debates, es importante que señale claramente cuál es esta. En cambio, si el Estado no desea adoptar una posición firme sobre determinado debate, ya sea porque no ha tomado una decisión o porque la evidencia no es concluyente, debería decirlo en términos claros.

Se han usado palabras clave para comunicar dichas intenciones. Por ejemplo, cuando una posición nacional afirma que el Estado 'debe' o 'está obligado' a hacer o abstenerse de algo, expresa la perspectiva de que el comportamiento correspondiente está basado en una obligación jurídica vinculante. Otra forma de expresar que cierta norma es vinculante a la luz del derecho internacional es decir que constituye *lex lata* (es decir, lo que el derecho es). Por el contrario, el uso de términos como 'debería' o 'podría' o 'pudiera' implica que el Estado no considera el comportamiento en cuestión como una obligación del derecho internacional.[57] De manera similar, el Estado puede decir que la afirmación es de *lex ferenda* (es decir, lo que el derecho debería ser) o constituye una 'norma no vinculante' si no considera que es vinculante conforme al derecho internacional. Del mismo modo,

55 Consulte, por ejemplo, las posiciones nacionales de Austria (2024), págs. 4 a 5 y del Reino Unido (2018), pág. 7.

56 Consulte, por ejemplo, la posición nacional de China (2021) (soberanía), pág. 2.

57 Consulte, por ejemplo, las posiciones nacionales de Canadá (2022), párr. 26, y Nueva Zelanda (2020), párr. 16.

si el Estado considera que el derecho internacional todavía no ha regulado cierto comportamiento, puede afirmar que no hay suficiente evidencia de la práctica de los Estados y/o de la *opinio juris* es necesaria,[58] y que se necesita 'más' práctica del Estado y/o *opinio juris*,[59] o que 'no está convencido' de que la regla en cuestión se haya 'cristalizado'.[60] Por otro lado, si el Estado considera que la evidencia existente de la práctica del Estado y/o de la *opinio juris* no es clara o es inconcluyente respecto a una afirmación definitiva sobre el derecho, puede afirmar que el asunto correspondiente requiere más estudio o 'reflexión'.[61]

La elección de palabras también puede evidenciar el estatus jurídico de la posición nacional, es decir, si la posición fue adoptada como practica del Estado y/o *opinio juris*, como ayuda interpretativa o como una declaración política.

También es posible que el estatus de la posición nacional varíe dependiendo de los temas o asuntos que trata. Por ejemplo, posiblemente Estonia expresaba su *opinio juris* para los fines desarrollar el derecho internacional consuetudinario sobre las contramedidas colectivas al afirmar que estaba 'avanzando una posición' sobre el asunto,[62] En contraste, Noruega aclaró en el principio de su posición nacional que estaba dando su 'interpretación de ciertas obligaciones del derecho internacional en su aplicación a las operaciones cibernéticas'.[63] Cuando un Estado usa lenguaje exhortativo, como el afirmar que los Estados 'deberían' comportarse de cierto modo, posiblemente solo esté haciendo una declaración política. Las declaraciones de este tipo se incluyen, por ejemplo, en las posiciones nacionales de Canadá, China y Nueva Zelanda.[64]

Como se indicó en el **Capítulo 2**, las posiciones nacionales también han usado **terminología distinta para promover diferentes políticas jurídicas sobre el ciberespacio**, incluyendo para confirmar que el derecho internacional existente es suficiente para regular las actividades cibernéticas o para argumentar que se necesita un nuevo instrumento jurídicamente vinculante para estas.[65] Por ejemplo, la posición nacional de Austria afirma que el 'derecho internacional aplica en su totalidad a las actividades cibernéticas' y que Austria 'no ve necesidad de desarrollar

58 Consulte, por ejemplo, las posiciones nacionales de Israel (2021), pág. 404 y del Reino Unido (2021), párr. 12.

59 Consulte, por ejemplo, la posición nacional de Canadá (2022), párr. 25.

60 Consulte, por ejemplo, posición nacional Nueva Zelanda (2020), párr. 17.

61 Consulte, por ejemplo, la posición nacional de Brasil (2021), pág. 23.

62 Posición nacional de Estonia (2019).

63 Posición nacional de Noruega (2021), pág. 2 (Trad. libre).

64 Consulte las posiciones nacionales de Canadá (2022), párr. 26 ("ningún Estado debe permitir intencionalmente que su territorio se use para actos contrarios a los derechos de otros Estados); China (2021) (general), (por ejemplo, 'iii. Los Estados deben mejorar la protección de la infraestructura de TIC crítica'); y Nueva Zelanda (2020), párr. 16 ("los Estados no deben permitir intencionalmente que su territorio sea utilizado para hechos internacionalmente ilícitos usando las TIC').

65 Consulte, por ejemplo, las posiciones nacionales de China (2021) (soberanía), pág. 1, Cuba (2024), párr. 4 y 5, Pakistán (2023), párr. 8, y Rusia (2021), pág. 80.

un nuevo instrumento jurídicamente vinculante' relacionado con las actividades cibernéticas.[66] De igual manera, la posición conjunta de la UE argumenta que el derecho internacional 'aplica por completo al ciberespacio' y que resulta 'adecuado para su propósito en la era digital'.[67] Por el contrario, la posición nacional de China indica que la 'comunidad internacional debería desarrollar normas, reglas y principios de aceptación universal en el marco de la ONU, para abordar conjuntamente los riesgos y desafíos, y mantener la paz, seguridad y prosperidad en el ciberespacio'.[68] En la misma línea, la posición nacional de Rusia 'promueve una idea más amplia del desarrollo y mejora progresiva del derecho internacional teniendo en cuenta las características específicas de las TIC' mediante la 'adopción de una convención universal vinculante sobre la seguridad de la información internacional a nivel de la ONU'.[69]

b. Idioma y traducción de la publicación

La gran mayoría de las posiciones nacionales y las dos posiciones conjuntas emitidas hasta la fecha han sido publicadas en inglés. El inglés es el idioma prevalente en los entornos jurídicos, diplomáticos y académicos relevantes, incluidos el GEG y el GTCA, al igual que en los procesos Tallin y Oxford. Para garantizar que las posiciones sean coherentes con la terminología existente del derecho internacional, entendidas claramente por la mayoría de las partes interesadas, y para mejorar el entendimiento común entre los Estados, es importante publicarlas en inglés. Por ejemplo, en inglés, el término 'norm' (norma) ahora se entiende como una expectativa de comportamiento o un estándar no vinculante, como las normas del GEG sobre el comportamiento responsable de los Estados en el ciberespacio. Sin embargo, el término equivalente en otros idiomas, como el francés (*norme*) o el italiano, el portugués y el español (*norma*), también puede referirse a una regla vinculante. Lo mismo puede pasar con los conceptos informáticos y de otros campos técnicos, que tienen una terminología generalizada en inglés. **Por lo tanto, usar el inglés en las posiciones nacionales puede garantizar la claridad y precisión, al igual que evita malentendidos, especialmente cuando se trata de términos jurídicos y vocabulario técnico**.

Unos cuantos Estados han optado por publicar su posición nacional en otros idiomas. Este ha sido el caso de Estados cuyo idioma oficial no es el inglés. Ejemplos de esto son las posiciones nacionales de Francia (publicada en francés en 2019 y traducida al inglés en 2021),[70] Finlandia (publicada en finlandés y en inglés en 2020),[71] Kazajistán (publicada solo en ruso en el Compendio Oficial del GEG en 2021), Suiza (publicada

66 Posición nacional de Austria (2024), pág. 3 (Trad. libre). Consulte, por ejemplo, la posición nacional de Costa Rica (2023), párr. 7.

67 Posición conjunta de la UA (2024), párr. 3 (Trad. libre).

68 Posición nacional de China (2021) (general), pág. 1 (Trad. libre).

69 Posición nacional de Rusia (2021), pág. 80 (Trad. libre).

70 Posición nacional de Francia (2021).

71 Consulte las versiones en finlandés e inglés de la posición nacional de Finlandia (2020).

en inglés y francés en el Compendio Oficial del GEG en 2021), Rusia (publicada en inglés y ruso en el Compendio Oficial del GEG en 2021), Cuba (publicada en español en 2024) y Colombia (publicada en inglés y español en 2025). Canadá publicó su posición nacional en 2022 en sus dos idiomas oficiales: inglés y francés.[72] La posición nacional del Reino Unido fue publicada en el Compendio Oficial del GEG en 2021 en todos los idiomas oficiales de la ONU: árabe, chino, inglés, francés, ruso y español.

Publicar la posición nacional en idiomas diferentes al inglés puede servir para una diversidad de propósitos. Primero, puede aumentar la accesibilidad de una posición para los públicos que no hablan inglés a nivel nacional y/o internacional. Aunque el inglés es el idioma más hablado del mundo, la mayoría de la población que vive en el Sur Global no lo habla: al momento de esta publicación, cerca del 13% de la población mundial habla inglés y solo el 5 % son hablantes nativos.[73] El chino mandarín, hindú, español, francés y árabe le siguen al inglés como los más hablados.[74] Por lo tanto, una estrategia de publicación multilingüe centrada en uno o más de estos idiomas puede mejorar la inclusividad, cerrar brechas de conocimiento y reducir las brechas digitales. En segundo lugar, como lo destacaron varios representantes de los Estados durante las mesas redondas del proyecto, publicar una posición nacional en uno o más idiomas diferentes del inglés puede garantizar que las partes interesadas nacionales, incluidos el gobierno y la sociedad civil, además de comprender la posición nacional, también se sientan apropiados del proceso y su resultado.[75] De manera similar, si la posición nacional se desarrolla a nivel nacional o regional en un idioma distinto del inglés, publicarla en ese idioma puede asegurar la coherencia con la terminología jurídica y su significado. Igualmente, cada idioma, región y/o país tiene sus propias tradiciones y expresiones jurídicas y culturales. Por lo tanto, publicar la posición nacional en el idioma local puede capturar dichas tradiciones y expresiones para garantizar que sea relevante y sensible al contexto local. Finalmente, emitir una posición nacional en varios idiomas, como hizo el Reino Unido en 2021, puede garantizar el control sobre las traducciones oficiales y lograr que haya uniformidad en el significado entre estas.

72 Posición nacional de Canadá (2022) (versiones en inglés y francés).

73 Enciclopedia Britannica, 'Idiomas por cantidad total de hablantes'; Dylan Lyons, "¿Cuántas personas hablan inglés y dónde se habla?', *Babbel* (10 de marzo de 2021); Encore, "¿Cuál es el idioma más hablado del mundo?'.

74 Consulte Enciclopedia Britannica, 'Idiomas por cantidad total de hablantes'; Wikipedia, 'Lista de idiomas por cantidad total de hablantes'; Statista, 'Los idiomas más hablados a nivel global en 2023'.

75 Comentarios hechos en las mesas redondas sobre las perspectivas de Asia, Pacífico, Latinoamérica y el Caribe (informe en el archivo con autores).

Sin embargo, se deben tener en cuenta ciertas consideraciones al decidir si la posición se publica o se traduce a idiomas diferentes del inglés. Como se indicó anteriormente, algunos términos jurídicos y otros técnicos pueden tener un significado diferente, o simplemente no existir en otros idiomas. Por ejemplo, el concepto de 'soberanía como regla' no se puede traducir fácilmente al francés, lo que da lugar a ambigüedad.[76] Esto significa que al menos una versión de la posición nacional debe publicarse en inglés si su objetivo es desarrollar o clarificar la aplicación del derecho internacional en el contexto cibernético. Además, sin importar si la posición nacional se publica originalmente en inglés u otro idioma, **es importante garantizar que la traducción sea precisa y coherente**.

