Responsabilidad internacional del Estado por la comisión de ciberoperaciones: violación de los principios de soberanía y no intervención

International responsibility of the State for cyber-attacks: the principles of sovereignty and non-intervention

Rosa Amilli Guzmán Pérez
Universidad de Monterrey, México
rosa.guzman@udem.edu

Daniela Monserrat Estrada Sáenz
Universidad de Monterrey, México
daniela.estradas@udem.edu

Resumen: La seguridad cibernética concierne todos los ámbitos de regulación del Estado: protección de datos personales, resguardo de información sensible, control de infraestructura privada o pública, operaciones de información, funcionamiento de sistemas informáticos y aplicación de tecnología en general. La mayoría de las ciberoperaciones no manifiestan consecuencias físicas, por lo que no constituyen en términos estrictos un "uso de la fuerza" prohibido en el derecho internacional. Este trabajo analizará en primer lugar la ilicitud de ciberoperaciones como comportamientos contrarios a los principios de soberanía y de no intervención y, en segundo lugar, los criterios de atribución ante las complicaciones que supone la identificación y la persecución de quien ejecuta estos actos.

Palabras clave: CIBEROPERACIONES; SOBERANÍA; INTERVENCIÓN; HECHOS INTERNACIONALMENTE ILÍCITOS.

Abstract: Cybersecurity encompasses all areas of state regulation, including personal data protection, the safeguarding of sensitive information, the control of private and public infrastructure, information operations, the functioning of computer systems, and the application of technology in general. Most

cyberoperations do not have physical consequences and, therefore, do not strictly constitute a "use of force" prohibited under international law. This paper will first analyze the illegality of cyberoperations as conduct that violates the principles of sovereignty and non-intervention and, second, examine the criteria for attribution, considering the challenges involved in identifying and prosecuting those responsible for such acts.

Keywords: CYBEROPERATIONS; SOVEREIGNTY; INTERVENTION; INTERNATIONALLY WRONGFUL ACTS

Fecha de recepción: 01/10/2023
Fecha de aceptación: 02/02/2024
Identificador doi: 10.62169/rg.i34.2449

Revista Electrónica. Instituto de Investigaciones Ambrosio L. Gioja
n° 34, junio – noviembre 2025, Buenos Aires, Argentina, ISSN 1851-3069, pp. 228-256

Responsabilidad internacional del Estado por la comisión de ciberoperaciones: violación de los principios de soberanía y no intervención

Rosa Amilli Guzmán Pérez y Daniela Monserrat Estrada Sáenz

I. Introducción

El Informe de Riesgos Globales 2024 del Foro Económico Mundial considera las fallas en la seguridad cibernética como una de las diez principales amenazas críticas para el mundo, a corto y mediano plazo. El riesgo de sufrir perjuicios por operaciones cibernéticas aumenta a medida que la tecnología invade todos los ámbitos: personal, económico, social, administración de justicia, elecciones, salud pública, servicios. Esto aunado a que los ejecutores de estos actos suelen ser difíciles de identificar y detener. Una persona con acceso a internet y los conocimientos adecuados puede causar daños importantes a otras personas, su información o, incluso, a la infraestructura de una empresa, organización o institución, sin ser detectada.

Es importante diferenciar los términos "ciberataque", "cibercrimen" y "ciberoperaciones", pues se refieren a diferentes conductas que pueden impactar, o no, el ámbito del derecho internacional. Los ciberataques pueden ser definidos como cualquier acción que socava las funciones de una red informática con un propósito político o de seguridad nacional (Hathaway et al., 2012b), estas acciones pueden llegar incluso a calificarse como "ataques armados" o realizarse en un contexto de guerra. Por otro lado, el cibercrimen se refiere a los delitos cometidos en el ciberespacio o con la utilización de herramientas de internet o tecnologías de la información, ya sea que repliquen los delitos ya existentes en el espacio físico o que emerjan como nuevos tipos penales; su calificación dependerá entonces del derecho interno de los Estados (Miró, 2012).

En este trabajo se empleará el término "ciberoperaciones" que comprende un catálogo más amplio de actividades cibernéticas que, además de variado, es cambiante en función de nuevas tecnologías y formas de utilización. Las ciberoperaciones pueden consistir en intrusiones no autorizadas, ataques de denegación de servicio (DoS) – que limitan o evitan que los usuarios accedan a los recursos de la red –, programas maliciosos (malware) como virus, gusanos o troyanos, e incluso Operaciones de Información (Information Operations, IO) que buscan manipular el discurso público o alterar el flujo de información entre individuos y grupos. Estas operaciones pueden tener como objetivo la destrucción o la alteración de datos, la obtención de información, la paralización de empresas o instituciones, entre otros, y pueden dirigirse contra personas o entes privados, o contra Estados.

Las ciberoperaciones pueden tener un impacto importante en las relaciones entre Estados. En julio de 2021 Estados Unidos, Canadá y el Reino Unido acusaron a China de uno de los peores ataques a la seguridad informática del que Microsoft había sido víctima. Aun cuando los responsables del ciberataque fueron identificados como entes privados, se argumentó que habían sido utilizados y financiados por el Ministerio de Seguridad de China, quien negó cualquier vinculación con el ataque. Derivado de estos hechos la Organización del Tratado del Atlántico Norte (OTAN) emitió un comunicado llamando a todos los Estados, incluida China, a respetar sus compromisos y obligaciones internacionales y actuar de manera responsable en el sistema internacional, incluido el ciberespacio (OTAN, 2021).

En el contexto de la guerra entre Rusia y Ucrania, el espacio cibernético se ha vuelto parte del campo de batalla. En febrero de 2022, Estados Unidos acusó a Rusia de los ciberataques que afectaron al sector bancario y al Ministerio de Defensa ucraniano. Anne Neuberger, vice-asesora de Seguridad Nacional de la Casa Blanca para Ciberseguridad y Tecnologías Emergentes, aseguró contar con información técnica que vinculaba esos ataques al servicio de inteligencia militar

ruso, el GRU; esto a través del análisis de dominios de internet y direcciones IP. Ucrania fue blanco del mayor ataque distribuido de denegación de servicio (DDoS) de su historia, afectando al Ministerio de Defensa, a las Fuerzas Armadas y a importantes entidades financieras del país como el Banco Estatal de Ahorros de Ucrania (U.S. Department of State, 2022).

Estas ciberoperaciones pueden ser consideradas hechos internacionalmente ilícitos y, por lo tanto, motivar la reclamación de la responsabilidad de un Estado. De acuerdo con los Artículos sobre Responsabilidad del Estado por Hechos Internacionalmente Ilícitos (AREHII) – elaborados por la Comisión de Derecho Internacional y acogidos por la Asamblea General de las Naciones Unidas en su Resolución 56/83 –, la responsabilidad internacional surge cuando el hecho en cuestión constituye una violación de una obligación internacional y es atribuible a un Estado (AREHII, artículo 2). Estos Artículos serán tomados como referencia a lo largo de este trabajo ya que constituyen una codificación de la práctica estatal en materia de responsabilidad y han sido reconocidos y aplicados por los Estados y por tribunales internacionales, incluida la Corte Internacional de Justicia (Crawford, 2013).

