Facultad de Derecho

Grado en Derecho y Relaciones Internacionales

Trabajo Fin de Grado

LA EFICACIA DE LOS LÍMITES DE LA SOBERANÍA ESTATAL FRENTE A LOS USOS MALICIOSOS DE LAS NUEVAS TECNOLOGÍAS.

Estudiante: Elisa Doussinague Gutiérrez

Directora: Profesora Raquel Regueiro Dubra

Madrid, abril 2020

ÍNDICE

1. INTRODUCCIÓN

El Estado se posiciona en la comunidad internacional como soberano e igual al resto de Estados que forman parte de ella. El principio de soberanía es inherente a los Estados como sujetos de Derecho Internacional, y dicho principio conlleva asimismo una serie de límites y obligaciones aplicables a todos los Estados. Los poderes estatales se han proyectado tradicionalmente sobre un territorio y una población determinada. Sin embargo, el avance de las nuevas tecnologías y auge de Internet ha dado lugar a la creación de un quinto espacio relacional sobre el cual el Estado proyecta su soberanía: el ciberespacio. No son pocas las cuestiones jurídicas que surgen alrededor de este nuevo ámbito, puesto que plantea dudas como el papel del Estado y hasta donde llegan las fronteras que no puede traspasar sin dañar lo que se encuentra bajo la potestad de otro Estado. El objetivo principal de este trabajo de investigación es el de explorar las distintas opciones relativas a la cuestión de la soberanía en el ciberespacio frente a los posibles usos maliciosos de las tecnologías. El estudio realizado se centra en los denominados ciberataques como nuevas amenazas a los Estados. Se trata de un tema de importancia creciente que se encuentra en el centro de debates doctrinales en el ámbito del Derecho Internacional Público, así como en el seno de gobiernos de Estados que buscan mejorar sus estrategias de ciberdefensa y seguridad.

Los motivos detrás de la elección de este tema de investigación se centran en la creciente importancia de la implantación de mecanismos de ciberseguridad a nivel estatal. Factores como el rápido desarrollo de las tecnologías, así como la globalización y el acceso universal a Internet han propiciado el incremento (tanto del número, como de la severidad) de las operaciones cibernéticas orientadas a causar daños a los Estados de la comunidad internacional. Esta situación ha propiciado el nacimiento de un interés dirigido a investigar el marco legal en que se encuentran los Estados, como sujetos de Derecho internacional y como miembros de la comunidad internacional, y sus respuestas frente a dichas amenazas a su poder soberano. Durante la pasada década se han incrementado las iniciativas estatales y regionales dirigidas a reforzar las defensas y aumentar la cooperación en el ámbito del ciberespacio, con el fin de poner fin a los ciberataques. En esta línea, el presente trabajo de investigación trata de exponer, de forma genérica, las cuestiones más controvertidas que nos encontramos en relación a la soberanía estatal como principio de Derecho internacional proyectada en un dominio que no es el tradicional: el ciberespacio. Asimismo, incluye una recopilación de opiniones doctrinales relativas a la equiparación de un ciberataque como violación a la prohibición del uso de la

fuerza consagrada en la Carta de las Naciones Unidas, y los distintos modos de reacción de los Estados.

El presente trabajo de investigación tiene como base bibliográfica principalmente fuentes primarias, entre las que se incluyen manuales de Derecho Internacional Público como los escritos por los juristas Manual Díez de Velasco y José Antonio Pastor Ridruejo. La investigación se apoya en numerosos artículos doctrinales escritos por el jurista americano especializado en el derecho internacional aplicable al ciberespacio Michael N. Schmitt, así como en otros artículos doctrinales publicados en revistas científicas, relevantes en la cuestión a tratar. Concretamente, la investigación se apoya especialmente en el Manual de Tallin, documento doctrinal editado por este mismo autor, elaborado en conjunto por un grupo de expertos independientes a petición del Centro de Excelencia para la Ciberdefensa Cooperativa de la OTAN, así como en el Manual de Tallin 2.0, segunda edición de este documento doctrinal. Además, en el presente trabajo se incluyen referencias a la normativa y jurisprudencia que, tanto a nivel nacional como en el contexto de la Unión Europea, presenta relevancia en el contexto de la investigación, así como documentos oficiales tales como resoluciones de la Asamblea General de las Naciones Unidas y otros documentos que emanan de las instituciones de la Unión.

La investigación se ha llevado a través del empleo del método deductivo, realizando un recorrido que parte de las cuestiones normativas generales a los aspectos más concretos de la cuestión. En el presente trabajo se incluye una recopilación del estado de la cuestión, a través de normas de Derecho Internacional y artículos doctrinales al respecto, para luego llegar al fondo del trabajo y tratar de esclarecer los aspectos más concretos y controvertidos relativos a la soberanía estatal en el ciberespacio.

A lo largo de esta investigación se presenta, en primer lugar, el principio de soberanía estatal consagrado como norma de naturaleza *ius cogens* en Derecho Internacional, imperativa para todos los miembros de la comunidad internacional. El desarrollo de dicho principio incluye un recorrido por los límites y obligaciones que conlleva para los Estados; el principio de igualdad soberana y el principio de no intervención. A continuación, se estudia el novedoso ámbito del ciberespacio como dominio estatal, revisando el marco conceptual y la medida en que el Estado proyecta su soberanía sobre él. En esta línea, se presenta la cuestión de la afectación de la soberanía estatal por operaciones realizadas en el ciberespacio. El siguiente apartado construye un análisis sobre los ciberataques como violaciones a la prohibición del uso de la fuerza,

estableciendo un marco conceptual de las operaciones cibernéticas consideradas ciberataques y los criterios empleados para su equiparación a un ataque armado. En último lugar, se incluyen los modos de reacción de los Estados a dichos ataques, que bien pueden responder a través de medios pacíficos o a través del uso de la fuerza, cuando se den los presupuestos necesarios para ello. El último apartado recoge las conclusiones extraídas de la investigación relativas a la eficacia de los límites del principio de soberanía estatal en el ámbito del ciberespacio.