76 Consulte Aude Géry, 'Navegar las perspectivas de Francia sobre la soberanía en el ciberespacio: Por qué Francia no está en los campos de 'soberanía como norma' 'soberanía 'pura', *EJIL: Talk!* (19 de septiembre de 2024).

4. Difusión

Las posiciones nacionales son documentos oficiales de naturaleza jurídica y/o política. Como tales, han sido publicadas y difundidas mediante **canales gubernamentales y diplomáticos formales**. Como se indicó en el **Capítulo 3**, estos incluyen boletines oficiales y comunicados de prensa oficiales,[77] sitios web gubernamentales,[78] repositorios en línea nacionales e internacionales, como la Biblioteca Digital de la ONU (para las posiciones nacionales que se encuentran en el Compendio Oficial del GEG)[79] y la base de datos documental del GTCA[80] (donde se han publicado muchas posiciones nacionales autónomas). Difundir las posiciones nacionales a través de estos canales mejora su autoridad y asegura que los públicos jurídicos y diplomáticos que están familiarizados con estos los puedan encontrar con facilidad. **Es particularmente útil publicar las posiciones nacionales en la base de datos documental del GTCA**, ya que es una plataforma muy conocida para documentos oficiales relevantes para sus debates sobre las implicaciones de las TIC en la paz y seguridad. Esto puede garantizar que, además de los gobiernos, otras partes interesadas que también siguen el proceso del GTCA (como la industria, la sociedad civil y la academia) tengan acceso a las posiciones nacionales.

Como se indicó anteriormente, algunas posiciones nacionales han sido publicadas como **artículos académicos**. En el caso de Dinamarca, la posición nacional se publicó exclusivamente como un artículo académico. En otros casos, el artículo es una transcripción de un discurso oficial (por ejemplo, los de Israel y Estados Unidos en 2016) o una reedición de un documento de posición autónomo (por ejemplo, de Finlandia, Noruega y Suecia). Esta estrategia de difusión puede ser adecuada para los públicos académicos. Sin embargo, como se señaló, es posible que los artículos académicos no sean muy accesibles para otros públicos, ya sea por su formato o estilo, o por su alcance, ya que puede que las personas no especialistas no estén familiarizadas con las publicaciones académicas.

Publicar una posición nacional, o una de sus versiones en un blog también puede aumentar su alcance entre públicos no expertos. Por ejemplo, la posición de Israel se ofreció originalmente como un discurso que también fue publicado en el blog *EJIL: Talk!* [81] Esto aumentó la visibilidad de la posición entre los abogados internacionalistas y los especialistas que siguen ese blog.

77 Consulte, por ejemplo, Consejo de la UE, Ciberespacio: El Consejo aprueba la declaración de un entendimiento conjunto sobre la aplicación del derecho internacional al ciberespacio' (18 de noviembre de 2024).

78 Consulte, por ejemplo, las posiciones nacionales de Canadá (2022), Francia (2019), Países Bajos (2019), y del Reino Unido (2018, 2021 y 2022).

79 Biblioteca digital de la ONU.

80 GTCA, Grupo de Trabajo de Composición Abierta sobre las tecnologías de la información y comunicación, documentos.

81 Roy Schöndorf, 'La perspectiva de Israel sobre la cuestiones jurídicas y prácticas relacionados con la aplicación del derecho internacional a las operaciones cibernéticas', EJIL. Talk! (9 de diciembre de 2020).

Un comentario sobre la posición conjunta de la UA, de autoría de su principal redactor (Mohamed Helal, relator especial de la UA sobre derecho internacional en el ciberespacio), fue publicado en el mismo blog.[82] La publicación incluyó comentarios sobre los temas cubiertos por la posición conjunta, así como sobre el proceso que llevó a su adopción por la UA. Esto, no solo aumentó la visibilidad de la posición conjunta, sino también el interés en ella. Las publicaciones en blogs pueden ser particularmente útiles para explicar la posición nacional a audiencias no especializadas, en particular si están escritas de manera accesible sin terminología jurídica o técnica.

Ya sea publicada como un discurso, una declaración en la ONU o un artículo académico, **la gran mayoría de las posiciones nacionales emitidas hasta la fecha se puede acceder en línea**. Como se indicó anteriormente, esto incluye sitios web gubernamentales, versiones en línea de revistas académicas y la base de datos documental del GTCA.[83] Bases de datos no oficiales también han publicado en línea posiciones nacionales. El *Cyber Law Toolkit*[84] es uno de los más populares, donde las posiciones nacionales están ordenadas por país y tema en un formato accesible. El Portal de Política Cibernética del Instituto de las Naciones Unidas para la Investigación sobre el Desarme también presenta las posiciones por país, usando un mapa del mundo interactivo.[85]

Publicar la posiciones nacionales en línea es importante por diversas razones. La primera es que los diferentes públicos, del gobierno, la industria o la sociedad civil, están dispersos por todo el mundo, y muchos no pueden asistir a las reuniones o eventos donde se anuncian, se leen o se debaten las posiciones nacionales. En segundo lugar, los hábitos de consumo en línea son cada vez mayores en todas las demografías. En tercer lugar, publicar la posición nacional en línea es más eficiente, en términos de tiempo y costo, además de ser más respetuoso con el medio ambiente. En cuarto lugar, los formatos digitales facilitan las búsquedas por palabras clave y las traducciones automatizadas, lo que facilita a las audiencias tener acceso a las posiciones nacionales en diferentes idiomas. Para resumir, publicar una posición nacional en línea garantiza el acceso rápido y fácil de todas las partes interesadas relevantes, sin importar dónde se encuentren.

82 Mohamed Helal, 'La posición conjunta africana sobre la aplicación del derecho internacional en el ciberespacio: Reflexiones sobre el proceso jurídico colaborativo', *EJIL: Talk!* (5 de febrero de 2024).

83 GTCA, Grupo de Trabajo de Composición Abierta sobre las tecnologías de la información y comunicación, documentos.

84 Consulte https://cyberlaw.ccdcoe.org

85 Consulte UNIDIR, Portal de Política Cibernética.

Del mismo modo, usar **canales de redes sociales** para anunciar la publicación de una posición nacional y/o un comentario sobre esta puede ser una estrategia de difusión eficiente para públicos expertos y no expertos.[86] Muchos diplomáticos, abogados gubernamentales, representantes de la industria y académicos tienen un perfil de redes sociales y siguen los desarrollos en política cibernética o derecho internacional en el ciberespacio mediante sus redes sociales. De igual manera, muchos miembros del público son usuarios ávidos de redes sociales. Por lo tanto, es más probable que vean e interactúen con la publicación de una posición nacional si se anuncia en una publicación en redes sociales. Las publicaciones en redes sociales también se pueden usar para crear conciencia sobre la posición nacional publicada en inglés para públicos que no lo hablan y viceversa, especialmente si no hay posibilidad de hacer una traducción oficial de la posición misma a otros idiomas. Los videos explicativos publicados en redes sociales y otras plataformas en línea también pueden ayudar a dar a conocer las posiciones nacionales y aumentar su accesibilidad a diferentes audiencias, particularmente entre las personas no expertas.

Otra estrategia de difusión para aumentar la visibilidad e impacto de la posición nacional es organizar **eventos públicos y/o privados** para publicitar el documento y/o debatir su contenido con diferentes partes interesadas. Como se ha señalado anteriormente, esto podría hacerse cuando se expone una posición nacional en forma de discurso en conferencias o eventos especiales, como en el caso de las posiciones nacionales de Estonia (2019), Israel, el Reino Unido (2018 y 2022) y los Estados Unidos (2012, 2016 y 2020). Además, los eventos paralelos al margen del GTCA y su futuro mecanismo permanente en Nueva York pueden ser buenas oportunidades para anunciar y publicitar las posiciones nacionales. Por ejemplo, en marzo de 2024, tuvo lugar un evento paralelo en el GTCA para difundir la posición conjunta de la AU entre los públicos de la ONU y africanos, quienes pudieron participar en el evento en línea. También se pueden organizar diálogos y conferencias académicas a nivel nacional o regional para sensibilizar a los públicos locales sobre la publicación de una posición nacional. Por ejemplo, la posición nacional de Italia fue debatida en una conferencia en la Universidad de Boloña en noviembre de 2021.[87] Dichos eventos son particularmente útiles si ofrecen a las audiencias locales la oportunidad de debatir, en el idioma local, una posición nacional que solo se publicó en inglés.

86 Por ejemplo, Bert Theuermann, X Post (31 de mayo 2024); República de Polonia ("Rzecznik MSZ'), X Post (29 de diciembre de 2022); Política Exterior de Canadá, X Post (28 de abril 2022); Alemania en las Naciones Unidas, X Post (9 de mayo de 2021).

87 Consulte François Delerue, 'Conferencia sobre la aplicación del derecho internacional al ciberespacio' organizada en la Universidad de Boloña', EU Cyber Direct (12 de noviembre de 2021).

Finalmente, los Estados deberían considerar la inclusión de **ayudas visuales** como parte de su estrategia de comunicación general. Varios representantes de los Estados consultados en el contexto de este proyecto hicieron énfasis en que el contenido de la posición nacional también debe acompañarse de la debida atención a la presentación. Como se indicó anteriormente, las ayudas visuales pueden incluir diagramas, infografías, tablas y cuadros.

Figura 11: Ejemplos de estrategias de difusión de posiciones nacionales.

5. Conclusión

Como se ha discutido en todo este capítulo, cada opción de formato, estilo, idioma y difusión de la posición nacional tiene sus ventajas y desventajas. En última instancia, estas elecciones deben basarse en el estatus jurídico, enfoque y objetivos que los Estados definen para sus posiciones. Por ejemplo, si una posición nacional se publica como una evidencia de la opinio juris de un Estado, o de sus perspectivas interpretativas y tiene como fin influenciar el desarrollo o interpretación del derecho internacional, un documento bien estructurado y escrito con detalle, publicado en inglés, podría ser más adecuado. Por el contrario, si la finalidad de la posición nacional es hacer comentarios sobre política o crear conciencia de los asuntos generales del derecho internacional en el ciberespacio, entonces puede ser suficiente un documento o discurso más corto y menos estructurado publicado en inglés y/o en otro idioma. No obstante, cualquiera que sea el estatus, enfoque y finalidades de la posición nacional, su contenido debe ser comprendido claramente y recibir la importancia adecuada de las audiencias relevantes. Por lo tanto, los Estados deben lograr un equilibrio delicado entre autoridad y accesibilidad al considerar cómo presentar sus posiciones nacionales.

Para lograr este equilibrio, puede ser efectivo seguir las tendencias probadas y comprobadas de formato, estilo, idioma y estrategias de difusión discutidas en este capítulo. Esto también puede ayudar a los Estados y a otras partes interesadas a compilar, comparar y contrastar las posiciones nacionales con miras a encontrar áreas de consenso, desacuerdo y vacíos en el entendimiento de cómo aplica el derecho internacional en el contexto cibernético. Sin embargo, cada Estado tiene necesidades, aspiraciones y tradiciones culturales y jurídicas diferentes. Por lo tanto, como con la elección de los temas sustantivos a cubrir y el proceso a seguir, no existe una plantilla de presentación única para las posiciones nacionales. Por el contrario, hay una gama de opciones y elementos que se pueden combinar y mezclar para ajustarse a las diferentes intenciones. Es decisión de los Estados cuáles de estas opciones seguir o si establecer un nuevo conjunto de tendencias.