Atendiendo a la ilicitud del hecho, una ciberoperación podría constituir una violación a la prohibición del uso de la fuerza conforme al artículo 2(4) de la Carta de las Naciones Unidas, que comprende cualquier uso de la fuerza, independientemente del arma o medio de guerra empleados (“Legalidad de la amenaza o el uso de armas nucleares”, 1996). El uso de la fuerza supone la existencia de un ataque armado, lo que implicaría asimilar la ciberoperación a las armas tradicionales; esto requiere la penetración en sistemas de infraestructura nacional crítica y el análisis de sus consecuencias físicas, como la destrucción o la muerte de personas (Delerue, 2020c).

Sin embargo, la mayoría de las ciberoperaciones de los Estados tienen lugar por debajo del umbral del uso de la fuerza (Moynihan, 2019), ya que sus consecuencias no se manifiestan de manera física, asimilables a un ataque

convencional. Incluso, como puede observarse en el ataque a Microsoft, pueden estar dirigidas contra empresas o servicios particulares, ajenos a las instituciones o servicios propios del Estado. El Manual de Tallin 2.0 – elaborado por iniciativa de la Organización del Tratado del Atlántico Norte (OTAN) – aborda estas actividades de manera limitada debido a la falta de consenso en cuanto a su calificación como hechos internacionalmente ilícitos. Además, si bien es un texto de gran influencia que pretende reflejar el derecho internacional existente al momento de su elaboración, no es un instrumento vinculante, ni prueba del desarrollo progresivo del derecho internacional. Este trabajo de investigación abordará entonces la responsabilidad del Estado derivada de operaciones cibernéticas que, aún teniendo un bajo grado de severidad, podrían calificarse como hechos internacionalmente ilícitos.

Un hecho es internacionalmente ilícito cuando constituye la violación de una obligación internacional; es decir, una obligación que se desprende de las fuentes formales del derecho internacional – tratados internacionales, costumbre o principios – o de otras con carácter obligatorio de forma particular – como las decisiones judiciales o los actos unilaterales –. Considerando la exclusión del estudio de la prohibición del uso de la fuerza, el primer análisis recaerá en la ilicitud de estas operaciones como comportamientos contrarios a los principios de soberanía y de no intervención.

Además de la acreditación del hecho como internacionalmente ilícito, para que surja la responsabilidad internacional, el comportamiento debe ser atribuible a un Estado. La atribución no es evidente si se considera, desde el punto de vista jurídico, la rigidez del derecho internacional y, desde el punto de vista técnico, las complicaciones que supone la identificación y la persecución de quien ejecuta la operación cibernética, especialmente si se trata de actores no estatales. Así pues, este trabajo abordará en una segunda sección los criterios para la atribución de un hecho al Estado y su eficacia en el contexto cibernético.

II. La ilicitud de las ciberoperaciones: violación al principio de soberanía y de no intervención

II.1. La violación de la soberanía territorial por medio de ciberoperaciones

Se entiende por soberanía estatal, en su dimensión interna, el control completo y exclusivo del Estado sobre las personas y propiedades dentro de su territorio; en su dimensión externa, el poder de actuar en un plano de igualdad frente a otros Estados en la esfera internacional (Crawford, 2019). El artículo 2(1) de la Carta de las Naciones Unidas reconoce el principio de igualdad soberana de todos los miembros de la organización. Asimismo, la Declaración sobre los principios de derecho internacional referentes a las relaciones de amistad y a la cooperación, adoptada en 1970 por la Asamblea General de las Naciones Unidas en su resolución 2625, establece que los Estados gozan de los derechos inherentes a la plena soberanía, y de la inviolabilidad de su integridad territorial e independencia política. Por su parte, la Corte Internacional de Justicia ha reconocido tanto el origen convencional como consuetudinario del principio de soberanía (Actividades Militares y Paramilitares (Nicaragua v. Estados Unidos de América), 1986; Lotus (Francia v. Turquía), 1927, Ciertas Actividades Realizadas por Nicaragua en la Zona Fronteriza, (Costa Rica v. Nicaragua), 2018), así como su carácter fundacional en el derecho internacional, en casos como Corfu Channel (Reino Unido de Gran Bretaña e Irlanda del Norte v. Albania, 1949), así como en la Opinión Consultiva del 22 de julio de 2010 sobre la conformidad con el derecho internacional de la declaración unilateral de independencia de Kosovo.

Si bien la soberanía tiene una dimensión territorial que dificulta su delimitación en el ciberespacio, el Grupo de Expertos encargado de la elaboración del Manual de Tallin 2.0 concluyó que el ciberespacio y las operaciones cibernéticas del Estado no están fuera del alcance de este principio; su componente territorial permite vincular el poder estatal a infraestructuras, personas o actividades, así como a las restricciones de la actividad estatal en este ámbito

(Manual de Tallin 2.0, 2017, Regla 1). En su dimensión interna, la soberanía implica la autoridad soberana de un Estado con respecto a la infraestructura cibernética, así como a las personas y actividades cibernéticas ubicadas dentro de su territorio (Manual de Tallin 2.0, 2017, Regla 2); otorga al Estado el derecho – y en algunos casos la obligación – de regular y controlar las actividades cibernéticas y la infraestructura en su territorio (Schmitt, 2014). En su dimensión externa, se refiere a las actividades cibernéticas del Estado en sus relaciones internacionales, con los límites de las normas vinculantes de derecho internacional (Manual de Tallin 2.0, 2017, Regla 3), que en general prohíben la injerencia no consensuada de los Estados en la integridad de la infraestructura cibernética de otros (Watts y Theodore, 2018).

El ciberespacio es un dominio global dentro del entorno de la información que consta de redes interdependientes de infraestructuras de tecnología de la información y datos, incluidos el Internet, redes de telecomunicaciones, sistemas informáticos, procesadores y controladores integrados (Delerue, 2020b). Si bien el ciberespacio es un territorio ficticio, se basa en infraestructuras reales y tangibles; por ende, las redes informáticas y sus componentes, que constituyen la arquitectura física del ciberespacio e Internet, son reales y se encuentran dentro de la soberanía territorial de los Estados (Delerue, 2020b). Las normas y principios del derecho internacional son aplicables a la conducta de los Estados en materia de las tecnologías de la información y de la comunicación, incluyendo las infraestructuras en su territorio (Delerue, 2020b).

En la mayoría de los casos, el simple hecho de ingresar a un área bajo soberanía territorial, sin autorización previa, se considera una violación; no es necesario que ocurra un acto o daño especifico (Delerue, 2020b; Fraser, 2016; Actividades Militares y Paramilitares (Nicaragua v. Estados Unidos de América), 1986). Esto es particularmente importante en el contexto cibernético, donde el cruce de la frontera de un Estado, por vía electrónica, es difícil de comparar con el cruce físico (Fraser, 2016). La Regla 4 del Manual de Tallin 2.0 establece que un

Estado no debe realizar operaciones cibernéticas que violen la soberanía de otro Estado; sin embargo, no resuelve una zona gris importante en el derecho internacional del ciberespacio: el grado de interferencia que configuraría una violación de la soberanía, así como el método por el cual se debe medir tal interferencia en el ciberespacio. En este sentido, Chircop (2019) enuncia cuatro enfoques predominantes de la soberanía territorial en el ciberespacio: el enfoque de daño material, los enfoques intermedios que consideran las operaciones cibernéticas moderadamente severas, el de inviolabilidad estricta y, por último, el que establece que todas las intrusiones en la infraestructura cibernética de otro Estado constituyen una violación de la soberanía territorial.