2. LA SOBERANÍA ESTATAL Y SUS LÍMITES

2.1. El Estado soberano

El Estado se constituye como sujeto originario del Derecho Internacional. Como entidad soberana, el Estado posee un poder estatal autónomo *suma potestas* en sus relaciones internas, así como un poder de conducir su actuación externa con otros Estados (Truyol y Serra, 1999, pág. 317). El término de "soberanía" fue acuñado en el siglo XVI por Bodino, en su obra De República. Para dicho autor, la soberanía constituía la *suma in cives ac súbditos legibusque soluta potestas*, lo cual implica que aunque el poder del Estado emana de las leyes que rigen su actuación, se encontraba asimismo sujeto al Derecho Divino, Natural y de Gentes (Bodin, 1576). La soberanía del Estado no se constituye como absoluta. El atributo de la soberanía, de no tener límites, no admitiría una coexistencia entre Estados, puesto que, de ser concebida de forma absoluta, tan sólo podría existir un único Estado soberano (Barboza, Derecho Internacional Público, 1999, pág. 167).

El Estado, como sujeto soberano de Derecho Internacional, no se encuentra sumido a la autoridad de ningún otro Estado o grupo de estados. En palabras de Barberis, el Estado soberano no depende de ningún orden jurídico distinto al suyo propio, ni de ningún otro sujeto de Derecho Internacional (Barberis, 1973, págs. 41-42). Por ello, el Estado depende sólo del Derecho Internacional. La independencia se configura como expresión básica de su soberanía. Como establece el profesor Carrillo Salcedo, la soberanía es un principio constitucional del Derecho internacional y se basa en una relación de cooperación entre los Estados de la comunidad internacional (Carrillo Salcedo, 1991, pág. 83). En palabras de este autor, la soberanía posee una dimensión jurídica que se materializa en el conjunto de derechos y obligaciones estatales que trae consigo. El Estado posee un derecho a ejercer sus propias actividades estatales sin intromisión de cualquier otro estado y tiene a su vez la obligación de

proteger ese mismo derecho de los demás Estados. Todo ello sin perjuicio de sus obligaciones con respecto a las normas de Derecho internacional, dirigidas a preservar la estabilidad de la comunidad internacional.

El Estado soberano se construye sobre cuatro elementos básicos: una población permanente; territorio determinado; gobierno; y capacidad de entrar en relación con otros Estados (Art. 1, Convención sobre los Derechos y Deberes de los Estados, 26 de diciembre de 1933). Las competencias más básicas del Estado tienen carácter territorial, y conforman la llamada "soberanía territorial". La soberanía territorial posee tres características básicas: plenitud, exclusividad e inviolabilidad (Pastor Ridruejo, 2013, pág. 327).En primer lugar, la plenitud del Estado implica que los límites a su soberanía territorial no se presumen, se trata de una soberanía plena puesto que la función de la misma es permitir al mismo desplegar sus funciones y así asegurar la satisfacción de los intereses generales de la población (Pastor Ridruejo, 2013, págs. 327-328). En segundo lugar, la soberanía territorial es exclusiva, lo que implica que sobre un determinado territorio estatal no puede otro Estado ejercer sus propias competencias territoriales (Pastor Ridruejo, 2013, págs. 327-328). El árbitro Max Huber se pronunció sobre ello en el asunto de la Isla de Palmas, al hablar de la independencia como el "derecho de un Estado de ejercer sobre su territorio las funciones que le son propias, con exclusión de cualquier otro Estado" (Island of Palmas Case (Netherlands v USA), 1928, p. 838). Siguiendo a Max Huber, la soberanía territorial también trae consigo el deber del Estado de proteger en su propio territorio los derechos de otros Estados, incluyendo el derecho a la integridad y a la inviolabilidad (Island of Palmas Case (Netherlands v USA), 1928, p. 839). El Tribunal de la Haya reitera esta doctrina en su Sentencia del 25 de marzo de 1948, relativa al caso del estrecho de Corfú, al afirmar la existencia de un deber de todo Estado de "no permitir la utilización de su territorio a fines de actos contrarios a los derechos de otros Estados" (Corfu Channel Case (United Kingdom v Albania), 1948, p. 22). Por último, la soberanía territorial se caracteriza por su inviolabilidad en tanto que en Derecho Internacional existe la obligación de respetar la soberanía e integridad territorial de todo Estado (Pastor Ridruejo, 2013, pág. 328). Ello fue asimismo afirmado por el Tribunal de la Haya en el ya citado caso del canal de Corfú, en el cual se refiere al respeto a la soberanía territorial como base esencial de las relaciones entre Estados (Corfu Channel Case (United Kingdom v Albania), 1948)

2.1. La igualdad soberana

El principio de igualdad soberana se constituye como uno de los principios rectores de la Organización de las Naciones Unidas. Se consagra como tal en el art. 2, apartado 1 de la Carta de las Naciones Unidas. La propia Asamblea General ha concretado su contenido en la Declaración de principios de la Resolución 2625 (XXV), estableciendo la igualdad en derechos y deberes entre todos los Estados (A/RES/2625(XXV)). Todo Estado es miembro de la comunidad internacional por igual, sin importar sus diferencias en el plano económico, político o social (A/RES/2625(XXV)). Los Estados se encuentran en un plano de igualdad jurídica y de igualdad frente al Derecho internacional. De este principio se garantiza el respeto a la integridad territorial y a la independencia política de los Estados (Díez de Velasco, Instituciones de derecho internacional público, 2017, págs. 278-279).

A pesar de la vigencia de este principio en Derecho internacional, la realidad es que existen desigualdades de hecho entre los Estados que pueden dar lugar a diferencias en las situaciones de cada uno de ellos. Para paliar estas desigualdades, los países en vías de desarrollo tratan de articular estrategias para intentar superarlas (Pastor Ridruejo, 2013). De la mano al principio de soberanía estatal viene el principio de no intervención en los asuntos internos de otros Estados, el cual se desarrollará en el apartado posterior. Este principio es una expresión de la igualdad formal entre los Estados, por lo tanto, no implica que no existan desigualdades reales entre ellos (McWhinney, 1979). En palabras de MCWhinney, "algunos estados son más iguales que otros" (McWhinney, 1979).

Todo Estado tiene la obligación de respetar la personalidad de los Estados, tal y como se establece en la Resolución 2625 (XXV) de la Asamblea General de las Naciones Unidas. El árbitro Max Huber estableció en el asunto de la isla de Palmas que los poderes que posee un Estado como ente soberano comportan a la vez con el deber de proteger los derechos del resto de Estados (Island of Palmas Case (Netherlands v USA) 1928, p. 839). El Tribunal Judicial Internacional se pronuncia en el mismo sentido en el asunto del Estrecho de Corfú cuando establece como base esencial de las relaciones entre los estados el respeto mutuo de la soberanía territorial de cada uno de ellos (Corfu Channel Case (United Kingdom v Albania), 1948, p.22). El profesor Pastor Ridruejo establece que este principio acentúa la independencia de los Estados y la prohibición que se les aplica de intervenir en los asuntos de los demás (Pastor Ridruejo, 2013, págs. 286-287).