CAPÍTULO 6:

CONCLUSIÓN

Las posiciones nacionales han cambiado la manera en que se entiende el derecho internacional en el contexto cibernético. Como cada vez más Estados han publicado sus perspectivas sobre cómo se aplica el derecho internacional a las actividades cibernéticas, el campo se ha alejado de las zonas grises y se ha acercado a lograr una mayor claridad. Sin duda, permanecen incertidumbres y desacuerdos sobre *qué* reglas y principios internacionales aplican a las tecnologías de la información y la comunicación (TIC), *cómo* se aplican y si es necesario desarrollar nuevas reglas. La alineación completa en estos asuntos es virtualmente imposible, y puede que incluso no sea deseable: el derecho internacional es inmenso, muchos de sus interrogantes son complejos, y en el desarrollo, interpretación y aplicación del derecho hay involucrados una gran cantidad de Estados y otros actores con diferentes historias, culturas y agendas. Sin embargo, como se discutió en todo este manual, las posiciones nacionales y conjuntas han facilitado mucho el mapeo de las áreas de convergencia y divergencia, al igual que los posibles vacíos. Este mapeo es fundamental para fomentar el diálogo y crear confianza entre los Estados para impulsar el avance en el campo, incluso cuando no pueda ser posible lograr entendimientos comunes.

En este sentido, las posiciones nacionales se han convertido en una herramienta invaluable para los Estados y otras partes interesadas del campo, incluidos académicos, representantes de la industria y miembros de la sociedad civil. Al momento de esta publicación, 33 Estados han publicado una posición nacional y dos organizaciones regionales, la Unión Africana (UA) y la Unión Europea (UE) han publicado posiciones conjuntas (consulte el **Anexo B**). Una serie de otros Estados han expresado interés en desarrollar una posición nacional, mientras que algunos de los que ya las tienen pueden querer revisarlas o actualizarlas Para orientarlos en el proceso de desarrollar o revisar una posición nacional, este manual explora los interrogantes clave que pueden surgir en el camino.

Primero, como se indicó en la **introducción**, las posiciones nacionales pueden tener implicaciones jurídicas en el contexto cibernético y más allá. Específicamente, pueden calificar como evidencia de opinio juris y, más controversialmente, como práctica del Estado. Por esto, pueden contribuir al desarrollo del derecho internacional consuetudinario. Del mismo modo, las posiciones nacionales pueden constituir práctica subsiguiente en la aplicación de los tratados internacionales o medios complementarios para interpretarlos. También existe el debate sobre si el silencio de los Estados que aún no publican una posición nacional puede constituir aquiescencia con las reglas consuetudinarias o interpretaciones de tratados propuestas por otros Estados en sus posiciones. Conforme con el derecho internacional, el silencio de los Estados solo puede equivaler a la aquiescencia de una regla consuetudinaria o interpretación de tratado si se cumplen ciertas condiciones estrictas.

Estas incluyen la existencia de una circunstancia suficientemente específica que justifique una reacción, conocimiento adecuado y el transcurso de una cantidad de tiempo razonable.[1]

En muchos aspectos, el impacto jurídico de las posiciones nacionales no se ha limitado a las actividades cibernéticas y se ha extendido al derecho internacional en su conjunto. La tendencia de publicar las posiciones nacionales surgió de la dificultad de aplicar el derecho antiguo a una nueva y generalizada tecnología: las operaciones cibernéticas maliciosas se han llevado a cabo con una velocidad sin precedentes y han tenido un impacto generalizado, superando fronteras nacionales, desafiando los conceptos tradicionales del derecho internacional, como la soberanía, la no intervención y las nociones de 'ataque' y 'objeto' en el derecho internacional humanitario (DIH). Al explorar cómo las normas internacionales y los principios de aplicabilidad general deberían entenderse en el contexto cibernético, las posiciones nacionales han revivido debates fundamentales que son relevantes en otros contextos. Algunos ejemplos son si la soberanía y la diligencia debida dan lugar a obligaciones de los Estados y si terceros Estados pueden recurrir a contramedidas colectivas.

En el **Capítulo 2** se desglosan las diversas motivaciones para desarrollar una posición nacional (u optar por no hacerlo). Se identificaron tres funciones generales: para comunicar a las diferentes partes interesadas las perspectivas del Estado sobre la aplicación del derecho internacional a las actividades cibernéticas (función comunicativa); para transformar o adaptar normas del derecho internacional en su aplicación a este contexto, incluido el desarrollo del derecho internacional consuetudinario o proponer nuevas interpretaciones de los tratados (función transformadora); y para disuadir, prevenir y/o mitigar las consecuencias negativas de las operaciones cibernéticas maliciosas llevadas a cabo por actores estatales y no estatales (función preventiva).

Estas funciones se pueden cumplir mediante fines específicos y articular como diferentes motivaciones. En particular, las posiciones nacionales pueden prevenir los errores de cálculo y las escaladas al aumentar la previsibilidad y estabilidad de las relaciones internacionales. Asimismo, pueden mejorar el cumplimiento y la rendición de cuentas al disuadir y prevenir las operaciones cibernéticas ilícitas. Las posiciones nacionales también pueden orientar la evolución del derecho internacional en su aplicación a las actividades cibernéticas y abordar la inseguridad jurídica. Adicionalmente, el impacto positivo de las posiciones nacionales puede sentirse a nivel nacional. En particular, pueden contribuir a clarificar lo que significa el comportamiento responsable de los Estados para las partes interesadas nacionales, fomentar la resiliencia cibernética nacional, mejorar la coordinación interinstitucional e impulsar importantes desarrollos jurídicos y de política.

1 CDI, *Proyecto de conclusiones sobre la identificación del derecho internacional consuetudinario con comentarios*, A/73/10 (2018), 120, conclusión 10(3); CDI, *Proyecto de conclusiones sobre los acuerdos ulteriores y la práctica ulterior con relación con la interpretación de los tratados*,(2018), 15, conclusión 10(2).

Sin embargo, varios factores pueden dificultar que los Estados logren estos fines. Entre estos, es muy importante la falta de capacidad. La gran mayoría de las posiciones nacionales publicadas hasta la fecha han sido emitidas por países desarrollados. Y el desarrollo de la posición conjunta de la UA fue posible gracias a los esfuerzos de creación de capacidades y al fuerte liderazgo de la organización.[2] El desarrollo de una posición nacional es un proceso que necesita muchos recursos e inversiones significativas para cerrar la brecha entre los países desarrollados y en desarrollo. Al mismo tiempo, algunos Estados carecen de la voluntad política necesaria para embarcarse en el proceso de desarrollar una posición nacional. Otros Estados pueden temer que al emitir una posición nacional, limitarán su libertad de acción o generarán incluso más desacuerdos sobre cómo se aplica el derecho internacional a las actividades cibernéticas. Por lo tanto, es importante continuar debatiendo las diversas funciones y finalidades de las posiciones nacionales, destacando que pueden fomentar la transparencia y construir confianza entre los Estados, incluso cuando no se puedan lograr entendimientos comunes sobre los contenidos.

El **Capítulo 3** trató con detalle los varios pasos que pueden estar involucrados en el desarrollo de una posición nacional. Como punto de partida, los Estados deben considerar la identificación de las partes interesadas internas y externas que quieren involucrar en el proceso, teniendo en cuenta que es altamente recomendable tener una combinación de experticia jurídica, política y técnica. También puede ser útil designar a un organismo particular como el redactor, con la tarea de coordinar el proceso y redactar la posición. Puede ser necesario seguir una serie de pasos organizacionales. Estos incluyen asignar roles a diferentes partes interesadas y evaluar interrogantes como el alcance y finalidades de la posición, la ubicación de las reuniones pertinentes y otras tareas, el cronograma y los diversos métodos para llevar a cabo cada tarea. Algunos Estados también pueden acoger con satisfacción la creación de capacidades en diferentes temas, como el derecho internacional, la política cibernética y la ciberseguridad, antes de poder elaborar una posición nacional.

Cuando se trata de redactar una posición nacional, los Estados pueden seguir diferentes estrategias. Por ejemplo, pueden empezar a partir de un texto exhaustivo y refinarlo en los debates siguientes. Por el contrario, un texto o esquema más simple se puede desarrollar para convertirlo en un documento de posición completo.

2 Mohamed Helal, 'La posición conjunta africana sobre la aplicación del derecho internacional en el ciberespacio: Reflexiones sobre el proceso jurídico colaborativo', *EJIL: Talk!* (5 de febrero de 2024).

Durante la etapa de redacción, los Estados pueden recurrir a fuentes formales e informales, al igual que a consultas con partes interesadas internas y externas. Puede que la adopción de la posición nacional también deba seguir un proceso institucional definido, como la aprobación formal de una autoridad específica. Las posiciones nacionales pueden estar sujetas a revisión, ya que los Estados pueden decidir ajustar o revisar su posición original sobre los diferentes asuntos que hay en juego.

Estos varios pasos y estrategias de redacción revelan que la tarea de desarrollar y publicar una posición nacional no es trivial, y que puede ser especialmente difícil para los Estados que afrontan vacíos de capacidad o barreras políticas. Puede ser frustrante que el duro trabajo invertido en el proceso por todas las partes interesadas involucradas no culmine en la publicación de una posición. Pero esto no debe desanimar a los Estados. El proceso mismo es valioso, sin importar su resultado. Puede, por ejemplo, fomentar mayor diálogo y coordinación entre órganos nacionales, ayudar a los Estados a formular posiciones internas que no es necesario publicar y prepararlos mejor para los debates en procesos multilaterales. En particular, el conocimiento adquirido durante las sesiones de capacitación, debate y/o redacción de una posición nacional puede usarse en negociaciones diplomáticas y presentaciones más dirigidas en el Grupo de Trabajo de Composición Abierta (GTCA) de la ONU y otros foros multilaterales. Como se ha indicado en diferentes capítulos de este manual, los Estados también pueden usar las presentaciones para expresar sus perspectivas sobre cómo aplican las diferentes reglas y principios del derecho internacional a las actividades cibernéticas.

El **Capítulo 4** ofrece una visión general de los diversos asuntos sustantivos cubiertos en las posiciones nacionales hasta la fecha, al igual que las consideraciones políticas subyacentes sobre cómo los Estados han seleccionado y abordado estos asuntos. Aunque existe cierta variación en la elección de los temas, así como en la profundidad del análisis, las posiciones nacionales publicadas hasta la fecha presentan una lista ampliamente consistente de asuntos o áreas del derecho internacional. Estos incluyen las reglas y principios fundamentales, como el principio de soberanía y sus corolarios, incluida la no intervención, la prohibición del uso de la fuerza y la diligencia debida, así como el arreglo pacífico de controversias y la autodeterminación. Las posiciones nacionales también abordan los regímenes especializados del derecho internacional, que incluyen, en particular, el DIH, el derecho internacional de los derechos humanos (DIDH) y el derecho penal internacional. La responsabilidad del Estado, que rige las consecuencias de incumplir las obligaciones internacionales, también es un tema popular, incluyendo la atribución, las contramedidas y el Estado de necesidad.

Las posiciones nacionales pueden ayudar a que los Estados entiendan sus diferencias, las debatan constructivamente y busquen un terreno común cuando tengan la oportunidad para hacerlo.