En el enfoque de daño material, solo las operaciones cibernéticas que causen una pérdida permanente de funcionalidad a la infraestructura cibernética o que resulten en daños físicos o lesiones se consideran violaciones de la soberanía territorial (Chircop, 2019; Kosik, 2015). Stuxnet es un claro ejemplo de este tipo de operación; este "gusano" – el primero en conocerse públicamente –, apuntó a la afectación de sistemas de control industrial, con el claro objetivo de sabotear plantas industriales del mundo tangible, más allá de sólo interrumpir sistemas tecnológicos abstractos (Piggin, 2010). Estados Unidos e Israel fueron acusados de haber implantado Stuxnet en la planta nuclear de Natanz en Irán; el "gusano" reprogramó las centrifugadoras cambiando su velocidad, lo que provocó finalmente que quedaran fuera de servicio (International Business Times [U.S. ed.], 2013). La implantación de Stuxnet ha sido incluso discutida como una violación a la prohibición del uso de la fuerza conforme al artículo 2(4) de la Carta de las Naciones Unidas, debido a sus consecuencias materiales (Moore, 2015).

A diferencia de este enfoque, el segundo considera que ciberoperaciones moderadamente severas pueden constituir una violación a la soberanía territorial de un Estado, debido a que el objeto y fin de este principio es garantizar el control absoluto del Estado en su territorio y actividades. Las violaciones a la soberanía pueden entonces configurarse a través de operaciones que alteren el

funcionamiento de infraestructura o de programas cibernéticos; la introducción de malware, la manipulación o supresión de datos almacenados, la instalación de puertas traseras y la pérdida de funcionalidad temporal, pero significativa (Chircop, 2019). Sin embargo, la oscuridad en cuanto a la definición del nivel de interferencia y de lo que debe entenderse por "pérdida de control" del Estado, dificulta la calificación de una ciberoperación como hecho internacionalmente ilícito.

El enfoque de inviolabilidad estricta establece que todas las operaciones que interfieren con infraestructura cibernética de un Estado violan la soberanía territorial, siempre que causen más que los efectos de minimis (Chircop, 2019). Esto implica por un lado, la acreditación de una interferencia en la infraestructura – lo que excluye, por ejemplo, las operaciones de ciberespionaje – y, por otro, que los daños, si bien pueden ser inmateriales, no sean tan menores o intangibles que no ameriten la atención del derecho internacional (Chircop, 2019). Si bien se trata de un criterio más amplio que los anteriores, no resuelve la ambigüedad de lo que debería considerarse violatorio de la soberanía en función de la gravedad de sus efectos.

El último enfoque considera que absolutamente todas las intrusiones en la infraestructura cibernética de otro Estado constituyen una violación de la soberanía territorial (Schmitt y Vihul, 2017). Esto descarta el análisis del nivel de interferencia, la consideración de la infraestructura blanco del ataque, o la cuantificación del daño. En este sentido, incluso las operaciones dirigidas contra personas o entidades privadas – y no directamente contra el Estado y sus instituciones o servicios – constituirían una violación al principio de soberanía, considerando que se estaría entrando en el espacio cibernético que corresponde a un Estado determinado.

El Grupo Internacional de Expertos encargado del Manual de Tallin 2.0 (2017), evaluó la legalidad de las ciberoperaciones considerando dos criterios: (1) el grado de violación de la integridad territorial del Estado objetivo; y (2) la

interferencia o usurpación de funciones inherentes al Estado. En cuanto al análisis del primero, el Grupo de Expertos consideró tres niveles: (1) daño físico; (2) pérdida de funcionalidad; y (3) infracción de la integridad territorial por debajo del umbral de pérdida de funcionalidad. La presencia de daños físicos permite, sin duda, constatar la comisión de un hecho internacionalmente ilícito ya sea la violación de la soberanía, del principio de no intervención o, incluso, de la prohibición del uso de la fuerza. Los Estados concuerdan, en general, que una conducta estatal que produce daño a nivel físico sería contraria al derecho internacional; sin embargo, no existe consenso en cuanto a los otros dos niveles: el grado de pérdida de funcionalidad o los casos inferiores al umbral de esa pérdida que puedan considerarse transgresiones a la integridad territorial (Chircop, 2019).

En cuanto al segundo criterio para la evaluación de legalidad de las ciberoperaciones, se considera que cuando éstas interfieren con datos o servicios necesarios para el ejercicio de funciones inherentes al Estado, se está frente a una violación del principio de soberanía, incluso si se trata de un servicio prestado por el sector privado (Manual de Tallin 2.0, 2017). Por ejemplo, la interferencia con datos o sistemas necesarios para la operación de servicios públicos, elecciones populares, recolección de impuestos o acciones de defensa.

El Manual de Tallin 2.0 descarta los ataques dirigidos contra entidades privadas, no relacionados con las funciones inherentes del Estado, pero que podrían causar un menoscabo importante como pérdida de información personal o afectaciones a un sector económico. Asimismo, excluye como violación de la soberanía el ciberespionaje en tiempos de paz, a menos que los medios para efectuarlo impliquen una violación territorial – por ejemplo, mediante la intervención de servidores o equipos de cómputo – o cuando de manera accidental o intencional se ocasionen daños materiales. La violación del principio de soberanía en lo que el Grupo de Expertos consideró como lex lata se vincula principalmente a la noción territorial y a la materialización de consecuencias tangibles como el daño físico o la pérdida o alteración de información; incluso, esas

consecuencias pueden ser insuficientes si se considera el nivel de gravedad de los daños o pérdidas, o un campo de la interferencia al margen de las funciones inherentes al Estado.

II.2. Ciberoperaciones como violación del principio de no intervención

El principio de soberanía es el fundamento de otras normas primarias como la prohibición de la intervención (Actividades Militares y Paramilitares (Nicaragua v. Estados Unidos de América), 1986). El artículo 2(7) de la Carta de las Naciones Unidas reconoce que hay "asuntos que son esencialmente de la jurisdicción interna de los Estados"; asimismo, la Declaración sobre los principios de derecho internacional referentes a las relaciones de amistad y a la cooperación (Asamblea General de las Naciones Unidas, 1970), establece en relación al principio de igualdad soberana de los Estados, el derecho de decidir libremente sobre su sistema político, social, económico y cultural.