2.2. El principio de no intervención

El principio de no injerencia en los asuntos internos de otros Estados forma parte del Derecho internacional consuetudinario, como estableció en Tribunal Judicial Internacional en su sentencia de 27 de junio de 1986 (Caso concerniente a las actividades militares y paramilitares en Nicaragua y contra ella; Nicaragua contra Estados Unidos de América, 1986). En palabras del Tribunal de la Haya, este principio se presenta como un "corolario del principio de igualdad soberana de los Estados" (Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v United States), 1986, p.106). Este principio prohíbe la interferencia, ya sea directa o indirecta, en los asuntos internos o externos de otro Estado, e incluye cualquier intervención armada, así como otras formas de injerencia o amenaza de la personalidad del Estado (Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v United States), 1986, p.106). En la citada sentencia del Tribunal Judicial Internacional (1986) se establece su verdadero fundamento, el derecho que poseen todos los Estados a elegir su sistema político, económico, social y cultural sin ninguna interferencia de otro Estado (Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v United States), 1986, p. 108). Se trata, en palabras del profesor Díez de Velasco, de una encarnación del principio de libre determinación de los pueblos aplicada al Estado (Díez de Velasco, Instituciones de derecho internacional público, 2017). La obligación de no intervención en los asuntos de otro Estado se aplica a su vez a las organizaciones internacionales, como bien se establece en el art. 2, apartado 7, de la Carta de las Naciones Unidas (Organización de las Naciones Unidas, 1945).

El principio de no intervención en asuntos internos implica la prohibición de intervenir en aquellas materias sobre las cuales los Estados pueden decidir libremente en virtud de su condición como Estado soberano (Pastor Ridruejo, 2013, pág. 288). Siguiendo al profesor Pastor Ridruejo, la acción de un Estado que implique la coerción en aspectos políticos, económicos, sociales y culturales de otro Estado constituiría una intervención ilícita (Pastor Ridruejo, 2013, pág. 288). Sin embargo, como explica el autor Pastor Ridruejo, el principio de no intervención se presenta como uno de los más susceptibles a ser interpretado en maneras divergentes, llegando incluso a ser manipulado por los distintos Estados (Pastor Ridruejo, 2013, pág. 289). Ello se muestra en las distintas intervenciones que las superpotencias han realizado en distintos Estados, las cuales se han clasificado en legítimas y no legítimas (Díez de Velasco, 2017). Estas incluyen las intervenciones que se presentaban como un apoyo dirigido a proteger la independencia del Estado en cuestión, que se veía amenazada. El profesor Pastor Ridruejo

establece que dicho principio ha sido "flagrantemente violado" por los Estados más poderosos movidos por sus intereses políticos (Pastor Ridruejo, 2013, pág. 289).

La Carta de las Naciones Unidas (1945) incluye una disposición dirigida a recoger la prohibición del uso de la fuerza entre Estados. Se establece en el párrafo 4 del artículo 2º de la Carta la prohibición de los estados miembros a recurrir a la amenaza o al uso de la fuerza contra cualquier otro Estado (Organización de las Naciones Unidas, 1945). Dicha prohibición se construye sobre la idea de condenar la guerra, y su origen se remonta a la conmoción provocada tras los crímenes cometidos en la Segunda Guerra Mundial. Previamente, dicha prohibición recibió un gran apoyo en el Pacto de Renuncia a la Guerra del 27 de agosto de 1928 en París ("Pacto Briand-Kellog") (McWhinney, 1979). Sin embargo, en dicho tratado no se establecía mecanismo institucional alguno para garantizar el cumplimiento de la prohibición del uso de la fuerza (Díez de Velasco, 1973, págs. 1041-1050). Con la creación de la Organización de las Naciones Unidas tras la Segunda Guerra Mundial, se consagró dicho principio de forma más completa que en el Pacto Briand-Kellog, puesto que en la Carta se incluye la prohibición del uso de la fuerza así como la amenaza del uso del mismo, y se ubica en el marco de otros principios de Derecho Internacional (Díez de Velasco, 1973, págs. 1041-1050).

En el asunto relativo a las actividades militares y paramilitares en y contra Nicaragua del año 1986, la Corte Internacional de Justicia estableció que la prohibición del uso de la fuerza forma parte del derecho internacional consuetudinario (Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v United States), 1986). Se trata de una norma de *ius cogens*, imperativa en Derecho Internacional (Díez de Velasco, 1973, pág. 1045).

La Carta de las Naciones Unidas regula las excepciones a la prohibición del uso de la fuerza, estableciendo una serie de situaciones en las que se permite a los Estados el empleo de fuerza armada. La primera excepción se encuentra en el artículo 42 de la Carta, el cual permite la ejecución de operaciones armadas necesarias para el mantenimiento o restablecimiento de la paz y seguridad internacionales (Organización de las Naciones Unidas, 1945). En segundo lugar, el artículo 51 de la Carta regula el derecho a la legítima defensa:

> Ninguna disposición de esta Carta menoscabará el derecho inmanente de legítima defensa, individual o colectiva, en caso de ataque armado contra un Miembro de las Naciones Unidas, hasta tanto que el Consejo de Seguridad haya tomado las medidas necesarias para mantener la paz y la seguridad internacionales. Las medidas tomadas por los Miembros en ejercicio del derecho de legítima defensa serán comunicadas inmediatamente al Consejo de Seguridad, y no afectarán en manera alguna la autoridad y responsabilidad del Consejo conforme a la presente Carta para ejercer en cualquier

momento la acción que estime necesaria con el fin de mantener o restablecer la paz y la seguridad internacionales (Organización de las Naciones Unidas, 1945).

Se reconoce el derecho de los Estados al uso de la fuerza en caso de la existencia de un ataque armado, en ejercicio del derecho de legítima defensa de todo Estado. Siguiendo al autor Pastor Ridruejo, esta disposición no autoriza la llamada legítima defensa preventiva, que se produciría frente un temor razonable de un ataque inminente (Pastor Ridruejo, 2013, pág. 628). La legalidad en Derecho internacional del uso de la fuerza como legítima defensa preventiva es discutida por la doctrina internacional, como se expondrá más adelante en el apartado relativo al uso de la fuerza en el ámbito del ciberespacio. El artículo transcrito prevé, además de la legítima defensa individual, también la legítima defensa colectiva. De este modo, el artículo 51 de la Carta de las Naciones Unidas se constituye como base jurídica de grandes alianzas militares entre Estados, como la Organización del Tratado Atlántico Norte ("OTAN") (Pastor Ridruejo, 2013, pág. 628).