Las posiciones nacionales han fomentado acuerdos sobre algunos de estos asuntos, lo que incluye, como punto de partida, que el derecho internacional se aplica a las actividades cibernéticas. También hay acuerdo respecto a que el DIH y el DIDH en principio son aplicables a las TIC. Es más, está emergiendo un consenso con relación a los componentes de reglas o principios específicos, como la no intervención y la responsabilidad del Estado. Sin embargo, como se indicó, las posiciones nacionales han revelado áreas de desacuerdo. Entre estas están si ciertos principios también dan lugar a obligaciones, los umbrales o condiciones que activan el incumplimiento de ciertas obligaciones, y si y hasta qué punto ciertos tipos de actividad cibernética, como el espionaje, pueden constituir violaciones. Como se indicó, algunos desacuerdos son inevitables, especialmente en un sistema jurídico descentralizado como el derecho internacional. Del mismo modo, no todos los desacuerdos son necesariamente perjudiciales para la paz y seguridad internacional. Pero, fundamentalmente, los desacuerdos deben conocerse para poderse debatir, y, si es necesario, solucionarlos. Las posiciones nacionales pueden ayudar a que los Estados entiendan sus diferencias, las debatan de manera constructiva y busquen un terreno común cuando tengan la oportunidad de hacerlo.

No solo importa el contenido de las posiciones nacionales, su presentación es igual de importante, ya que será lo que marque el impacto que puedan tener. En el **Capítulo 5** se habló de las diferentes opciones que tienen los Estados con relación al formato, estilo, idioma y difusión de su posición nacional. Estas características varían significativamente entre las posiciones nacionales publicadas hasta la fecha, y reflejan elecciones políticas importantes, como el estatus jurídico, el enfoque y los fines de dichas posiciones. Aunque algunas posiciones nacionales fueron emitidas como discursos gubernamentales, declaraciones en la ONU y artículos académicos, la gran mayoría fueron publicadas como documentos escritos autónomos. Su estilo también es variado, desde documentos cortos de dos a cinco páginas, hasta más largos de 22 páginas. Por supuesto, las posiciones nacionales más cortas son más generales, y en ocasiones priorizan los interrogantes de la política. Las más largas cubren más temas y profundizan más en cuestiones jurídicas específicas, lo que las hace más adecuadas si el objetivo es clarificar y/o desarrollar el derecho internacional en su aplicación a las actividades cibernéticas. La mayoría de las posiciones nacionales contienen referencias y encabezados, que pueden aumentar su autoridad jurídica, legibilidad y claridad. Los resúmenes, apartados numerados, ejemplos y ayudas visuales también pueden aumentar significativamente la accesibilidad de una posición, pero muy pocas incorporan estos elementos.

Todas las posiciones nacionales emplean el vocabulario tradicional del derecho internacional y utilizan terminología específica para indicar su posición sobre diferentes cuestiones jurídicas. La mayoría de las posiciones nacionales y las dos conjuntas fueron publicadas en inglés, la lengua común del derecho internacional y la diplomacia. Esto ha garantizado el uso de terminología jurídica consistente y visibilidad entre los públicos relevantes, incluidos los abogados gubernamentales, diplomáticos y académicos. Sin embargo, para aumentar la accesibilidad de las posiciones nacionales para otras audiencias, especialmente las partes interesadas nacionales y extranjeras en el Sur Global, puede que los Estados quieran considerar la publicación de sus posiciones nacionales en otros idiomas diferentes del inglés, como los demás idiomas oficiales de la ONU (árabe, chino, francés, ruso y español). Los Estados también deberían considerar diferentes estrategias para difundir sus posiciones a los públicos destinatarios, incluyendo su publicación en bases de datos en línea relevantes, revistas académicas, blogs y redes sociales, así como organizar eventos públicos y privados para debatirlas. En general, al decir la elección de formato, estilo, idioma y las estrategias de difusión, los Estados deben buscar un equilibrio entre la autoridad jurídica y la accesibilidad.

¿Qué sigue?

Si las posiciones nacionales se han convertido en el principal vehículo mediante el que los Estados expresan sus perspectivas sobre el derecho internacional en el contexto cibernético, más Estados deberían sentirse empoderados para desarrollar y publicar sus posiciones nacionales, si desean hacerlo. Como se trató anteriormente, eso requiere esfuerzos concertados para crear conciencia sobre la importancia de las posiciones nacionales, así como para desarrollar la capacidad de los Estados en el aspecto sustantivo del derecho internacional y el proceso de desarrollar posiciones, priorizando a los que más la necesitan.

Como se indicó en la **introducción**, el equipo principal de este proyecto llevó a cabo tres consultas regionales con representantes de Estados de África, las Américas, Asia y el Pacífico. El objetivo fue intercambiar perspectivas sobre los diferentes temas abordados en este manual y entender qué se necesita para cerrar las brechas de capacidad entre Estados. No obstante, hay espacio para extender estos debates a otras regiones, en particular a Europa de Este y el Medio Oriente, con la debida consideración de las diferencias lingüísticas y culturales que pueden afectar el entendimiento del derecho internacional en esas regiones. Este tema también se beneficiaría de debates más profundos en foros internacionales, como la ONU. El futuro mecanismo permanente que podría suceder al GTCA en las discusiones generales sobre las implicaciones de seguridad de las TIC sería una buena opción para continuar la conversación sobre las posiciones nacionales en la ONU.[3]

3 Consulte Asamblea General de las Naciones Unidas, *Desarrollos en el campo de la información y las telecomunicaciones en el contexto de la seguridad internacional*, A/79/214*(2024), párr. 5, 7 y 56 a 60.

También ha habido algunos debates sobre la adopción de otros instrumentos o materiales sobre la aplicación del derecho internacional en el contexto cibernético. Por ejemplo, la posición conjunta de la UA sugiere que el 'proceso de articular reglas del derecho internacional que aplican al uso de TIC en el ciberespacio se beneficiaría de la adopción de una declaración de las Naciones Unidas sobre este tema'.[4] Es poco probable que el Consejo de Seguridad de la ONU adopte una resolución sobre la aplicación del derecho internacional a las actividades cibernéticas, dados los desacuerdos persistentes entre sus miembros permanentes. Por otro lado, la mayoría de los países miembros de las Naciones Unidas podría apoyar la adopción de una resolución sobre el tema por parte de la Asamblea General de la ONU, tal vez fundamentada en el trabajo del sucesor del GTCA. No obstante, el contenido de esta declaración probablemente sería general, como la mayoría de las resoluciones que hasta ahora ha adoptado la Asamblea General de las Naciones Unidas.

Algunos también han pedido que la Asamblea General u otro organismo competente de la ONU solicite una opinión consultiva a la Corte Internacional de Justicia (CIJ) sobre la aplicación del derecho internacional a las actividades cibernéticas.[5] Sin embargo, puede que la CIJ no esté bien posicionada para resolver la cuestión, dada la cantidad significativa de áreas y asuntos del derecho internacional, desde reglas generales y regímenes especializados hasta interrogantes sobre la responsabilidad del Estado, que son pertinentes a las actividades cibernéticas. Otros han especulado que la Comisión de Derecho Internacional debería iniciar un estudio y eventualmente emitir un informe sobre el tema, pero al momento de esta publicación, no ha habido señales de dicha propuesta. Sin embargo, se debe destacar que el asunto de aplicar el derecho internacional a las actividades cibernéticas actualmente está siendo estudiado por el *Institut de Droit International*.[6]

4 Posición conjunta de la UA (2024), párr. 7 (Trad. libre).

5 Consulte Estatuto de la Corte Internacional de Justicia, artículo 96.

6 Institut de Droit International, *Las aplicaciones del derecho internacional a las actividades cibernéticas* (2023).

Como se discute en este manual, algunos Estados han pedido un tratado jurídicamente vinculante para regir los diferentes aspectos de las TIC, como la información o la seguridad de los datos.[7] Diferentes partes interesadas también han propuesto la adopción de un tratado para ampliar las protecciones que ya ofrece el derecho internacional en el contexto cibernético, como un Convenio de Ginebra digital o un convenio para la protección de la infraestructura crítica frente a las operaciones cibernéticas.[8] Aunque estas propuestas puedan o no hacerse realidad, no riñen necesariamente con los esfuerzos para clarificar cómo el derecho internacional existente aplica a las actividades cibernéticas, incluido mediante posiciones nacionales. Los dos tipos de iniciativas pueden coexistir y complementarse entre sí.

Las posiciones nacionales también pueden catalizar la adopción de legislación nacional y documentos de política para internalizar y seguir desarrollando estándares de comportamiento responsable de los Estados en el contexto cibernético. En particular, los Estados pueden articular, mediante legislación nacional, los pasos prácticos que creen que se deben tomar internamente para implementar obligaciones tales como la soberanía, no intervención y diligencia debida, al igual que las protecciones de los derechos humanos contra las operaciones cibernéticas. De igual manera, los Estados pueden incorporar y desarrollar sus perspectivas sobre cómo aplica el DIH a las TIC en sus propios manuales militares o normas de intervención.

Ya sea a nivel nacional o internacional, también hay lugar para más debates prácticos sobre el contenido de las posiciones nacionales, tales como mediante ejercicios basados en escenarios o casos de estudio. Como se indicó en el **Capítulo 5**, muchas posiciones nacionales profundizan en las complejidades y controversias sobre las diferentes reglas y principios internacionales que son particularmente relevantes en el contexto cibernético. Sin embargo, lo hacen, principalmente, de un modo muy abstracto y solo unas cuantas posiciones referencian incidentes de la vida real, incluidos ejemplos de operaciones cibernéticas que hipotéticamente podrían violar el derecho internacional, o proponen pasos prácticos para implementar las obligaciones internacionales en el contexto cibernético.

Por último, dado el impacto positivo general de las posiciones nacionales, incluido en el derecho internacional en general, el modelo se puede aprovechar para fomentar el diálogo y los entendimientos comunes sobre otros desafíos mundiales que han dado lugar a inseguridad jurídica y desacuerdos entre los Estados. Este es el caso particular de los asuntos para los cuales no hay un tratado específico y/o un foro permanente para debates multilaterales o adjudicación; por ejemplo,

7 Por ejemplo, Federación Rusa, *Concepto actualizado de la Convención de las Naciones Unidas sobre garantizar la seguridad de la información internacional*, (2023); República Popular de China, *Iniciativa global sobre seguridad de los datos,* 2022).

8 Consulte, por ejemplo Patryk Pawlak y Aude Géry, "¿Por qué el mundo necesita un nuevo tratado sobre ciberseguridad para la infraestructura crítica', Carnegie Endowment for International Peace (28 de marzo de 2024); Microsoft, 'La necesidad de un Convenio de Ginebra digital' (14 de febrero de 2017).

otras tecnologías emergentes, como la inteligencia artificial. De hecho, los Estados han comenzado a publicar perspectivas nacionales sobre cómo piensan que el derecho internacional, especialmente el DIH, aplica a los sistemas de armas letales autónomas.[9] Y recientemente, la Asamblea General de las Naciones Unidas invitó a los Estados miembro a presentar sus perspectivas sobre la paz internacional y las implicaciones de seguridad del uso de la inteligencia artificial en el dominio militar, más allá de las armas letales autónomas, incluyendo cómo aborda el asunto el derecho internacional.[10]

Otras áreas, como el espacio ultraterrestre y los derechos humanos en un conflicto armado, también se podrían beneficiar de declaraciones sobre cómo aborda el derecho internacional los desafíos emergentes, dado su panorama rápidamente cambiante y la ausencia de un foro multilateral especializado. Estas declaraciones no tienen que ser tan exhaustivas como las posiciones nacionales publicadas en el contexto de las TIC, ya que muchas de estas ya cubren los interrogantes generales del derecho internacional en mayor detalle (por ejemplo, soberanía, no intervención y diligencia debida). Las posiciones nacionales sobre inteligencia artificial y otros asuntos pueden basarse en este acervo, para dirigirse a preguntas más específicas del derecho internacional que suponen desafíos concretos en estos contextos.