La intervención se entiende como la injerencia en los asuntos de otro Estado con el fin de mantener o alterar el estado actual de las cosas (Buchan y Nicholas, 2017). Es decir, denota el despojo de la soberanía de un Estado, limitando su autoridad en relación con asuntos que caen bajo sus prerrogativas soberanas, o desplazando su autoridad. Bajo un criterio estricto, una interferencia extranjera puede ser calificada como intervención ilegal cuando incide en asuntos en los que cada Estado tiene permitido decidir libremente (su sistema político, económico, social y cultural, así como la formulación de su política exterior) e involucra métodos de coerción con respecto a tales decisiones (Actividades Militares y Paramilitares (Nicaragua v. Estados Unidos de América, 1986).

Los derechos soberanos pueden ser definidos a través del concepto de *domaine réservé* que engloba en la esfera exclusiva del Estado, las cuestiones que no son reguladas por el derecho internacional. Se trata de una noción relativa ya que el derecho internacional es variable y, por lo tanto, lo que anteriormente podía considerarse *domaine réservé*, ahora podría no serlo, favoreciendo la intervención

legal en áreas actualmente reguladas por el derecho internacional (Moulin, 2020). Este concepto resulta inadecuado para abordar las ciberoperaciones; las comunicaciones son un ámbito comprendido, al menos en parte, por instrumentos internacionales como la Constitución de la Unión Internacional de Telecomunicaciones, su Convenio y sus reglamentos administrativos: el Reglamento de las Telecomunicaciones Internacionales y el Reglamento de Radiocomunicaciones.

Considerando la intervención como un concepto elástico que describe formas de interferencia coercitiva en las prerrogativas soberanas de un Estado (Buchan y Nicholas, 2017), resulta más apropiada la noción de *domaine privilégié.* El *domaine privilégié* protege los intereses fundamentales de un Estado y su población (Moulin, 2020); incluye no sólo los elementos necesarios para la propia supervivencia de un Estado, sino también los esenciales para su independencia, autonomía y estabilidad. De acuerdo con Moulin (2020), debe entenderse que se está frente a intervenciones prohibidas siempre que un Estado sea privado del control sobre asuntos comprendidos en el dominio privilegiado, debido a la acción deliberada de otro Estado. Así pues, la prohibición de la intervención puede extenderse a las operaciones cibernéticas dirigidas incluso contra actores privados, que sean vitales para el sistema económico, social o cultural de un Estado (Moulin, 2020). La capacidad para salvaguardar los aspectos esenciales de su condición de Estado, dependen no solo del control de sus fronteras o espacios territoriales, sino también del control de su economía y fuentes privadas de riqueza (Skinner, 2014).

Por otro lado, si bien la existencia de la prohibición de la intervención y su estatus como regla del derecho internacional consuetudinario no es controvertida, su contenido exacto está lejos de ser obvio (Helal, 2019). Una definición excesivamente limitada de intervención corre el riesgo de permitir políticas coercitivas que socaven la independencia política de los Estados o menoscaben el derecho a la autodeterminación; mientras que una definición irracionalmente

amplia podría prohibir formas legítimas de presión que los Estados ejercen en la búsqueda de sus intereses o los de la comunidad internacional en general (Helal, 2019).

La Regla 66 del Manual de Tallin 2.0 sobre el Derecho Internacional Aplicable a las Operaciones Cibernéticas, menciona que un Estado no puede intervenir de manera coercitiva, incluso por medios cibernéticos, en los asuntos internos y externos de otro. De ahí se desprende que no todo acto de interferencia viola el principio de no intervención; una intervención será ilícita cuando se componga de tres elementos: (1) un acto realizado por un Estado en contra de otro, (2) con el fin de coaccionar a este último (3) sobre su capacidad de decidir libremente (Delerue, 2020b).

Las operaciones cibernéticas pueden ser utilizadas con el propósito de subordinar el ejercicio de los derechos soberanos de un Estado u obtener ventajas de algún tipo (Delerue, 2020b; Haataja, 2017). Por ejemplo, en 2007 Estonia se convirtió en el primer Estado sujeto a ataques distribuidos de denegación de servicio (DDoS) a gran escala. Estonia había decidido trasladar una estatua conmemorativa de guerra del centro de Tallin a un cementerio militar cercano, lo que provocó el descontento de los rusos étnicos de Estonia y sus seguidores en Rusia, resultando en protestas, disturbios y múltiples ataques cibernéticos que duraron en total más de tres semanas (Haataja, 2017). Algunos de los ataques fueron rastreados a direcciones de Protocolo de Internet (IP) rusas, por lo que inicialmente Estonia culpó a Rusia e incluso afirmó que su soberanía estaba bajo ataque. Sin embargo, Rusia negó su participación y el incidente se trató como un caso penal doméstico (Haataja, 2017). De haberse confirmado el control o la participación directa de Rusia en tales operaciones cibernéticas, se habría acreditado una intervención ilícita. Esto debido a la gravedad, la duración de los ataques cibernéticos – que afectaron la actividad económica, tanto en el sector público como en el privado – y la coerción intencional contra el gobierno de

Estonia, ya que se buscaba forzarlo a revertir su política de reubicar la estatua del Soldado de Bronce (Buchan, 2017).

La violación del principio de no intervención se distingue entonces de otras violaciones de la soberanía, por la presencia del elemento coercitivo (Moynihan, 2019). La coerción implica un elemento de presión o compulsión por parte del Estado coaccionador, pues sin este requisito la línea entre la coerción y los meros intentos de influencia se volvería ambigua (Moynihan, 2019); se refiere a un acto afirmativo diseñado para privar a otro Estado de su libertad de elección (Banks, 2021). Por ejemplo, el ciberespionaje por sí mismo podría constituir una violación al principio de soberanía, pero no al principio de no intervención.

El motivo del Estado que interviene es de poca relevancia, basta acreditar el comportamiento coercitivo con respecto al libre albedrío del Estado víctima sobre sus funciones soberanas (Watts, 2015). La coerción tampoco es un enfoque basado en resultados; si el uso de medidas coercitivas tuvo éxito o no, no tiene importancia (Moulin, 2020). En el contexto cibernético, el comportamiento coercitivo del Estado ejecutor suele ser encubierto, por lo que surge la pregunta de si el Estado víctima necesita saber que está siendo coaccionado para que se establezca este elemento (Moynihan, 2019). Considerando que el simple hecho de la conducta coercitiva del Estado es lo que establece la coacción, y que la coacción no tiene que ser exitosa para ser ilícita, se puede concluir que no es necesario que el Estado víctima sea consciente de la coacción (Moynihan, 2019).

Sin embargo, el grado de presión que se requiere para privar del control de sus funciones a un Estado, no es fácilmente cuantificable ya que varía según los hechos. Si la presión puede resistirse de manera razonable, la voluntad soberana del Estado objetivo no se considera subordinada y, por lo tanto, no se materializa la intervención (Moynihan, 2019). Esto es relevante en el caso de las llamadas Operaciones de Información (OI) que buscan manipular el discurso público o alterar el flujo de información entre individuos y grupos (Uyheng, J., Cruickshank, I.J. y Carley, K.M., 2022). Una OI con el propósito de influenciar la elección

democrática de un Estado constituye una violación al principio de no intervención en función del grado de presión o coerción ejercidos (van Benthem, T., Dias, T., y Hollis, D. B., 2022).