3. EL CIBERESPACIO. PECULIARIDADES Y EFICACIA DE LOS LIMITES TRADICIONALES DEL PRINCIPIO DE SOBERANÍA

3.1. El ciberespacio como nuevo ámbito relacional

El Manual de Tallin 2.0[1] define el término "ciberespacio" como aquel entorno "formado por componentes físicos y no físicos para almacenar, modificar e intercambiar datos usando redes informáticas" (Schmitt, 2017). El ciberespacio se desarrolla en una dimensión diferente a la tradicional dimensión del mundo físico o real: convive con el espacio digital o virtual (Lessig, 2001, pág. 356). El término fue acuñado en el año 1984 por el escritor americano William Gibson, y actualmente no existe un consenso internacional sobre la definición del ciberespacio. El Departamento de Defensa de Estados Unidos lo define como un dominio global compuesto por redes interdependientes de tecnologías de la información (Department of Defense Dictionary of Military and Associated Terms, 2010, pág. 58). Desde la propia Unión Europea se ha confirmado dicha consideración del ciberespacio como dominio global, al referirse al

[1] El Manual de Tallin ("*Tallinn Manual on the International Law Applicable to Cyber Warfare*") es un documento doctrinal redactado por un grupo de expertos en ciberseguridad a petición del Centro de Excelencia en la Defensa Cooperativa Cibernética de la OTAN, publicado en el año 2013 (Schmitt, 2013). El Manual contiene un análisis de las normas internacionales aplicables para combatir ataques cibernéticos. No se trata de un cuerpo normativo oficial de la OTAN pero constituye una guía, puesto que es el primer cuerpo de ideas sobre la materia (Fonseca, Perdomo, Arozarena, & Ulises, 2013). En el año 2017, se publicó una segunda edición denominada Manual de Tallin 2.0 (Schmitt, 2017).

ciberespacio como "quinto teatro de operaciones" (Informe del 25 de mayo de 2018, de la Comisión de Asuntos Exteriores, sobre ciberdefensa).

El ciberespacio posee una serie de rasgos que lo diferencian del tradicional territorio donde se proyecta la soberanía de los Estados. La definición incluida en la Doctrina para el empleo de las Fuerzas Armadas[2] establece que el ciberespacio se caracteriza por su extensión, anonimato, la inmediatez y su fácil acceso (Ministerio de Defensa, 2018). Este documento también hace referencia al carácter artificial del ciberespacio y su rápida evolución, rasgos que generan vulnerabilidades y oportunidades a la vez (Ministerio de Defensa, 2018, pág. 81). El ciberespacio queda incluido dentro de los cuatro *global commons*: junto con la superficie de las aguas internacionales, el espacio aéreo y el espacio exterior, se refiere al ciberespacio como bien común por el que circulan ideas y datos (de Tomás, 2019, pág. 100). La diferencia que existe entre estos dominios preexistentes y el ciberespacio es la naturaleza artificial de este último, puesto que se trata de un ámbito creado por el hombre (de Tomás, 2019, pág. 100). Siguiendo a Martin Libicki, el espacio cibernético está formado por tres capas: sintáctica, semántica y física, y cada una de ellas presenta distintas vulnerabilidades (Libicki, 2009, pág. 12). Por último, la capa humana, compuesta por el ser humano como creador y explotador del ciberespacio, se convierte en la parte más vulnerable del ciberespacio (Shackelford, 2009).

Otro de los aspectos más característicos del ciberespacio es su universalidad (Johnson & Post, 1996). El acceso a internet es global, y explica el vínculo existente entre la globalización y el desarrollo los medios informáticos. Otro de las notas más relevantes del quinto dominio es la aparición de amenazas por parte de actores no estatales (de Tomás, 2019, pág. 100). La forma de llevar a cabo los ataques a través de medios informáticos implica un bajo coste en comparación con los grandes desembolsos que un ataque tradicional necesariamente requería (Johnson & Post, 1996). No es necesaria la formación de un ejército, sino que un individuo o un pequeño grupo de individuos pueden perpetrar ataques dañinos con escasos conocimientos informáticos (Johnson & Post, 1996). Otro de los caracteres del ciberespacio es su naturaleza transnacional, según se afirma desde la Unión Europea:

> El ciberespacio tiene una naturaleza inherentemente transnacional y consta de una serie de redes e infraestructuras interdependiente. Por ejemplo, entre otras, internet y las redes de telecomunicación, constituyen uno de los canales presentes y futuros más importantes para satisfacer

[2] La PDC-01 (A) "Doctrina para el empleo de las Fuerzas Armadas" constituye la publicación doctrinal militar de más alto nivel. Es un documento doctrinal conjunto que describe la forma de actuación de las Fuerzas Armadas y las normas que rigen en este contexto (Ministerio de Defensa, 2018).

> las necesidades, intereses y derechos de los ciudadanos de la UE y de sus Estados miembros constituyéndose en un activo indispensable del crecimiento económico de la UE (Secretaria General del Consejo de la Unión Europea, 2013).

3.2. La soberanía estatal en el ciberespacio

El principio de soberanía ha encontrado tradicionalmente su máxima expresión sobre el territorio físico (Pastor Ridruejo, 2013). Hoy encuentra proyección a su vez en el ciberespacio (de Tomás, 2019, pág. 100). El Manual de Tallin establece las normas relativas a la aplicación del concepto de soberanía en el ciberespacio. En dicho estudio académico, se establece que la soberanía territorial que poseen los Estados les da a su vez el derecho a controlar las ciber-infraestructuras y las actividades cibernéticas que se encuentren en su territorio (Schmitt, 2013, pág. 25). El Manual de Tallin 2.0 establece asimismo en su Regla número 4 la prohibición de que los Estados lleven a cabo operaciones cibernéticas que constituyan una violación de la soberanía de otro Estado (Schmitt, 2017). En la misma línea, el autor Michael N. Schmitt establece que:

> Es un error afirmar que debe existir una regla específica para las operaciones cibernéticas que no equivalen a un uso ilícito de la fuerza o intervención coercitiva, pero que se manifiesta en el territorio de otro Estado, y se califican como violaciones de la soberanía territorial (Schmitt & Vihul, 2017, pág. 1647).