Sea cual fuere el futuro de las posiciones nacionales, e independientemente de si surgen nuevos instrumentos o acuerdos adicionales sobre derecho internacional en el ciberespacio y otros contextos, una cosa está clara: las posiciones publicadas hasta ahora son un legado para el progreso que los Estados ya han hecho, y pueden contribuir a construir sobre ellas en un entorno desafiante. Son una señal de que, incluso si subsisten diferencias jurídicas y tensiones geopolíticas, el diálogo constructivo es posible. Esperamos que este manual pueda inspirar a los Estados a continuar por este camino, fomentando la transparencia, el debate y los entendimientos comunes sobre cómo el derecho internacional puede ayudar a abordar uno de los mayores desafíos del mundo en línea y fuera de línea.

9 Consulte Asamblea General de las Naciones Unidas, *Sistemas de armas letales autónomas: Informe del Secretario General*, A/79/88 (1 de julio de 2024).

10 Asamblea General de las Naciones Unidas, *Inteligencia artificial en el dominio militar y sus implicaciones para la paz y seguridad internacional*, A/RES/79/239 (31 de diciembre de 2024).

Manual para el desarrollo de una posición nacional sobre el derecho internacional y las actividades cibernéticas:
Una guía práctica para los Estados

BIBLIOGRAFÍA

Libros y monografías

Cryer, Robert, Robinson, Darryl y Vasiliev, Sergey, *An Introduction to International Criminal Law and Procedure* [Una introducción al derecho y procedimiento penal internacional] (CUP 2019).

Dias, Talita, *Beyond Imperfect Justice: The Principles of Legality and Fair Labelling in International Criminal Law* [Más allá de la justicia imperfecta: Los principios de la legalidad y la categorización justa en el derecho penal internacional] (Brill 2022).

Gallant, Kenneth S, *The Principle of Legality in International and Comparative Criminal Law* [El principio de la legalidad en el derecho penal internacional y comparativo] (CUP 2010).

Knop, Karen, *Diversity and Self-Determination in International Law* [Diversidad y autodeterminación en el derecho internacional] (CUP 2009).

Lahmann, Henning, *Unilateral Remedies to Cyber Operations: Self-Defence, Countermeasures, Necessity, and the Question of Attribution* [Reparaciones unilaterales para las operaciones cibernéticas: Legítima defensa, contramedidas, necesidad y el interrogante de la atribución] (CUP 2020).

Milanovic, Marko, *Extraterritorial Application of Human Rights Treaties: Law, Principles, and Policy* [Aplicación extraterritorial de los tratados de derechos humanos: legislación, principios y política] (OUP 2011).

Roscini, Marco, *Cyber Operations and the Use of Force in International Law* [Operaciones cibernéticas y uso de la fuerza en el derecho internacional] (OUP 2014).

– *International Law and the Principle of Non-Intervention* [Derecho internacional y el principio de la no intervención] (OUP 2024).

Schabas, William A, *The Customary International Law of Human Rights* [El derecho internacional consuetudinario de los derechos humanos](OUP 2021).

Sparks, Tom, *Self-Determination in the International Legal System* [Autodeterminación en el sistema jurídico internacional] (Bloomsbury 2023).

Sterio, Milena, *The Right to Self-Determination under International Law* [El derecho a la autodeterminación conforme al derecho internacional] (Routledge 2013).

Urs, Priya, Dias, Talita, Coco, Antonio y Akande, Dapo, *The International Law Protections against Cyber Operations Targeting the Healthcare Sector* [Las protecciones del derecho internacional contra las operaciones cibernéticas que tienen como objetivo el sector sanitario] (ELAC 2023).

Zoller, Elizabeth, *Peacetime Unilateral Remedies: An Analysis of Countermeasures* [Reparaciones unilaterales en tiempos de paz: Un análisis de las contramedidas](Transnational 1984).

Libros editados y documentos de referencia

Fisher, Ryan (editor), *Operational Law Handbook* [Manual jurídico operativo] (Departamento de Seguridad Jurídica Nacional, Escuela del Juez Defensor General, Ejército de los Estados Unidos, 2022).

Henckaerts, Jean-Marie y Doswald-Beck, Louise (editores), *Customary International Humanitarian Law: Volume I, Rules* [Derecho internacional humanitario consuetudinario] (CICR y CUP 2005).

CICR (editor), *Commentary on the Third Geneva Convention* [Comentario sobre el Tercer Convenio de Ginebra] (CUP 2021).

Schmitt, Michael N (editor), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* [Manual de Tallin 2.0 sobre el derecho internacional aplicable a las operaciones cibernéticas] (CUP 2017).

Contribuciones a colecciones editadas

Akande, Dapo, 'Sources of International Criminal Law' [Fuentes del derecho penal internacional], en Antonio Cassese (editor), *The Oxford Companion to International Criminal Justice* [Compendio de Oxford sobre derecho penal internacional] (OUP 2009).

Hollis, Duncan B y van Benthem, Tsvetelina, 'Threatening Force in Cyberspace' [Amenaza de uso de la fuerza en el ciberespacio], en Laura A Dickinson y Edward W Berg (editores), *Big Data and Armed Conflict: Cuestiones jurídicas sobre y bajo el umbral del conflicto armado* (OUP 2024).

Mačák, Kubo y Gisel, Laurent, 'The Legal Constraints of Cyber Operations in Armed Conflicts' [Las restricciones jurídicas de las operaciones cibernéticas en los conflictos armados] in Rajeswari Pillai Rajagopalan (editor), *Future Warfare and Technology: Issues and Strategies* [Futuro de la guerra y la tecnología: Problemas y estrategias] (Wiley 2022).

Pellet, Alain, 'Peaceful Settlement of International Disputes' [Arreglo pacífico de controversias internacionales] en Rüdiger Wolfrum (editor), *Max Planck Encyclopedia of Public International Law* (edición en línea, OUP 2013).

Tams, Christian, 'Article 2(4)' [Artículo 2(4)] en Bruno Simma et al (editores), *The Charter of the United Nations: A Commentary*, Vol. I [La Carta de las Naciones Unidas: Un comentario] (OUP 2024).

Tomuschat, Christian, 'Article 2(3)' [Artículo 2(4)] en Bruno Simma et al (editores), *The Charter of the United Nations: A Commentary,* Vol. I [La Carta de las Naciones Unidas: Un comentario] (OUP 2024).

Tsagourias, Nicholas, 'Cyber Disputes as International Legal Disputes' [Controversias cibernéticas como controversias del derecho internacional], en Nicholas Tsagourias, Russell Buchan y Daniel Franchini (editores, *Peaceful Settlement of Inter- State Cyber Disputes* [Arreglo pacífico de controversias cibernéticas entre Estados] (Hart 2024).

– 'Electoral Cyber Interference, Self-Determination and the Principle of Non- intervention in Cyberspace' [Interferencia electoral cibernética, autodeterminación y el principio de la no intervención en el ciberespacio], en Dennis Broeders y Bibi van den Berg (editores), *Governing Cyberspace: Behavior, Power, and Diplomacy* [Gobernar el ciberespacio: Comportamiento, poder y diplomacia](Rowman & Littlefield 2020).

Ziegler, Katja S, *'Domaine réservé'* en Rüdiger Wolfrum (editor), Max Planck Encyclopedia of Public International Law (edición en línea, OUP 2013).

Artículos de revistas

Cleveland, Sarah H, 'Embedded International Law and the Constitution Abroad' [Derecho internacional incorporado y la constitución exterior] (2010) 110 Columbia Law Review 225.

Coco, Antonio, and de Souza Dias, Talita, 'Cyber Due Diligence': A Patchwork of Protective Obligations in International Law' [Diligencia debida cibernética: Un entramado de obligaciones de protección en el derecho internacional] (2021) 32 *European Journal of International Law* 795.

Coco, Antonio, Dias, Talita y van Benthem, Tsvetelina, 'Illegal: The SolarWinds Hack under International Law' [Ilegal: El hack de SolarWinds a la luz del derecho internacional] (2022) 33(4) *European Journal of International Law* 1275.

Deeks, Ashley, 'Defend Forward and Cyber Countermeasures' [Defensa preventiva y contramedidas cibernéticas], Grupo de trabajo de Hoover sobre seguridad nacional, tecnología y legislación (2020).

Dias, Talita, 'Finding Common Ground: The Right to be Free from Incitement to Discrimination, Hostility, and Violence in the Digital Age' [Encontrado bases comunes: El derecho a estar libres de incitación a la discriminación, hostilidad y violencia en la era digital] (2024) 16(4) *Global Responsibility to Protect* 391.

Droege, Cordula, 'Elective affinities? Human rights and humanitarian law' [¿Afinidades electivas? Derechos humanos y derecho humanitario] (2008) 90 International Review of the Red Cross 501.

– 'Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians' [Sal de mi nube: Guerra cibernética, derecho internacional humanitario y la protección de los civiles] (2012) 94(886), Revista Internacional de la Cruz Roja.

Egan, Brian J, 'International Law and Stability in Cyberspace' [Derecho internacional y estabilidad en el ciberespacio] (2017) 35(1) *Berkeley Journal of International Law* 169.

Engdahl, Ola, 'Sweden's Position Paper on the Application of International Law' [Posición de Suecia en la aplicación del derecho internacional] en Cyberspace' (2023) 92(3) *Nordic Journal of International Law* 489.

Helal, Mohamed, 'On Coercion in International Law' [Sobre la coerción en el derecho internacional] (2019) 52(1) NYU *Journal of International Law and Politics* 1.

Henriksen, Anders, 'The end of the road for the UN GGE process: The future regulation of cyberspace' [El final del camino para el proceso del Grupo de Expertos Gubernamentales (GEG) de la ONU: La reglamentación futura del ciberespacio] (2019) 5(1) *Journal of Cybersecurity* 1.

Jackson, Miles, and Paddeu, Federica, 'The Countermeasures of Others' [Las contramedidas de los demás](2024) 118(2) *American Journal of International Law* 231.

Kjelgaard, Jeppe Mejer, and Melgaard, Ulf, 'Denmark's Position Paper on the Application of International Law in Cyberspace' [Documento de posición de Dinamarca sobre la aplicación del derecho internacional en el ciberespacio] (2023) 92(3) *Nordic Journal of International Law* 446.

Lahmann, Henning, 'The Plea of Necessity in Cyber Emergencies' [El argumento de la necesidad en las emergencias cibernéticas] (2023) 92(3) N*ordic Journal of International Law* 422.

Lehto, Marja, 'Finland's views on International Law and Cyberspace' [Perspectivas de Finlandia sobre el derecho internacional y el ciberespacio] (2023) 92(3) *Nordic Journal of International Law* 456.

Mačák, Kubo, 'Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law' [Objetivos militares 2.0: El caso de la interpretación de los datos informáticos como objetivos conforme al derecho internacional humanitario] (2015) 48 *Israel Law Review* 55.

Mendelson, Maurice, "The Formation of Customary International Law' [La formación del derecho internacional consuetudinario](1998) 272 *Recueil des Cours* 155.

Milanovic, Marko, and Schmitt, Michael N, 'Cyber attacks and cyber (mis)information operations during a pandemic' [Ataques cibernéticos y operaciones de desinformación cibernética durante una pandemia] (2020) 11(1) Journal of National Security Law and Policy 247.