III. La atribución de responsabilidad internacional al Estado derivada de ciberoperaciones

III.1. Criterios para la atribución de responsabilidad al Estado por ciberoperaciones realizadas por actores no estatales

La segunda condición esencial para que se configure la responsabilidad internacional, es que el comportamiento ilícito pueda adjudicarse a un Estado. En este sentido, las operaciones cibernéticas representan un desafío considerando, por un lado, los aspectos técnicos que permitirían localizar el origen de la operación, y por otro, la identificación de quien realiza el ataque como órgano u agente de un Estado.

El supuesto más evidente de la atribución es el del comportamiento de los órganos del Estado en cualquiera de sus funciones – legislativa, ejecutiva, judicial – y en cualquier nivel según su organización territorial – local, regional, federal, central – (AREHII, art. 4). El comportamiento de los particulares no es, por sí solo, atribuible a un Estado, en especial si no se trata del comportamiento de personas o entidades, facultadas por el derecho doméstico para ejercer atribuciones del poder público (AREHII, art. 5), o el de personas en ausencia o defecto de las autoridades estatales (AREHII, art. 9).

Un acto estatal se materializa a través de la actividad de los individuos, que la norma imputa al Estado, debiendo incluir aquellas conductas que un Estado no querría realizar directamente a través de sus propios órganos, pues de lo contrario, los Estados podrían eludir la responsabilidad subcontratando grupos privados o individuos (Mačák, 2016). En este sentido, se ha desarrollado una doctrina para responsabilizar a los Estados por hechos internacionalmente ilícitos

de sus socios actores no estatales (AREHII con comentarios, art. 8; Actividades Militares y Paramilitares (Nicaragua v. Estados Unidos de América), 1986; Tadić, 1997).

En el caso de las ciberoperaciones, éstas pueden ser conducidas por una o varias personas, en uno o varios Estados, con o sin autorización de éstos (Delerue, 2020a). La función legal de la atribución es considerar si la conducta de una persona física o entidad tiene una dimensión pública que es idéntica a un acto de Estado, usando alguno de los estándares de atribución existentes (Tanyildizi, 2017). De acuerdo con Levite (2022), en el contexto cibernético, los esfuerzos de atribución se abordan desde tres perspectivas distintas: la técnica, la política y la legal. Desde el punto de vista técnico, el Estado debe comprender lo que sucedió y rastrear las actividades cibernéticas maliciosas hasta un dispositivo o ubicación (Levite, 2022). Una vez que se haya alcanzado un cierto nivel de certeza en cuanto al origen de la operación cibernética, Levite (2022) afirma que el Estado deberá tomar la decisión política de cómo, cuándo y de qué forma responsabilizar al actor. Por último, desde una perspectiva jurídica, la atribución permitirá vincular la violación de una obligación internacional, con el Estado ofensor, y legitimar medidas de respuesta del Estado lesionado, como la legítima defensa o la aplicación de contramedidas, según la naturaleza y la gravedad de las operaciones cibernéticas (Levite, 2022).

El artículo 8 de los Artículos sobre la Responsabilidad del Estado considera como hecho atribuible al Estado "el comportamiento de una persona o de un grupo de personas si esa persona o ese grupo de personas actúa de hecho por instrucciones o bajo la dirección o el control de ese Estado al observar ese comportamiento". Así pues, establece tres criterios autónomos para la atribución de la responsabilidad por la conducta de actores no estatales: la instrucción, la dirección y el control. Si el vínculo real entre el Estado y un actor no estatal no cumple con los criterios de atribución, el Estado no será responsable de los hechos en cuestión. Por otra parte, si dicha relación supera estos requisitos y se acredita

una dependencia total del ente privado al Estado, el primero será considerado como un órgano de facto del segundo. Es decir, se consideraría como comportamiento de un órgano del Estado, ya que un órgano de facto es una persona o entidad asimilada o absorbida por la estructura del mismo (Stokes, 2014).

Bajo el primero de los criterios – la instrucción – el Estado decide realizar el hecho ilícito, pero no lo hace por medio de sus órganos, sino que da instrucciones a una entidad no estatal para que actúe en su lugar, sin que tal entidad haya sido facultada por la legislación doméstica para efectuar actos del poder público (Mačák, 2016). Los órganos estatales complementan su propia acción reclutando a personas o grupos privados que actúan como "auxiliares" mientras permanecen fuera de la estructura oficial del Estado (AREHII con comentarios, art. 8). Este criterio implica corroborar la aceptación de las instrucciones y la posterior actuación conforme a ellas. Sin embargo, las instrucciones no requieren un alto grado de especificidad; en el caso de instrucciones ambiguas o generales, los actos incidentales, accesorios a la encomienda, serán atribuidos al Estado (Crawford, 2013). En este sentido, una ciberoperación instruida de manera general por un Estado contra otro, sin especificar los medios o métodos a utilizar, sería atribuible al Estado en su totalidad.

En cuanto al criterio de dirección, para Mačák (2016) éste implica guiar la conducta de los actores no estatales, pudiendo incurrir en responsabilidad por actos individuales incluso en ausencia de instrucciones expresas para cometer esos actos. En el contexto cibernético, el ejemplo del caso Stuxnet es relevante para el criterio de dirección que atribuye responsabilidad a los Estados por actos de actores no estatales. En un análisis realizado por el Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN, se concluyó que la complejidad y la cantidad de recursos requeridos para este tipo de operación cibernética, sugerían la participación directa o el apoyo de Estados (De Falco, 2012). Partes de este proyecto fueron "contratadas a una serie de organizaciones involucradas en delitos

cibernéticos"; si bien no puede constatarse una instrucción general, la conducta de los actores no estatales se inscribe en una relación continua de subordinación que encuadra bajo la noción de dirección (Mačák, 2016).

El tercer criterio – de control – ha sido objeto de distintas interpretaciones en cuanto al grado de control que debe acreditarse para atribuir a un Estado la conducta privada. Una de las interpretaciones más aceptadas en el derecho internacional es la del "control efectivo" propuesto en el caso Actividades Militares y Paramilitares (Nicaragua v. Estados Unidos de América), que exige un alto grado de dependencia de los actores no estatales para su equiparación a órganos del Estado. En las situaciones en las que un particular realiza actos ilegales, se requiere demostrar que el Estado de control emitió instrucciones específicas para ese acto en particular contrario al derecho internacional, lo que coloca al individuo en una capacidad de facto (Tanyildizi, 2017). El Estado debe estar en capacidad de controlar la operación en sus diferentes etapas: planeación, elección de objetivos, desarrollo, métodos y medios (Mačák, 2016). Una autoridad genérica sobre el individuo no sería suficiente para atribuir la responsabilidad internacional de un Estado. En el contexto cibernético, en el que la evidencia es difícil de recabar, la aplicación de este estándar haría prácticamente imposible la atribución de responsabilidad a un Estado.