El Manual de Tallin 2.0 establece que toda violación de la soberanía como una norma primaria de Derecho internacional, y trata de aclarar las circunstancias en las que una operación cibernética podría constituir una violación a la soberanía territorial de un Estado (Schmitt & Vihul, 2017, pág. 1647). El comentario de la Regla 4 establece que "cualquier operación que impida o haga caso omiso del ejercicio por parte de otro Estado de sus prerrogativas soberanas constituyen una violación de dicha soberanía" (Schmitt, 2017).

La sujeción del ciberespacio a la soberanía estatal se fundamenta en los siguientes factores: en primer lugar, el ciberespacio requiere necesariamente de una entidad que lo controle y de una infraestructura física con soporte territorial que permita el acceso a sus usuarios. En palabras del autor Patrick W. Franzese, "el ciberespacio requiere de una arquitectura física para existir" (Franzese, 2009, pág. 17). Asimismo, las relaciones financieras que se establecen dentro del ciberespacio requieren regulación determinada materializada en leyes estatales (Franzese, 2009, pág. 17). En tercer lugar, todo contenido transmitido a través del ciberespacio tiene implicaciones en la realidad física y, por lo tanto, está sujeto a las leyes de los respectivos estados, ya que éstos tienen un interés y un control legítimo sobre las transacciones cibernéticas

(Khanna, 2018, pág. 150). En cuarto lugar, los Estados están tratando gradualmente de imponerse en el ciberespacio con fines de seguridad nacional y, a fin de prevenir los daños y reducir su vulnerabilidad, el ciberespacio no puede quedar exento de regulación propia (Khanna, 2018, pág. 152). Asimismo, al igual que ocurre en el territorio físico, el ciberespacio también requiere la soberanía de los Estados para regular, proteger y castigar a los diversos actores que en él actúan (Khanna, 2018, pág. 152).

Con respecto a la violación de la integridad territorial de otro Estado, el Manual de Tallin 2.0 clasifica toda operación cibernética de un Estado que causa daños o lesiones físicas en el territorio de otro Estado como violación a la soberanía territorial de este último (Schmitt, 2017). Asimismo, el grupo de expertos también estuvo de acuerdo en que una operación cibernética que provocara una pérdida de funcionalidad (de tal grado tal que su equipo básico necesitara ser reparado o reemplazado) constituiría una violación a la soberanía territorial del Estado afectado (Schmitt, 2017, págs. 20-21).

El carácter innovador de la tecnología que subyace tras el ciberespacio no obstaculiza la aplicabilidad del principio de soberanía a los componentes y a las actividades de este (Schmitt, 2017, págs. 20-21). La gran mayoría de normas y principios del derecho internacional consuetudinario se aplican al ciberespacio y a las actividades cibernéticas (Heinegg, 2012, pág. 10). En la Estrategia Internacional para el Ciberespacio de 2011 publicada por el gobierno de Estados Unidos, el entonces presidente Barack Obama afirmó que "la elaboración de normas para la conducta de los Estados en el ciberespacio no requiere una reinvención del derecho internacional consuetudinario ni hace obsoletas las normas internacionales existentes" (International Strategy for Cyberspace, 2011, pág. 9). Esto no quiere decir que dichas normas y principios sean aplicables al ciberespacio en su interpretación tradicional. El carácter novedoso del ciberespacio, y la vulnerabilidad de la infraestructura cibernética traen consigo gran incertidumbre entre los gobiernos y los juristas en cuanto a si las normas y principios tradicionales del derecho internacional consuetudinario se encuentran a la altura de dar las respuestas deseadas determinadas cuestiones (Schmitt, 2017, págs. 20-21). Por consiguiente, los Estados deben llegar a un acuerdo, no sólo sobre la aplicación principal del Derecho internacional consuetudinario al ciberespacio, sino también llegar a una interpretación común que tenga en cuenta las características singulares de este nuevo dominio (Heinegg, 2012, pág. 11). El Manual 2.0 de Tallin clasifica también como violación de la soberanía aquellas

operaciones cibernéticas que interfieren en el control de otro Estado sobre funciones inherentes al gobierno de este (Schmitt, 2017, pág 21).

Como establece el autor Michael N. Schmitt, el enfoque del Manual de Tallin 2.0 relativo a la soberanía expuesto en este apartado parece gozar de una amplia aceptación (Schmitt & Vihul, 2017, pág. 1649). En el contexto internacional actual, la Asamblea General invitó a los Estados Miembros a la creación de "Grupos de Expertos Gubernamentales sobre los Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional" (A/RES/53/70). En el informe elaborado en el año 2013, se afirmó el principio de soberanía de los Estados sobre las infraestructuras de tecnologías de la información situadas en su territorio:

> La soberanía del Estado y las normas y los principios internacionales que emanan de ella son aplicables a la realización de actividades relacionadas con las tecnologías de la información y las comunicaciones por parte de los Estados y a su jurisdicción sobre la infraestructura de tecnologías de la información y las comunicaciones dentro de su territorio; los Estados deben cumplir sus obligaciones internacionales en relación con los hechos internacionalmente ilícitos que se les puedan imputar (Informe del Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional, 2013, párr. 20).

La elaboracion de dichos informes, dirigidos a informar al Secretario General de las Naciones Unidas, muestran la preocupación de los Estados y su voluntad de elaborar una serie de principios que garanticen la seguridad de los sistemas de información mundiales, así como la conciencia de la "existencia de terrorismo y delincuencia en la esfera de la información" (A/RES/53/70, párr. 2).

3.3. La afectación de la soberanía estatal ante los ciberataques

El término ciberataque puede definirse como el empleo de acciones para modificar, alterar, engañar, destruir o denigrar los sistemas informáticos o redes de otro sujeto o los programas que transitan por esos sistemas o redes informáticas (Owens, Dam, & Lin, 2009). El Departamento de Defensa de Estados Unidos ha clasificado las actividades de ciberguerra dentro de las llamadas operaciones de redes informáticas, y las ha dividido en tres categorías distintas: ataques a redes informáticas, explotación de redes informáticas y defensa de redes informáticas (Cartwright, 2011, pág. 8). La naturaleza de los ciberataques hace difícil la labor de clasificar estas operaciones como actos de guerra o como mecanismos de defensa. Algunos ejemplos comunes de ciberataques incluyen los sabotajes en las infraestructuras críticas y negación de servicios.