Musæus, Vibeke, 'Norway's Position Paper on International Law and Cyberspace' [Documento de posición de Noruega sobre el derecho internacional y el ciberespacio] (2023) 92(3) *Nordic Journal of International Law* 470.

Ohlin, Jens D, 'Did Russian Cyber-Interference in the 2016 Election Violate International Law?' [¿La interferencia cibernética de Rusia en las elecciones de 2016 violó el derecho internacional?] (2017) 95 *Texas Law Review* 1579.

Petridou, Evangelia, 'Theories of the Policy Process' [Teorías del proceso de las políticas] (2014) 42 *Policy Studies Journal* S12.

Roscini, Marco, 'Gravity in the Statute of the International Criminal Court and Cyber Conduct that Constitutes, Instigates or Facilitates International Crimes' [Gravedad en el Estatuto de la Corte Penal Internacional y la conducta cibernética que constituye, instiga o facilita los crímenes internacionales] (2019) 30 *Criminal Law Forum* 247.

Schmitt, Michael N y Watts, Sean, 'Collective cyber countermeasures?' [Contramedidas cibernéticas colectivas] (2021) 12 *Harvard National Security Journal* 373.

Schöndorf, Roy, 'Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations' [La perspectiva de Israel sobre las cuestiones jurídicas y prácticas relacionados con la aplicación del derecho internacional a las operaciones cibernéticas] (2021) 97 *International Law Studies* 395.

Shany, Yuval, 'Taking Universality Seriously: A Functional Approach to Extraterritoriality in International Human Rights Law' [Tomar la universalidad con seriedad: Un enfoque funcional a la extraterritorialidad en el derecho internacional de los derechos humanos] (2013) 7 *The Law and Ethics of Human Rights* 47.

Shany, Yuval, and Schmitt, Michael N, 'An International Attribution Mechanism for Hostile Cyber Operations' [Un mecanismo de atribución internacional para las operaciones cibernéticas hostiles] (2020) 96 *International Law Studies* 196.

van Benthem, Tsvetelina, Dias, Talita, and Hollis, Duncan B, 'Information Operations under International Law' [Operaciones de información conforme con el derecho internacional] (2022) 55 *Vanderbilt Journal of Transnational Law* 1217.

Informes seleccionados y otras fuentes en línea

Australia, *Australia's Cyber Security Strategy* [Estrategia de Ciberseguridad de Australia] (2016).

– Departamento de Asuntos y Comercio Exterior, *Australia's International Cyber Engagement Strategy* [Internacional de Australia] (Octubre de 2017).

Instituto de Política Estratégica Australiano, International Cyber Policy Centre, *The UN norms of responsible state behaviour in cyberspace Guidance on implementation for Member States of ASEAN* [Las normas de la ONU para el comportamiento responsable de los Estados en el ciberespacio: Orientación sobre la implementación para los Estados miembro de ASEAN] (Marzo de 2022).

Austria, *Pre-Draft Report of the OEWG – ICT: Comments by Austria* [Preproyecto del informe del GTCA – TIC: Comentarios de Austria] (31 de marzo de 2020).

Chatham House, *Applying the Plea of Necessity to Cyber Operations*, [Aplicar la invocación de necesidad a las operaciones cibernéticas], resumen de reunión, International Law Programme (27 de septiembre de 2023).

Ministerio de Relaciones Exteriores de Chile, *Derecho Internacional*, ONU, Nueva York, GTCA, Sexta sesión sustantiva (11 a 15 de diciembre de 2023).

– *National Cybersecurity Policy* [Política de ciberseguridad nacional] (2017-2022).

China (República Popular de China), *Global Initiative on Data Security* [Iniciativa global sobre seguridad de los datos](2022).

Misión china ante la ONU, *Statement by the Chinese Delegation at the Thematic Debate of the First Committee of the 72th UNGA* [Declaración de la delegación china en el Debate temático del Primera Comisión de la UNGA 27](2017).

Christou, George, 'Cyber Diplomacy: From Concept to Practice' [Diplomacia cibernética: del concepto a la práctica], *Tallinn Paper* n.º 14, OTAN CCDCOE (2024).

Consejo de la Unión Europea, 'EU sanctions – New recital in Council Decision' [Sanciones de la Unión Europea: nuevo recital en la decisión de Consejo], (CFSP) 2023/191 del 27 de enero de 2023 – Countermeasures, WK 5169/2023 INIT (2023).

Oficina del representante exterior del Cuba, *71 AGNU: Cuba at the final session of the Group of Governmental Experts on the developments in the field of information and telecommunications in the context of international security* [Cuba en la sesión final 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 2017).

Dias, Talita, *Countermeasures in international law and their role in cyberspace* [Contramedidas en el derecho internacional y su rol en el ciberespacio] (Chatham House, 2024).

Ministerio de Asuntos Exteriores de Estonia, *Tallinn Workshops on International Law and Cyber Operations, Compendium of reports* [Talleres Tallin sobre derecho internacional y operaciones cibernéticas: Compendio de informes](2023).

Comisión Europea, *The EU's Cybersecurity Strategy for the Digital Decade* [La estrategia de ciberseguridad de la Unión Europea para la década digital] (2020).

Ministerio Federal de Asuntos Exteriores de Alemania, '"Cyber Security as a Dimension of Security Policy' [Ciberseguridad como dimensión de la política de seguridad]. Discurso del embajador Norbert Riedel, Comisionado para Política Cibernética Internacional, Ministerio Federal de Asuntos Exteriores, Berlín, en Chatham House, Londres (18 May 2015).

CICR, *International humanitarian law and the challenges of contemporary armed conflicts* [Derecho internacional humanitario y los desafíos de los conflictos armados contemporáneos] (Octubre de 2015).

– *International humanitarian law and cyber operations during armed conflicts* [Derecho internacional humanitario y las operaciones cibernéticas durante los conflictos armados] (2019).

– *How is the term 'armed conflict' defined in international humanitarian law?* [¿Cómo se define el término 'conflicto armado' en el derecho internacional humanitario?],

Kavanagh, Camino, *The United Nations, Cyberspace and International Peace and Security. Responding to Complexity in the 21st Century* [Las Naciones Unidas, ciberespacio y paz y seguridad internacional. Responder a la complejidad del siglo XXI], UNIDIR (2017).

McLaughlin, Robert, *'Data as a Military Objective'* [Los datos como objetivo militar], Australian Institute of International

Microsoft, 'The need for a Digital Geneva Convention' [La necesidad de un Convenio de Ginebra digital] (14 de febrero de 2017).

Moynihan, Harriet, *The Application of International Law to State Cyberattacks: Sovereignty and Non-Intervention* [Las aplicaciones del derecho internacional a los ataques cibernéticos estatales: Soberanía y no intervención] (Chatham House 2019).

National Cybersecurity Guide, *Guide to Developing a National Cybersecurity Strategy* [Guia para desarrollar una estrategia nacional de seguridad], segunda edición (2021).

Foro de las Islas del Pacífico, *Declaración del Presidente del PIF en nombre del Foro de las Islas del Pacífico*, ONU (Nueva York, 4 de diciembre de 2024).

Misión permanente de Liechtenstein ante las Naciones Unidas, *The Council of Advisers' Report on the Application of the Rome Statute to Cyberwarfare* [Informe sobre la aplicación del Estatuto de Roma a la guerra cibernética] (Agosto de 2021).

Persi Paoli, Giacomo, Dominioni, Samuele, Rafiq, Aamna y Filipová, Lenka, *Accelerating ICT Security Capacity-Building: Puntos clave de la Mesa Redonda Mundial 2024 sobre creación de capacidades sobre las TIC* , UNIDIR, Ginebra (2024).

Federación Rusa, *Updated Concept of the Convention of the United Nations on Ensuring International Information Security* [Concepto actualizado de la Convención de las Naciones Unidas sobre garantizar la seguridad de la información internacional] (2023).

Suráfrica, *Statement by South Africa in the ninth session of the Open-Ended Working Group on security of and in the use of ICTs (2021-2025) - International Law,* [Declaración de Sudáfrica en la novena sesión del Grupo de Trabajo de Composición Abierta sobre seguridad y uso de las TIC (2021 – 2025) – Derecho internacional], ONU, Nueva York (4 de diciembre de 2024).

Asamblea General de las Naciones Unidas, Informe de los, *Report of the International Law Commission on the work of its fifty-second session* [Informe de la Comisión de Derecho Internacional sobre el trabajo de su cincuentaidosava sesión], A/CN.4/513 (15 de febrero de 2001).

– Asamblea General de las Naciones Unidas, *Informe del Grupo de Expertos Gubernamentales sobre los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional,* A/65/201 (30 de julio de 2010).

– *Desarrollos en el campo de la información y las telecomunicaciones en el contexto de la seguridad internacional. Informe del Secretario General,* A/66/152 (15 de julio de 2011)

– Asamblea General de las Naciones Unidas, *Informe del Grupo de Expertos Gubernamentales sobre los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional,* A/68/98 (24 de junio de 2010).

– Asamblea General de las Naciones Unidas, *Informe del Grupo de Expertos Gubernamentales sobre los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional*, A/70/174 (22 de julio de 2015).

– *Informe del Grupo de Trabajo de Composición Abierta sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional*, A/AC.290/2021/CRP.2 (10 de marzo de 2021).

– *Resumen del Presidente sobre el Grupo de Trabajo de Composición Abierta sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional*, A/AC.290/2021/CRP.3 (10 de marzo de 2021).

– *Informe del Grupo de Trabajo de Composición Abierta sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional*, A/75/816 (18 de marzo de 2021).

– *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*, A /76/136* (13 de julio de 2021).

– Asamblea General de las Naciones Unidas, *Informe del Grupo de Expertos Gubernamentales sobre los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional*, A/76/135 (14 de julio de 2021).

– *Informe del Grupo de Trabajo de Composición Abierta sobre la seguridad y el uso de las tecnologías de la información y comunicación 2021–2025 [I]*, A/77/275 (8 de agosto de 2022).

– *Informe del Grupo de Trabajo de Composición Abierta sobre la seguridad y el uso de las tecnologías de la información y comunicación 2021-2025*, A/78/265 (1 de agosto de 2023).

– *Análisis para estudiar el panorama de los programas e iniciativas de creación de capacidad dentro y fuera de las Naciones Unidas y a escala mundial y regional*, A/AC.292/2024/2 (22 de enero de 2024).

– *Lethal autonomous weapons systems: Report of the Secretary-General* [Sistemas de armas letales autónomas: Informe del Secretario General], A/79/88 (1 de julio de 2024).

– *Informe del Grupo de Trabajo de Composición Abierta sobre la seguridad y el uso de las tecnologías de la información y comunicación*, A/79/214 (22 de julio de 2024).

– *Informe inicial sobre la propuesta para diseñar y poner en funcionamiento un portal mundial de cooperación y creación de capacidad en materia de seguridad de las tecnologías de la información y las comunicaciones*, A/AC.292/2025/1 (14 de enero de 2025).

ONU, *Fourth report on international liability for injurious consequences arising out of acts not prohibited by international law, by Robert. Q. [Cuarto informe sobre la responsabilidad internacional por las consecuencias injuriosas que surgen de actos no prohibidos por el derecho internacional, por Robert Q.] Quentin-Baxter, Relator especial*, A/ CN.4/373 y Corr.1&.2 (27 de junio de 1983).