Así pues, el criterio del control efectivo puede considerarse contrario a la lógica del derecho internacional sobre responsabilidad ya que el fundamento de estas normas es impedir que los Estados eludan su responsabilidad internacional haciendo que particulares lleven a cabo tareas que no pueden o no deben ser realizadas por funcionarios del Estado (Tadić, 1999). Los Estados no pueden actuar de facto a través de individuos y desvincularse de dicha conducta. El criterio de "control general" propuesto en el caso Tadić (1999) considera que el grado de control puede variar según las circunstancias de hecho de cada caso.

El control general de un Estado puede acreditarse cuando tiene un papel en la organización, coordinación o planificación de las acciones militares del grupo

militar, además de financiar, entrenar y equipar o brindar apoyo operativo a ese grupo (Tadić, 1999). Este estándar considera dos condiciones para la acreditación del control: asistencia – que el Estado proporcione al actor no estatal asistencia financiera y de capacitación, equipo militar y/o apoyo operativo –, y organización o coordinación de las operaciones de la entidad (Mačák, 2016). Un Estado que ejerce un control general sobre un grupo, coordinando o ayudando en la planificación general de su actividad, puede ser entonces considerado internacionalmente responsable por cualquier conducta indebida del grupo (Tanyildizi, 2017).

III.2. Eficacia de los criterios para la determinación de atribución de responsabilidad al Estado por actos de actores no estatales

Como quedó establecido en la sección anterior, para determinar la atribución de la responsabilidad del Estado por conductas de actores no estatales, se debe demostrar la instrucción, dirección o control sobre éstos. Sin embargo, estos criterios siguen dejando una brecha en la rendición de cuentas debido a las dificultades para su acreditación en tribunales internacionales (Hathaway et al., 2012a). Este problema se magnifica en el ciberespacio por la velocidad, el anonimato y complejidades técnicas de los ataques cibernéticos, dificultando la distinción entre las acciones de criminales y las de Estados.

La doctrina del control efectivo reconoce el control de un Estado sobre actores no estatales sólo si estos últimos actúan en total dependencia del Estado, "más allá de toda duda", eliminando un estándar de duda razonable (Shackelford, 2010). En el contexto cibernético, la acreditación de ese nivel de control y, por lo tanto, la atribución de responsabilidad al Estado se ve obstaculizada por los atacantes, que ocultan deliberadamente sus identidades. Incluso con los avances tecnológicos recientes, identificar los dispositivos o las direcciones IP responsables de un ataque es difícil, lento y costoso (Banks, 2021). En una operación cibernética global sofisticada, datos faltantes o corruptos pueden ser suficientes para refutar el control del Estado e impedir la rendición de cuentas (Shackelford, 2010).

La ciencia de rastrear ataques cibernéticos requiere de un mayor desarrollo; la base actual de las comunicaciones de red en el ciberespacio – el protocolo de control de transmisión (TCP) y el protocolo de internet (IP) – se remonta a 1982 (Shackelford, 2010). Las amenazas en el ciberespacio superan sus parámetros de diseño, sin mencionar las innumerables estrategias empleadas para dificultar el seguimiento, como la tunelización, la destrucción del registro de datos o el encubrimiento de la dirección de origen (Lipson, 2002).

Incluso si la dirección IP puede ser identificada, esto no garantiza la atribución de la operación cibernética a un Estado. Por ejemplo, los ataques distribuidos de denegación de servicio (DDoS) son operaciones en las que un gran número de máquinas o "red de bots", atacan un sitio o un conjunto de sitios con el objetivo de interrumpir el servicio al sobrecargar un servidor; están diseñados para ser detectados, por lo que tienen el carácter único de ser visibles e intrusivos (Clark y Landau, 2011). Este tipo de ataque, dirigido contra Estonia en 2007, aun cuando fue rastreado a direcciones IP rusas, no fue atribuido al Estado ya que su participación no podía ser demostrada.

A diferencia del control efectivo, la aplicación de un criterio de control general – que comprenda la coordinación o la ayuda en la planificación de un hecho ilícito – sería más adecuada para acreditar la responsabilidad internacional de un Estado (Tanyildizi, 2017). Al ir más allá del marco rígido del criterio de control efectivo, permitiría responsabilizar a los patrocinadores estatales de ataques cibernéticos cuando exista evidencia significativa de su participación (Shackelford, 2010). Sin embargo, si bien un estándar más flexible puede favorecer una mayor ciberseguridad internacional, su adopción es cuestionable ya que se incrementa el riesgo de acusaciones infundadas contra un Estado por motivos meramente políticos (Payne y Finlay, 2017). Algunos Estados prefieren la mayor carga de prueba consagrada en el criterio de control efectivo, aun cuando el criterio de control general exija la acreditación de la participación del Estado "más allá de una duda razonable" (Shackelford, 2010).

Debido a que los criterios tradicionales no parecen ser adecuados al dominio cibernético, surge un estándar alternativo denominado "criterio de control virtual" (Payne y Finlay, 2017). Dicho criterio atribuye la carga de la prueba al Estado que financia, equipa o brinda refugio a una entidad privada que posteriormente se involucra en una operación cibernética contra otro Estado (Margulies, 2013). En este sentido, se crea una presunción de vínculo entre el Estado y el actor privado, que deberá ser desvirtuada por el Estado; la carga de la prueba se atribuye a la parte con mayor acceso a la información, que deberá probar su inocencia (Levite et al., 2022). La información producida por el Estado bajo este criterio puede mostrar que no estaba involucrado en la ciberoperación, o que no pudo controlar al actor no estatal.

Este criterio alienta a los Estados a monitorear y controlar las actividades cibernéticas que se despliegan desde su infraestructura (Margulies, 2013). Bajo este criterio, se requiere una indicación prima facie que vincule el Estado acusado con el actor no estatal; sin embargo, no se precisan las condiciones jurídicas para la atribución de la carga de la prueba. Por ejemplo, cuál es la carga de producción del Estado acusado, o qué nivel de mens rea es requerido para desencadenar esa carga (Delbert, 2018). Además, se deben considerar las posibles violaciones a la privacidad, ya que los Estados tendrían un incentivo para monitorear las comunicaciones privadas de sus ciudadanos en mayor medida y así cumplir eventualmente con la carga de la prueba (Margulies, 2013). Estas preocupaciones pueden ser exageradas si se considera que la vigilancia estaría limitada a las entidades privadas que reciben apoyo material o financiero del Estado, acreditando la vinculación prima facie (Margulies, 2013; Delbert, 2018).

Otra oposición al criterio de control virtual es la posibilidad de contribuir a la escalada del conflicto debido a que el Estado víctima podría aplicar medidas defensivas en contra del Estado que se presume como agresor (Margulies, 2013). Sin embargo, el derecho internacional limita las respuestas de un Estado víctima imponiendo condiciones sumamente restrictivas – como en el caso de las

contramedidas o la legítima defensa –. Al contrario, el criterio de control virtual puede contribuir a la disminución de conflictos derivados de ciberoperaciones ejecutadas por actores no estatales al promover que los Estados vigilen o renuncien a cualquier relación que puedan establecer con estos grupos (Delbert, 2018).