En primer lugar, numerosos ataques dirigidos a las infraestructuras críticas de un Estado se llevan a cabo a través de ataques informáticos. El término "infraestructura crítica" se refiere a aquellas infraestructuras estratégicas (es decir, aquellas que proporcionan servicios esenciales) cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales" (Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas). En la actualidad, dichas infraestructuras dependen en gran medida de las tecnologías, convirtiéndose en objetivos vulnerables de los ataques informáticos perpetrados en el ciberespacio (Giraldo, 2017, pág. 18). En el marco europeo, el Consejo de la Unión Europea se ha pronunciado sobre su definición, refiriéndose a las infraestructuras críticas como:

> El elemento, sistema o parte de este situado en los Estados miembros que es esencial para el mantenimiento de funciones sociales vitales, la salud, la integridad física, la seguridad, y el bienestar social y económico de la población y cuya perturbación o destrucción afectaría gravemente a un Estado miembro al no poder mantener esas funciones (Consejo de la Unión Europea, 2011).

El programa Stuxnet constituye uno de los ejemplos más destacados de ciberataques consistentes en un sabotaje de infraestructuras (Weinberger, 2011, pág. 142). Dicho programa consiste en un programa invasivo empleado presuntamente por Estados Unidos e Israel para atacar las instalaciones nucleares de Irán (Sebenius, 2017). Estados Unidos e Israel no reivindicaron oficialmente su responsabilidad, sin embargo, no son pocos los autores que les atribuyen dicho ataque puesto que complejidad del programa hacía que resultara improbable que hubiera sido dirigido por cualquier otro Estado con tanto interés en disuadir la capacidad nuclear de Irán (Chen & Abu-Nimeh, 2011, pág. 91). El programa fue introducido en la red iraní por medio de una unidad de memoria USB, se propagó dentro de la red y causó un daño significativo a las redes nucleares de Irán (Weinberger, 2011, pág. 142). El autor Maxwell Montgomery establece, a modo de exagerar aún más lo que podría haber ocurrido, que si un reactor nuclear se hubiera fundido y causado un daño civil significativo, este ciberataque habría estado a la par de un ataque nuclear tradicional, con Estados Unidos como el agresor (Montgomery, 2019, pág. 502). Esta operación ilustró que el programa maligno en un ordenador podía causar daños físicos en la infraestructura del Estado víctima, potencialmente equivalentes a los causados por un ataque militar tradicional (Weinberger, 2011, pág. 142). Otros autores establecen que el caso de Stuxnet no constituye un supuesto en el que se haya superado el umbral establecido en el artículo 2.4 de la Carta, puesto que dicho ataque no causó daños a seres humanos, ni supuso un daño a una infraestructura crítica comprometiendo el

funcionamiento o la estabilidad de Irán (Solano Díaz, 2014, pág. 51) (Tsang, 2009) (Gill & Ducheine, 2013, pág. 463).

En segundo lugar, el ataque distribuido de denegación de servicio constituye una modalidad de ciberataque que podría paralizar la capacidad de una nación para comunicarse o acceder a la información durante períodos prolongados (Tamkin, 2017). En el año 2007 un grupo de piratas informáticos de nacionalidad rusa participaron presuntamente en un ataque de denegación de servicio distribuida, causando el cierre de partes de Internet en el estado de Estonia, y limitó los canales de comunicación en el país (Tamkin, 2017). El ciberataque contra Estonia duró semanas. El ataque incluyó; manipulación de las páginas web, eliminación de contenido de las mismas y su sustitución por propaganda rusa, el cierre completo de sitios populares (incluidos páginas web del gobierno), el cierre del principal medio de comunicación del país y la saturación de las redes críticas utilizadas para las redes de los móviles (Shackelford, 2009, pág. 205).

A pesar de que la Carta de las Naciones Unidas establece un marco de normas dirigidas al "derecho de la guerra", o *ius ad bellum*, carece de una doctrina clara sobre cómo debe proceder una nación después de un ciberataque que equivalga a un ataque armado. En el párrafo 4º del art. 2 de la Carta, como se ha desarrollado en un apartado previo, se establece la prohibición del uso de la fuerza (Organización de las Naciones Unidas, 1945). Se plantean cuestiones fundamentales sobre los tipos y grados de ataques a la red que pueden entrar en el ámbito jurídico del artículo, puesto que no se pronuncia sobre otros ataques más sutiles, que no implican una amenaza percibida de fuerza armada (Joyner & Lotrionte, 2001). La práctica de los Estados ha demostrado que la mera coacción u otras formas de agresión no activan las protecciones del artículo 2.4 (Shackelford, 2009). Por consiguiente, un Estado podría tener derecho a la legítima defensa en respuesta a un ciberataque sólo cuando este alcanzara el nivel de un ataque armado (Schmitt, 2007). El caso de Estonia ilustra los principales obstáculos jurídicos para la obtención de una justificación del uso de la defensa propia: en primer lugar, la atribución del ataque a un Estado determinado, y en segundo lugar, demostrar que el ataque cibernético alcanzó el nivel de un ataque armado tradicional de las fuerzas militares (Shackelford, 2009).

El problema de la atribución se excede al ámbito de investigación de este trabajo, sin embargo, conviene hacer referencia al mismo dada su importancia en el contexto del trabajo. En primer lugar, la Asamblea General de las Naciones Unidas se pronunció sobre la responsabilidad de

los Estados por sus actuaciones en la Resolución 56/83, del 12 de diciembre de 2001, relativa a la responsabilidad de los Estados por actos internacionalmente ilícitos. El artículo 8 de la Resolución establece que los Estados son responsables de los actos internacionalmente ilícitos llevados a cabo por instrucciones o bajo la dirección o control del Estado (A/RES/56/83). La problemática de la atribución de la responsabilidad por las operaciones llevadas a cabo en el ciberespacio tiene lugar respecto a operaciones cibernéticas realizadas por actores no estatales que están vinculados a un Estado (Schmitt, 2007, pág. 9).

En la actualidad, incluso ataques a menor escala poseen un potencial de "dañar o perturbar gravemente la defensa nacional u otros servicios sociales vitales y provocar un grave daño al bienestar público" (Joyner & Lotrionte, 2001). La dependencia a la tecnología de redes de las sociedades modernas es tal que un daño sustancial a la infraestructura de información podría paralizar su sociedad o hacerla colapsar (Shackelford, 2009, pág. 198).