UNIDIR, *A Compendium of Good Practices: Developing a National Position on the Interpretation of International Law and State Use of ICT* [Compendio de buenas prácticas: Desarrollo de una posición nacional sobre la interpretación del derecho internacional y el uso de las TIC por los Estados] (2024).

Tratados internacionales, resoluciones y otros documentos

26ª Conferencia Internacional de la Cruz Roja y de la Media Luna Roja, *Resolution 1: International Humanitarian Law – From Law to Action* [Resolución 1: Derecho internacional humanitario: del derecho a la acción], 26IC/95/R1 (3 de diciembre de 1995).

34ª Conferencia Internacional de la Cruz Roja y de la Media Luna Roja, *Resolución 2: Protección de la población civil y de otras personas y bienes protegidos ante el posible costo humano de las actividades relacionadas con las tecnologías de la información y las comunicaciones durante conflictos armados* durante el conflicto armado, 34IC/24/R2 (octubre de 2024).

Carta Africana de Derechos Humanos y de los Pueblos, CAB/LEG/67/3 ver. 5, 21 ILM 58 (1982) (27 de junio de 1981).

Convención Americana sobre Derechos Humanos, Serie de tratados, n.° 36 (abierto para firma de 22 November 1969, entered into force 18 July 1978), 1144 UNTS 123.

Carta de las Naciones Unidas (adoptada el 26 de junio 1945, en vigor el 24 de octubre de 1945) 1 UNTS 16

Convención para la prevención y la sanción del crimen de genocidio (firmada el 9 de diciembre de 1948, en vigor desde el 12 de enero 1951) 78 UNTS 277.

Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, según enmiendas núm. 11 y 14, ETS 5, (4 de noviembre de 1950).

Primer Convenio de Ginebra, para Aliviar la Suerte de la Condición de los Heridos de los Ejércitos en Campaña (firmado el 12 de agosto de 1949, en vigor desde el 21 de octubre de 1950) 75 UNTS 3.

Segundo Convenio de Ginebra, para el Mejoramiento de la Condición de los Heridos, Enfermos y Náufragos de las Fuerzas Armadas en el Mar(firmado el 12 de agosto de 1949, en vigor desde el 21 de octubre de 1950) 75 UNTS 85.

Tercer Convenio de Ginebra, relativo al tratamiento de los prisioneros de guerra (firmado el 12 de agosto de 1949, en vigor desde el 21 octubre de 1950) 75 UNTS 135.

Cuarto Convenio de Ginebra, relativo a la protección debida a las personas civiles en tiempo de guerra (firmado el 12 de agosto de 1949, en vigor desde el 21 de octubre de 1950) 75 UNTS 287.

CDH, *Observación general núm. 31[31]: La naturaleza de la obligación jurídica general impuesta general impuesta a los Estados Partes del Pacto*, CCPR/C/21/Ver.1/Add.13 (26 de mayo de 2004).

– *Observación general núm. 34: Artículo 19: Libertad de opinión y libertad de expresión,* CCPR/C/GC/34 (12 de septiembre de 2011).

– *General Comment No 36: Article 6: Right to Life* [Observación general 36: Artículo 6: Derecho a la vida], CCPR/C/GC/36 (3 de septiembre de 2019).

CDI, *Draft Articles on Prevention of Transboundary Harm from Hazardous Activities, with commentaries* [Proyecto de artículos sobre la prevención de los daños transfronterizos causados por actividades peligrosas, con comentarios], A/56/10 (2001).

– *Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries* [Artículos sobre la responsabilidad de los Estados por hechos internacionalmente ilícitos], A/56/10 (2001).

– *Draft conclusions on subsequent agreements and subsequent practice in relation to the interpretation of treaties* [Proyecto de conclusiones sobre los acuerdos ulteriores y la práctica ulterior con relación con la interpretación de los tratados], A/73/10 (2018).

– *Draft conclusions on the identification of customary international law, with commentaries* [Proyecto de conclusiones sobre la identificación del derecho internacional consuetudinario con comentarios], A/73/10 (2018).

– *Draft articles on Prevention and Punishment of Crimes Against Humanity* [Proyecto de conclusiones sobre la prevención y castigo de los crímenes de lesa humanidad], A/74/10 (2019).

– *Draft conclusions on identification and legal consequences of peremptory norms of*

general international law (jus cogens) [Proyecto de conclusiones sobre la identificación y consecuencias jurídicas de las normas imperativas del derecho internacional general (jus cogens)], A/77/10 (2022).

International Convention on the Elimination of All Forms of Racial Discrimination [Convención Internacional sobre la Eliminación de todas las Formas de Discriminación Racial] (21 de diciembre de 1965) 660 UNTS 195.

Pacto Internacional de Derechos Civiles y Políticos (16 de diciembre de 1966) 999 UNTS 171.

ACNUDH, *Principios Rectores sobre las empresas y los derechos humanos: puesta en práctica del marco de las Naciones Unidas para 'proteger, respetar y remediar,* respetar y remediar' de las Naciones Unidas] (2011).

Protocolo adicional a los Convenios de Ginebra del 12 de agosto de 1949 relativo a la protección de las víctimas de los conflictos internacionales armados (Protocolo I) (firmado el 12 de diciembre de 1977, en vigor desde el 7 de diciembre de 1978) 1125 UNTS 3.

Protocolo adicional a los Convenios de Ginebra del 12 de agosto de 1949 relativo a la protección de las víctimas de los conflictos armados no internacionales (Protocolo II) (firmado el 12 de diciembre de 1977, en vigor desde el 7 de diciembre de 1978) 1125 UNTS 609.

Estatuto de Roma de la Corte Penal Internacional (adoptado el 17 de julio de 1998, en vigor desde el 1 de julio de 2002) 2187 UNTS 90 (y sus enmiendas).

Estatuto de la Corte Internacional de Justicia del 26 de junio 1945, anexado a la Carta de las Naciones Unidas.

Asamblea General de las Naciones Unidas, Declaración, *Declaración sobre la concesión de la independencia a los países y pueblos coloniales*, res. 1514 (XV) (14 de diciembre de 1960).

– *Declaración sobre los principios de derecho internacional referentes a las relaciones de amistad y a la cooperación entre los Estados de conformidad con la Carta de las Naciones Unidas,* A/RES/2625 (XXV) (24 de octubre de 1970) Anexo

– *Declaración sobre la inadmisibilidad de la intervención e interferencia en los asuntos internos de los Estados,* A/RES/36/103 (9 de diciembre de 1981).

– *Declaración de Manila sobre el Arreglo Pacífico de Controversias Internacionales,* A/RES/37/10 (15 de noviembre de 1982).

– *Resolución adoptada por la Asamblea General el 22 de diciembre de 2018 [sobre el informe del Primera Comisión (A/73/505)] 73/266. Avanzar el comportamiento responsable de los Estados en el ciberespacio en el contexto de la seguridad internacional,* A/RES/73/266 (2 de enero de 2019).

– *Pacto Digital Global,* A/79/L.2 (22 de septiembre de 2024).

– *Inteligencia artificial en el dominio militar y sus implicaciones para la paz y seguridad internacional,* A/RES/79/239 (31 de diciembre de 2024).

ONU, Proclamación de Teherán, Acto final de la conferencia internacional sobre derechos humanos, Teherán, 22 de abril a 13 de mayo de 1968, A/CONF.32/41.

UNCDH, *Promoción, protección y disfrute de los derechos humanos en Internet,* A/ HRC/RES/32/13 (1 de julio de 2016).

Declaración Universal de los Derechos Humanos (Resolución de la Asamblea General de la ONU 217 A (III) del 10 de diciembre de 1948).

Convención de Viena sobre el Derecho de los Tratados (adoptada el 23 de mayo de 1969, en vigor desde el 27 de enero de 1908) 1155 UNTS 331.

Jurisprudencia internacional

TEDH, *Banković and others v Belgium and others (App no 52207/99)* [Banković y otros vs. Bélgica y otros (Ap. núm. 52207/99)] (12 de diciembre de 2001).

– *Al-Skeini and others v United Kingdom (App no 55721/07)* [Al-Skeini y otros vs. Reino Unido (ap. núm. 55721/07)] (7 de julio de 2011)

Corte IDH, *Velásquez Rodríguez vs. Honduras*, (Fondo) (Ser C) núm. 4 (29 de julio de 1988).

CPI, Fiscalía vs. Ntaganda, *Appeals Judgment on the appeals of Mr Bosco Ntaganda and the Prosecutor against the decision of Trial Chamber VI of 8 July 2019 entitled 'Judgment'* [Fiscalía vs. Ntaganda, Sentencia de apelación sobre las apelaciones de Bosco Ntaganda y el Fiscalía contra la decisión de la Cámara del tribunal VI del 8 de julio de 2019 titulada 'Sentencia'] (30 de marzo de 2021), ICC-01/04-02/06-2666-Red 30-03-2021.

CIJ, *Caso del Canal de Corfú (Reino Unido vs. Albania)* (Fondo) [1949] CIJ Rep. 4.

– *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v US)* [Actividades militares y paramilitares en y contra Nicaragua (Nicaragua vs. Estados Unidos)] (Fondo) [1986] CIJ Rep. 14.

– *Timor del Este (Portugal vs. Australia)* (Sentencia) [1995] CIJ Rep. 90.

– *Legality of the Threat or Use of Nuclear Weapons* (Opinión consultiva) [Legalidad de la amenaza o uso de armas nucleares. Opinión Asesora] (1996) CIJ Rep. 226.

– *Gabčíkovo-Proyecto Gabčíkovo-Nagymaros (Hungría/Eslovaquia)* (Sentencia) [1997] CIJ Rep. 7.

– *Jurisdicción de pesqueras (España vs. Canadá)* (Jurisdicción de la Corte) [1998 CIJ Rep. 432.

– *Caso relacionado con plataformas petroleras (Irán vs. EE. UU.)* (Sentencia) [2003] CIJ Rep. 161.

– *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory* (Opinión consultiva) [Consecuencias jurídicas de la construcción de un muro en el territorio palestino ocupado (Opinión consultiva)] (2004) CIJ Rep. 136.

– *Case Concerning Armed Activities in the Territory of the Congo (Democratic Republic of Congo v Uganda)* [Caso relacionado con las actividades armadas en el territorio del Congo (República Democrática del Congo vs. Uganda)] (Fondo) [2005] CIJ Rep. 168.

– *Case Concerning the Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro)* (Sentencia) [Caso relacionado con la aplicación de la Convención para la prevención y la sanción del crimen de Genocidio (Bosnia y Herzegovina vs. Serbia y Montenegro) (Sentencia)] (2007) CIJ Rep. 43.

– *Plantas de Celulosa sobre el Río Uruguay (Argentina vs. Uruguay)* (Sentencia) [2010] CIJ Rep. 14.

– *Legal Consequences of the Separation of the Chagos Archipelago from Mauritius in 1965* (Opinión consultiva) [Consecuencias jurídicas de la separación del Archipiélago Chagos de Mauricio en 1965] (2019) CIJ Rep. 95.

TPIY, *Prosecutor v Tadić* (Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction) ICTY-94-1-A [Fiscalía vs. Tadić (Decisión de la moción de defensa de apelación interlocutoria sobre la jurisdicción)](2 de octubre de 1995).

– *Prosecutor v Tadić* [Fiscalía vs. Tadić](Sentencia de apelación) IT-94-1-A (15 de julio de 1999).

– *Prosecutor v Tadić* [Fiscalía vs. Tadić](Sentencia del juicio) ICTY-03-66-T (15 de noviembre de 2005).