Finalmente, el deber de cuidado o de prevención que se desprende del criterio de control virtual es consistente con el principio de debida diligencia; los Estados deben ejercer la debida diligencia para garantizar que el territorio y los objetos sobre los que gozan de soberanía no se utilicen para dañar a otros Estados (Corfu Channel (Reino Unido de Gran Bretaña e Irlanda del Norte v. Albania), 1949). Este principio se extiende a las operaciones cibernéticas realizadas por actores no estatales que, si bien no violan el derecho internacional per se, pueden tener consecuencias adversas graves y afectar los derechos del Estado objetivo (Manual de Tallin 2.0., Regla 6). Esto responde al creciente peligro que los actores no estatales representan para los Estados, particularmente en el campo de las ciberoperaciones.

IV. Conclusiones

En la actualidad, las operaciones cibernéticas impactan todos los ámbitos de competencia de un Estado; desde el campo regulatorio de la actividad privada (protección de la información, prevención, persecución y sanción del cibercrimen), hasta el dominio de lo público (elecciones populares, seguridad pública y nacional, prestación de servicios públicos). En este sentido, una operación cibernética puede tener efectos devastadores, aun cuando no cause daños físicos.

En el derecho internacional, cuando un Estado es responsable de la comisión de un hecho internacionalmente ilícito, tiene la obligación de reparar al Estado lesionado y, además, de ofrecer garantías y seguridades para que el hecho no se repita. Por su parte, el Estado lesionado podría emplear un medio de respuesta,

como la legítima defensa, o imponer contramedidas para inducir el cumplimiento de la obligación internacional violada.

En el contexto cibernético, la asignación de responsabilidad internacional se dificulta en sus dos componentes: la calificación del hecho como internacionalmente ilícito y su atribución como comportamiento de un Estado. En cuanto al primer elemento, se analizaron los principios de soberanía y de no intervención. El ciberespacio, aun siendo un territorio intangible, goza de una arquitectura física que pertenece al dominio de un Estado e incide en el campo de sus funciones soberanas.

Si bien no puede constatarse un consenso que extienda el campo de aplicación de la soberanía estatal a la generalidad del ciberespacio, no puede negarse que el derecho internacional debe adaptarse a las cada vez más recurrentes operaciones cibernéticas conducidas por Estados, de manera directa, o por medio de actores no estatales. Las intrusiones cibernéticas en tiempos de paz resultan contrarias a los estándares de conducta esperados para el mantenimiento de la paz, la seguridad internacional y el desarrollo de relaciones de amistad y cooperación entre los Estados. Los Estados gozan de los derechos inherentes a la plena soberanía y, en sentido contrario, tienen el deber de abstenerse de privar de esos derechos a otro, aun cuando el riesgo no parezca evidente.

El principio de no intervención, si bien se desprende del de soberanía, implica la intrusión en el ejercicio de los derechos soberanos de un Estado, de forma coercitiva. Una operación cibernética es contraria a este principio si ejerce un grado de presión que priva al Estado de su capacidad de decisión o libertad de acción. Esto es particularmente relevante en el caso de las Operaciones de Información que manipulan el discurso público o alteran información con el propósito de influenciar la elección democrática de un Estado o de impactar su estabilidad política, constituyendo una violación al principio de no intervención en función del grado de presión o coerción ejercidos.

Ahora bien, la acreditación de un hecho contrario a la soberanía o la prohibición de la intervención es sólo el primer paso. El ciberespacio proporciona una anonimidad que dificulta la atribución de la conducta ilegal a un Estado y, por lo tanto, la adjudicación de su responsabilidad internacional. La identificación del origen de una operación cibernética es sólo la primera de las complicaciones; la atribución de responsabilidad requiere la acreditación de un grado de control aceptado por el derecho internacional que permita considerar el hecho como conducta del Estado. Más que una falta de claridad en los criterios determinantes, el derecho internacional mantiene criterios rígidos que no se ajustan a la realidad de las ciberoperaciones y la falta de consenso entre los Estados impide el surgimiento de nuevos criterios consuetudinarios.

La aplicación de los criterios de control al ámbito cibernético no es del todo eficaz. El grado de evidencia requerida para ciberoperaciones prácticamente irrastreables, obstaculiza la atribución de responsabilidad a un Estado por hechos de actores no estatales. Incluso el criterio de control virtual, que atribuye la carga de la prueba al Estado origen del ataque, es criticable en cuanto a que los Estados no se encuentran en un plano de igualdad en sus capacidades técnicas o desarrollo tecnológico; los Estados menos desarrollados son incapaces, por sí solos, de prevenir, detectar o defenderse ante tales operaciones.

En el contexto cibernético, se aboga por una mayor flexibilidad en los criterios de atribución de responsabilidad al Estado, ya que el objetivo principal es detener los ataques y favorecer el cumplimiento de obligaciones internacionales. Sin embargo, ante la falta de consenso y los factores políticos que impiden la creación de normas vinculantes en este campo, la vía inmediata se traduce en la cooperación internacional a través de las diferentes iniciativas en materia de ciberseguridad (Asamblea General de la ONU, Res. 77/298); desarrollar la capacidad de los Estados para enfrentar los desafíos que representan las nuevas tecnologías.

Referencias bibliográficas

BANKS, Williams (2021). Cyber Attribution and State Responsibility. *Stockton Center for International Law*, 97, 1039-1072.

BUCHAN, Russell, NICHOLAS, Tsagourias (2017). The Crisis in Crimea and the Principle of Non- Intervention. *International Community Law Review*, 19(2/3), 165-193.

CHIRCOP, Luke (2019). Territorial Sovereignty in Cyberspace After Tallinn Manual 2.0. *Melbourne Journal of International Law*, 20(2), 349-377.

CLARK, David D., LANDAU, Susan (2011). Untangling Attribution. *Harvard National Security Journal,* 2(2), 1-45.

CRAWFORD, James. (2019). *Brownlie's principles of public international law* (9a ed.). Oxford.

CRAWFORD, James. (2013). *State responsibility: The general part.* Cambridge University Press.

DE FALCO, Marco. (2012). *Stuxnet Facts Report: A Technical and Strategic Analysis*. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence.

DELBERT, Tran (2018). The Law of Attribution: Rules for Attributing the Source of a Cyber-Attack. *Yale Journal of Law and Technology*, 20, 376-441.

DELERUE, François (2019). "Attribution to State of Cyber Operations Conducted by Non-State Actors". En CARPANELLI, Elena, LAZZERINI, Nicole (eds). Use and Misuse of New Technologies (pp. 233-255). Springer Cham.

DELERUE, François (2020a). "Circumstances Precluding or Attenuating the Wrongfulness of Unlawful Cyber Operations". En *Cyber Operations and International Law* (Cambridge Studies in International and Comparative Law, pp. 343-352). Cambridge University Press.

DELERUE, François (2020b). "Internationally Wrongful Cyber Acts: Cyber Operations Breaching Norms of International Law. En *Cyber Operations and International Law* (Cambridge Studies in International and Comparative Law, pp. 193-272). Cambridge University Press.

DELERUE, François (2020c). "The Threshold of Cyber Warfare: From Use of Cyber Force to Cyber Armed Attack". En *Cyber Operations and International Law* (Cambridge Studies in International and Comparative Law, pp. 273-342). Cambridge University Press.