La respuesta de la Unión Europea, consciente del peligro que las ciber amenazas suponen para los Estados miembros, se materializa en el Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) nº 526/2013 (en adelante, "Reglamento sobre la ciberseguridad") emitido el 17 de abril de 2019, con el objetivo de fortalecer las capacidades de los Estados miembros y sus empresas, así como de "mejorar la cooperación, el intercambio de información y la coordinación entre los Estados miembros y las instituciones, órganos y organismos de la Unión" (Reglamento sobre la ciberseguridad, 2019, párr. 6). El objeto de este reglamento es establecer los objetivos y mandato de la ENISA, y el establecimiento de un marco para la creación de los esquemas europeos de certificación de seguridad, dirigidos a regular la armonizacion de las medidas de ciberseguridad dentro de la Unión (Reglamento sobre la ciberseguridad, 2019, art.1). En relación a dichas certificaciones, se establece que "en el futuro podría revelarse necesario convertir en obligatorias para algunos productos, servicios o procesos de TIC, determinadas exigencias específicas en materia de ciberseguridad, así como la certificación relacionada con ella" (Reglamento sobre la ciberseguridad, 2019, párr. 92).

4. LOS CIBERATAQUES COMO VIOLACIONES A LA PROHIBICIÓN DEL USO DE LA FUERZA

4.1. La equiparación de un ciberataque a un ataque armado

Como señala el autor Pastor Ridruejo, en el Derecho Internacional clásico los Estados soberanos tenían derecho ilimitado a hacer la guerra (Pastor Ridruejo, 2013, pág. 619), y como señalan los autores Oppenheim y Lauterpacht, la guerra era una "función natural del Estado y una prerrogativa de su soberanía incontrolada" (Oppenheim & Lauterpacht, 1944, págs. 144-145). Sin embargo, la evolución de la comunidad internacional, así como la conmoción producida por los graves crímenes cometidos en contextos bélicos, implicaron que los Estados introdujeran en la Carta de las Naciones Unidas la prohibición del uso de la fuerza, así como un mecanismo institucional para las violaciones de la misma (Pastor Ridruejo, 2013, pág. 628). El Estado ejerce sus poderes principalmente sobre su territorio, sin perjuicio de las zonas del ciberespacio que se encuentren a su vez bajo su soberanía, como se ha explicado en el apartado anterior. Por ello, y frente la amenaza de los usos maliciosos de las nuevas tecnologías, cabe preguntarse cuándo puede una operación realizada en el ciberespacio ser considerado un ataque armado y, por ende, una violación a la prohibición establecida en el artículo 2.4 de la Carta de las Naciones Unidas. En palabras del autor Juan Alberto Salinas Macías, "el reto más importante en un escenario de conflicto en el ciberespacio es la ausencia de certidumbre jurídica" (Salinas Macías, 2015, pág. 130). El marco jurídico internacional de la amenaza y el uso de la fuerza, descrito en el primer apartado de este trabajo, es único y aplicable a cualquier uso de la fuerza, con independencia del arma empleada, como estableció la Corte Internacional de Justicia en relación a la amenaza y uso de las armas nucleares (Opinión consultiva de 8 de julio de 1996 sobre legalidad de la amenaza y uso de armas nucleares, 1996, párr. 139).

En la Orden del Ministerio de Defensa por la que se crea el Mando Conjunto de Ciberdefensa de las Fuerzas Armadas se define el término ciberataque como:

> La acción producida en el ciberespacio que compromete la disponibilidad, integridad y confidencialidad de la información mediante el acceso no autorizado, la modificación, degradación o destrucción de los sistemas de información y telecomunicaciones o las infraestructuras que los soportan (Orden Ministerial 10/2013, de 19 de febrero, por la que se crea el Mando Conjunto de Ciberdefensa de las Fuerzas Armadas).

El Manual de Tallin establece en su art. 51.2 la definición de ataque cibernético como "toda operación cibernética, ya sea ofensiva o defensiva, que se espera razonablemente que cause

lesiones o la muerte a personas o daños o destrucción de objetos" (Schmitt, 2013, pág. 91). Otros autores han propuesto distintas definiciones para el término ciberataque, describiéndolo como "aquella expresión que se utiliza para describir un conjunto de actividades nocivas que tienen lugar en el ciberespacio" (Cornish, Livingstone, Clemente, & Yorke, 2010). Determinar si un ciberataque constituye una violación a la prohibición general del uso de la fuerza exige estudiar en primer lugar, la interpretación del término "uso de la fuerza" en Derecho internacional; y en segundo lugar, si un ciberataque puede llegar a ser considerado como tal con arreglo a esas normas[3] (Gervais, 2012, pág. 536).

Para dar comienzo a este análisis partimos de la Convención de Viena sobre el Derecho de Tratados, que establece las normas de interpretación de los tratados. El artículo 31 de la Convención establece que "un tratado deberá interpretarse de buena fe conforme al sentido corriente que haya de atribuirse a los términos del tratado en el contexto de estos teniendo en cuenta su objeto y fin" (Convención de Viena sobre el Derecho de los Tratados, 1969). El significado tradicional de "fuerza" es amplio y abarca el empleo de medidas coercitivas (Black, 2009, pág. 717). Las medidas coercitivas incluyen el empleo de instrumentos financieros (como la concesión o la retención económica para conseguir un objetivo); instrumentos diplomáticos (como la negociación y promoción entre los representantes de los Estados) (Reisman & Baker, 2011, págs. 30-32). Siguiendo a Gervais, bajo una interpretación extensiva del término "fuerza", cada uno de estos instrumentos podría ser objeto de regulación de la Carta (Gervais, 2012, pág. 536).

Sin embargo, a la luz del objeto y propósito de la Carta, el término "fuerza" debería ser interpretado de forma restrictiva (Gervais, 2012, pág. 536) . Como se establece en el Preámbulo de la Carta, el objeto de las Naciones Unidas constituye el mantenimiento de la paz y la seguridad internacionales, así como "preservar a las generaciones venideras del flagelo de la Guerra " (Organización de las Naciones Unidas, 1945). La historia de la redacción de la Carta refuerza la conclusión defendida por Gervais, puesto que se presentó una propuesta para ampliar el alcance del párrafo 4 del artículo 2 a la coerción económica y fue expresamente rechazada por las Naciones Unidas (Summary Report of Eleventh Meeting of Committee I/1,

[3] Un ataque cibernético puede no considerarse como violación del artículo 2 de la Carta y al mismo tiempo, seguir siendo incompatible con el Derecho internacional. La Corte Internacional de Justicia estableció en el asunto de las actividades militares y paramilitares en y contra Nicaragua que "el principio de no intervención implica el derecho de todo Estado soberano a conducir sus asuntos sin interferencias externas [...] es parte integrante del derecho internacional consuetudinario" (Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v United States), 1986).