– *Prosecutor v Boškoski and Tarčulovski* (Sentencia del juicio) ICTY-04-82-T [Fiscalía vs. Boškoski y Tarčulovski] (10 de julio de 2008).

Island of Palmas (US v Netherlands) [Isla de Palmas (Estados Unidos vs. Países Bajos] (1928) II RIAA 829.

Caso Trail Smelter (EE. UU. vs. Canadá) (1941) 3 RIAA 1911.

ANEXO A:
Lista de verificación para desarrollar una posición nacional

Esta lista de verificación ofrece una lista no exhaustiva de consideraciones que pueden ayudar a los Estados en el desarrollo o revisión de una posición nacional sobre la aplicación del derecho internacional a las actividades cibernéticas. Está organizada de acuerdo con la estructura del manual y pretende ser una herramienta de referencia práctica de ayuda para la planificación interna, coordinación y toma de decisiones. No todos los puntos serán relevantes en cada contexto, y puede ser necesario ajustar la secuencia de acuerdo con los requisitos del Estado.

Motivaciones (para más información, consulte el Capítulo 2)

- ☐ Identificar las principales motivaciones para desarrollar una posición nacional.
- ☐ Considerar las funciones para las que la posición debe servir (por ejemplo, comunicativa, transformadora o preventiva).
- ☐ Describir los objetivos respectivos y los resultados esperados de la posición nacional.
- ☐ Identificar los posibles riesgos, limitaciones o sensibilidades, incluidas las relacionadas con divulgación, flexibilidad operacional, capacidad disponible o falta de consenso interno.
- ☐ Decidir si desarrollar o no una posición nacional.
- ☐ Considerar si proceder con una posición pública, parcial o solo interna, y cómo gestionar mejor las omisiones estratégicas, de ser necesario.

Proceso (para más información, consulte el Capítulo 3)

- ☐ Evalúe los aspectos nacionales específicos para ajustar el proceso y el orden de los pasos.
- ☐ Asegure el mandato para iniciar el proceso.
- ☐ Identifique a las partes interesadas relevantes en todo el gobierno y otros sectores.
- ☐ Determine el organismo líder y los mecanismos de coordinación.
- ☐ Nombre uno o más redactores, y, de ser posible, un equipo de redacción multidisciplinario.
- ☐ Desarrolle un plan y cronograma para el proceso que incluya los hitos principales. Considere usar el marco de las 5 preguntas clave *(¿Quién? ¿Qué? ¿Por qué? ¿Cuándo? ¿Dónde? ¿Cómo?).*
- ☐ Identifique las necesidades de creación de capacidades y evalúe cómo se pueden abordar (por ejemplo, mediante alianzas, capacitación o apoyo externo).

- [ ] Consulte a las partes interesadas nacionales e internacionales relevantes, incluidos los organismos y agencias técnicas y operativas, asesores jurídicos y, cuando corresponda, al público general o a la sociedad civil.
- [ ] Lleve a cabo investigaciones de escritorio y reúna materiales de referencia de posiciones nacionales existentes, foros multilaterales, fuentes académicas y documentos internos.
- [ ] Seleccione un enfoque de redacción (deductivo, inductivo o híbrido).
- [ ] Redacte la posición mediante un proceso iterativo, incluyendo la cantidad adecuada de etapas de revisión interna, consolidación y refinamiento.
- [ ] Prepárela para la adopción formal en línea con los requisitos jurídicos y procedimentales nacionales.
- [ ] Planifique las revisiones, actualizaciones o seguimientos futuros con base en los desarrollos de la legislación o política.

Contenido (para más información, consulte el Capítulo 4)

- [ ] Determine el alcance y profundidad deseados del análisis, de acuerdo con los intereses y prioridades nacionales.
- [ ] Consulte posiciones nacionales existentes y otras fuentes relevantes como el Cyber Law Toolkit, el *Proceso de Oxford*, y el *Manual de Tallin 2.0.*
- [ ] Identifique las reglas y principios del derecho internacional que se incluirán (por ejemplo, soberanía, diligencia debida, no intervención y prohibición del uso de la fuerza).
- [ ] Decida si se incluirán perspectivas sobre regímenes especializados del derecho internacional (por ejemplo, el DIH, el derecho internacional de los derechos humanos o el derecho penal internacional).

Formato y difusión (para más información, consulte el Capítulo 5)

- [ ] Elija el formato adecuado (por ejemplo, discurso, presentación en un foro multilateral, artículo académico o documento escrito autónomo).
- [ ] Estructure el documento con claridad y considere usar encabezados, resúmenes y apartados numerados.
- [ ] Determine el tono y nivel de detalles técnicos adecuados para los públicos previstos.
- [ ] Considere incluir escenarios prácticos o ejemplos del mundo real para ilustrar los puntos clave.
- [ ] Revise la consistencia de la terminología y el encuadre en todos los temas.
- [ ] Asegure la accesibilidad, lo que incluye las posibles traducciones a otros idiomas y si resulta correspondiente, el uso de ayudas visuales.
- [ ] Desarrolle una estrategia de difusión, que incluya opciones para el lanzamiento, como un evento público o un anuncio en línea.

ANEXO B:

Lista de posiciones nacionales y conjuntas sobre el derecho internacional y las actividades cibernéticas

Posiciones conjuntas

1. **Unión Africana**
   Posición conjunta de la Unión Africana (2024)
2. **Unión Europea**
   Posición conjunta de la Unión Europea (2024)

Posiciones nacionales

1. **Australia**
   Posición nacional de Australia (2017)
   Posición nacional de Australia (2021)
2. **Austria**
   Posición nacional de Austria (2024)
3. **Brasil**
   Posición nacional de Brasil (2020)
   Posición nacional de Brasil (2021)
4. **Canadá**
   Posición nacional de Canadá (EN) (2022)
   Posición nacional de Canadá (FR) (2022)
5. **China**
   Posición nacional de China (general) (2021)
   Posición nacional de China (soberanía) (2021)
6. **Colombia**
   Posición nacional de Colombia (EN) (2025)
   Posición nacional de Colombia (ES) (2025)
7. **Costa Rica**
   Posición nacional de Costa Rica (2023)
8. **Cuba**
   Posición nacional de Cuba (2024)
9. **República Checa**
   Posición nacional de República Checa (2020)
   Posición nacional de República Checa (2024)
10. **Dinamarca**
    Posición nacional de Dinamarca (2023)
11. **Estonia**
    Posición nacional de Estonia (2019)
    Posición nacional de Estonia (2021)
12. **Finlandia**
    Posición nacional de Finlandia (inglés) (2020)
    Posición nacional de Finlandia (finlandés) (2020)
13. **Francia**
    Posición nacional de Francia (EN) (2019)
    Posición nacional de Francia (FR) (2019)
    Posición nacional de Francia (EN) (2021)

14. **Alemania**
    Posición nacional de Alemania (2021)
15. **Irán**
    Posición nacional de Irán (2020)
16. **Irlanda**
    Posición nacional de Irlanda (2023)
17. **Israel**
    Posición nacional de Israel (2021)
18. **Italia**
    Posición nacional de Italia (2021)
19. **Japón**
    Posición nacional de Japón (2021)
20. **Kazajistán**
    Posición nacional de Kazajistán (2021)
21. **Kenia**
    Posición nacional de Kenia (2021)
22. **Holanda**
    Posición nacional de Países Bajos (2019)
23. **Nueva Zelanda**
    Posición nacional de Nueva Zelanda (2020)
24. **Noruega**
    Posición nacional de Noruega (2021)
25. **Pakistán**
    Posición nacional de Pakistán (2023)
26. **Polonia**
    Posición nacional de Polonia (2022)
27. **Rumania**
    Posición nacional de Rumania (2021)
28. **Rusia**
    Posición nacional de Rusia (2021)
29. **Singapur**
    Posición nacional de Singapur (2021)
30. **Suecia**
    Posición nacional de Suecia (2022)
31. **Suiza**
    Posición nacional de Suiza (2021)
32. **Reino Unido**
    Posición nacional del Reino Unido (2018)
    Posición nacional del Reino Unido (2021)
    Posición nacional del Reino Unido (2022)
33. **Estados Unidos**
    Posición nacional de Estados Unidos (2012)
    Posición nacional de Estados Unidos (2016)
    Posición nacional de Estados Unidos (2020)
    Posición nacional de Estados Unidos (2021)

ANEXO C:
Lista de Estados participantes

1. Argelia
2. Angola
3. Argentina
4. Benín
5. Brasil
6. Burundi
7. Camboya
8. Camerún
9. Canadá
10. Chile
11. Colombia
12. Comoras
13. Congo (República del)
14. Costa de Marfil
15. República Dominicana
16. Egipto
17. El Salvador
18. Estonia
19. Etiopia
20. Gambia
21. Indonesia
22. Japón
23. Kenia
24. Lesoto
25. Malasia
26. Mauritania
27. México
28. Moroco
29. Mozambique
30. Nueva Zelanda
31. Paraguay
32. Perú
33. Filipinas
34. República de Corea
35. República Saharaui
36. Senegal
37. Singapur
38. Sudáfrica
39. Sudán del Sur
40. Tailandia
41. Togo
42. Uganda
43. República Unida de Tanzania
44. Estados Unidos de América
45. Uruguay
46. Zambia

La inclusión en este anexo refleja la participación en las mesas redondas del proyecto y no implica ningún reconocimiento de estatus jurídico. De igual modo, la participación en el proyecto no constituye su respaldo al contenido de este manual.

ANEXO D:
Lista de eventos del proyecto

2024

Lanzamiento del proyecto 'Manual para el desarrollo de una posición nacional sobre el derecho internacional en el ciberespacio: Una guía práctica para los Estados', XVI Conferencia Internacional sobre el Conflicto Cibernético: En el Horizonte (CyCon 2024), 28 de mayo de 2024, Tallin.

Panel: Navegar las dinámicas jurídicas: Perspectivas nacionales sobre el derecho internacional y los potenciales de convergencia', Tercer Simposio Presencial Anual sobre Derecho internacional y cibernético, conflicto futuro: La convergencia del derecho internacional sobre la cibernética y la información, 24 de septiembre de 2024, Washington, D.C.

Mesa redonda sobre el desarrollo de posiciones nacionales sobre el derecho internacional en el ciberespacio: Perspectivas de Latinoamérica y el Caribe, sede de la Organización de Estados Americanos, 25 y 26 de septiembre de 2024, Washington, D.C.

Panel: 'Posiciones nacionales sobre el derecho internacional en el ciberespacio: Desafíos, oportunidades y buenas prácticas', Semana Internacional Cibernética en Singapur, 15 de octubre de 2024, Singapur.

Mesa redonda sobre el desarrollo de posiciones nacionales sobre el derecho internacional en el ciberespacio: Perspectivas de Asia y el Pacífico, Centro de Derecho internacional (CIL), Universidad Nacional de Singapur, 16 de octubre de 2024, Singapur.

Mesa redonda para los Estados miembro de la Unión Africana sobre el desarrollo de una posición nacional sobre el derecho internacional en el ciberespacio, sede de la Unión Africana, 25 y 26 de noviembre de 2024, Addis Ababa.

2025

Lanzamiento del Manual para el desarrollo de una posición nacional sobre el derecho internacional y las actividades cibernéticas: Una guía práctica para los Estados, XVII Conferencia Internacional sobre Conflicto Cibernético: El paso a seguir (CyCon 2025), 29 de mayo de 2025, Tallin.

ISBN 978-9916-9227-0-5

2025HASS007