FRASER, Angus (2016). Territorial Sovereignty in the Cyber Age. *Pandora's Box*, 23, 165-174.

HAATAJA, Samuli (2017). The 2007 Cyber Attacks against Estonia and International Law on the Use of Force: An Informational Approach. *Law, Innovation & Technology*, 9(2), 159-189.

HATHAWAY, Oona A., CHERTOFF, Emily, DOMÍNGUEZ, Lara, MANFREDI, Zachary, y TZENG, Peter (2012a). Ensuring Responsibility: Common Article 1 and State Responsibility for Non- State Actors. *Texas Law Review*, 100(4), 539-590.

HATHAWAY, Oona A., CROOTOF, Rebecca, LEVITZ, Philip, NIX, Haley, NOWLAN, Aileen, PERDUE, William y SPIEGEL, Julia (2012b). The Law of Cyber-Attack. *California Law Review*, 100(4), 817-885.

HELAL, Mohamed S. (2019). On Coercion in International Law. *New York University Journal of International Law and Politics*, 52(1), 1-122.

ILC (2001), "Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries". *Yearbook of the International Law Commission*, vol. II(2), 31-143.

KOSIK, Andrey L. (2015). The Concept of Sovereignty as a Foundation for Determining the Legality of the Conduct of States in Cyberspace. *Baltic Yearbook of International Law Online*, 14, 93-103.

LEVITE, Ariel, CHUANYING, Lu, PERKOVICH, George y YANG, Fan (2022). *Managing U.S.-China Tensions Over Public Cyber Attribution*. Carnegie Endowment for International Peace.

LIPSON, Howard F. (2002). *Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues*. Carnegie Mellon University, CERT Coordination Center.

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

Manual de Tallin 2.0 sobre el Derecho Internacional Aplicable a las Operaciones Cibernéticas (2017). *Grupos Internacionales de Expertos por Invitación del Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN.* Cambridge University Press.

MARGULIES, Peter (2013). Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility. *Melbourne Journal of International Law*, 14(2), 496-519.

MIRÓ LINARES, Fernando. (2012). *El cibercrimen: fenomenología y criminología de la delincuencia en el ciberespacio.* Marcial Pons Ediciones Jurídicas y Sociales.

MOORE, Andrew (2015). Stuxnet and Article 2(4)'S Prohibition against the Use of Force: Customary Law and Potential Models. *Naval Law Review*, 64, 1-27.

MOULIN, Thibault (2020). Reviving the Principle of Non-Intervention in Cyberspace: The Path Forward. *Journal of Conflict & Security Law*, 25(3), 423-447.

MOYNIHAN, Harriet (2019). *The Application of International Law to State Cyberattacks Sovereignty and Non-intervention*. Chatham House.

OTAN (2021). Statement by the North Atlantic Council in solidarity with those affected by recent malicious cyber activities including the Microsoft Exchange Server compromise [Comunicado de prensa].

PAYNE, Christian y FINLAY, Lorraine (2017). Addressing Obstacles to Cyber-Attribution: A Model Based on State Response to Cyber-Attack. *George Washington International Law Review*, 49(3), 535-568.

PIGGIN, Richard (2010). The Reality of Cyber Terrorism. *Engineering & Technology*, 5(17), 36-38.

SCHMITT, Michael N. (2014). "Below The Threshold' Cyber Operations: The Countermeasures Response Option and International Law. *Virginia Journal of International Law*, 54(3), 698-732.

SCHMITT, Michael N., VIHUL, Liis (2017). Respect for Sovereignty in Cyberspace. *Texas Law Review*, 95(7), 1639–1670.

SHACKELFORD, Scott J. (2010). State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem. *Georgetown Journal of International Law*, 42, 197-208.

SKINNER, Christina Parajon (2014). An International Law Response to Economic Cyber Espionage. *Connecticut Law Review*, 46(6), 1165-1207.

STOKES, Paul (2014). *State Responsibility for Cyber Operations: International Law Issues Event Report.* British Institute of International and Comparative Law.

TANYILDIZI, M. Emrah (2017). State Responsibility in Cyberspace: The Problem of Attribution of Cyberattacks Conducted by Non-State Actors. *Law & Justice Review,* 8(14), 119-176.

U.S. DEPARTMENT OF STATE (2022). Attribution of Russia's Malicious Cyber Activity Against Ukraine [Comunicado de prensa].

UYHENG, Joshua, CRUICKSHANK, Iain J. y CARLEY, Kathleen M. (2022). Mapping state-sponsored information operations with multi-view modularity clustering. *EPJ Data Sci*, 11(25).

VAN BENTHEM, Tsvetelina, DIAS, Talita, y HOLLIS, Duncan B. (2022). Information Operations under International Law. *Vanderbilt Journal of Transnational Law*, 55(5), 1217-1286.

WATTS, Sean (2015). "Low-Intensity Cyber Operations and the Principle of Non-Intervention". En OHLIN, Jens David, GOVERN, Kevin, FINKELSTEIN, Claire (eds). *Cyber War: Law and Ethics for Virtual Conflicts* (pp. 249-270). Oxford.

WATTS, Sean, THEODORE, Richard (2018). Baseline Territorial Sovereignty and Cyberspace. *Lewis & Clark Law Review,* 22(3), 771-840.

Documentos

Actividades Militares y Paramilitares (Nicaragua v. Estados Unidos de América), 1986, Corte Internacional de Justicia, 27 de junio de 1986.

Ciertas Actividades Realizadas por Nicaragua en la Zona Fronteriza, (Costa Rica v. Nicaragua), 2018, Corte Internacional de Justicia, 18 de febrero de 2018.

Conformidad con el derecho internacional de la declaración unilateral de independencia de Kosovo, Opinión Consultiva del 22 de julio de 2010, Corte Internacional de Justicia, I.C.J. Reports, 2010.

Corfu Channel (Reino Unido de Gran Bretaña e Irlanda del Norte v. Albania), 1949, Corte Internacional de Justicia, 9 de abril de 1949.

Fiscal v. Tadić, 1997, Tribunal Internacional Penal para la Antigua Yugoslavia, 7 de mayo de 1997.

Fiscal v. Tadić, 1999, Cámara de Apelaciones del Tribunal Internacional Penal para la Antigua Yugoslavia, 15 de julio de 1999.

Legalidad de la amenaza o el uso de armas nucleares, Opinión Consultiva del 8 de julio de 1996, Corte Internacional de Justicia, I.C.J. Reports, 1996.

Lotus (Francia v. Turquía), 1927, Corte Permanente de Justicia Internacional, 7 de septiembre de 1927.

Resolución 2625 (XXV), Declaración Relativa a 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, Asamblea General de las Naciones Unidas, del 24 de octubre de 1970.

Resolución A/RES/56/83, Responsabilidad del Estado por hechos internacionalmente ilícitos, Asamblea General de las Naciones Unidas.

Resolución A/RES/77/298, Estrategia Global de las Naciones Unidas contra el Terrorismo: octavo examen, Asamblea General de las Naciones Unidas, del 22 de junio de 2023.