1945). Por tanto, al excluir explícitamente la coacción económica de la definición de fuerza en la redacción del párrafo 4 del artículo 2, la redacción de la carta se centra en instrumentos militares.

Por otro lado, el Tribunal Internacional de Justicia ha estipulado que la Carta no abarca todo el ámbito de aplicación de la regulación de la fuerza, y que es necesario recurrir a normas consuetudinarias de Derecho internacional para completar la regulación del uso de la fuerza (Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v United States), 1986, parr. 14).

4.2. Criterios para la equiparación de un ciberataque como ataque armado

Siguiendo a Schmitt, cuando un ataque tradicional puede considerarse un ataque armado, también puede considerarse como tal un ataque cibernético que cause daños o perjuicios (Schmitt, 2014, pág. 279). La cuestión más controvertida es la relativa a la posibilidad de aplicar la prohibición del uso de la fuerza a una operación cibernética que, sin conllevar graves efectos destructivos, provoque consecuencias no-físicas.

La doctrina ha desarrollado principalmente tres criterios para medir si una operación cibernética puede ser considerada como ataque contrario a la prohibición del uso de la fuerza. En primer lugar, el criterio instrumental o "*instrumentality approach*; en criterio basado en objetivos o "*target-based approach*" y el criterio basado en las consecuencias o "*consequentiality approach"* (Sharp, 1999) (Raboin, 2011) (Gervais, 2012). El criterio instrumental consiste en evaluar los medios empleados más que sus consecuencias; ello implica que la mayoría de las operaciones cibernéticas no serían consideradas como fuerza armada ya que carecen típicamente de las características presentes tradicionalmente en los ataques militares y los efectos físicos de los mismos (Gervais, 2012).

El segundo criterio clasifica una operación cibernética como uso de la fuerza según el nivel de afectación a infraestructuras críticas del Estado, aun cuando no haya destrucción o heridos significativos (Raboin, 2011, págs. 655-656). Bajo este modelo, cualquier ataque cibernético dirigido contra infraestructuras críticas es un uso de la fuerza (Sharp, 1999, págs. 129-131). Desde el momento en que un ciberataque tiene como objetivo una infraestructura crítica, existe una amenaza inminente que crea un nivel de daño suficiente para justificar la autodefensa anticipada del Estado que va a ser atacado (Gervais, 2012, pág. 538). La debilidad de este

argumento recae en la naturaleza de los efectos de los ciberataques, ya que un ataque puede no dirigirse intencionalmente a una infraestructura crítica y terminar interrumpiéndola (Gervais, 2012, pág. 538). Adicionalmente, siguiendo a Gervais, "este modelo de responsabilidad objetiva autorizaría la autodefensa para el delito más benigno" (Gervais, 2012, pág. 538)

El tercer criterio, el criterio basado en las consecuencias, analiza los efectos producidos por la operación, entendiendo que se puede considerar uso de la fuerza cuando los daños producidos por el acto sean equivalentes a los de una operación militar tradicional, y existirá por tanto una violación a la prohibición del art. 2(4) de la Carta (Raboin, 2011, págs. 655-656). Bajo este modelo, un ataque cibernético se considera un uso de la fuerza si el atacante busca causar destrucción física directa, lesiones o muerte (Gervais, 2012, pág. 586). Este enfoque elimina la necesidad de examinar el instrumento de ejecución, y permite a la comunidad internacional adaptar la Carta a la evolución de la tecnología (Brownlie, 2002, pág. 362). El mayor defecto de este enfoque lo señala el autor Gervais, explicando la dificultad que existe en trazar la línea entre los efectos directos e indirectos de un ataque cibernético, y la mayoría de los ataques cibernéticos no causan directamente daños físicos o la muerte (Gervais, 2012, pág. 587). A título de ejemplo, un ciberataque que cierra temporalmente las líneas de comunicación de la policía de emergencia y los servicios de ambulancia puede no causar daños físicos o muertes directamente, pero podría causar ambos de manera indirecta. Este último criterio ha sido adoptado por el Grupo Internacional de Expertos en el Manual de Tallin en la regla número 11, con el objetivo de clarificar cuando una operación cibernética constituye uso de la fuerza (Schmitt, Tallinn Manual on The International Law Applicable to Cyber Warfare, 2013, pág. 48). Asimismo, en el Manual de Tallin se recomienda el empleo de los criterios de Schmitt para analizar las operaciones que no puedan clasificarse claramente como un uso de la fuerza (Schmitt, Tallinn Manual on The International Law Applicable to Cyber Warfare, 2013, pág. 48). El autor Michael N. Schmitt plantea un modelo de análisis que se enmarca en el último criterio, por el cual deberán valorarse una serie de factores de la operación: la severidad; inmediatez; vinculación directa; intrusión militar; medida de los efector; carácter militar; participación estatal; y presunta legalidad (Schmitt, 2011, págs. 578-581). En este contexto, Schmitt establece un conjunto de factores dirigidos a guiar a los Estados en su decisión sobre la legalidad de un ataque cibernético (Schmitt, 2010, pág. 155). Los criterios propuestos por el autor son los siguientes:

- En primer lugar, el nivel de severidad (*severity* en inglés) de la amenaza o del daño físico causado por el ataque cibernético en cuestión constituye el factor más relevante del análisis (Schmitt, 2010, pág. 155). El autor establece que "los efectos de un ataque que impliquen daños físicos a las personas o a la propiedad serán por sí solas un uso de la fuerza" (Schmitt, 2010, pág. 155):

- La inmediación (*immediacy* en inglés) de la operación cibernética, se refiere a aquellas operaciones cuyos efectos son inmediatos, dejando a los Estados poco margen para invocar medidas pacíficas de solución de controversias (Schmitt, 2010, pág. 156);

- La causalidad directa (*directness* en inglés): se trata de medir la existencia de un nexo causal directo entre la operación en cuestión y los efectos dañinos producidos (Schmitt, 2010, pág. 156);

- El carácter intrusivo (*invasiveness* en inglés) de la operación mide el nivel de intensidad en que se ha invadido los sistemas cibernéticos del Estado objetivo (Schmitt, 2010, pág. 155);

- La mensurabilidad (*measurability* en inglés) se centra en valorar si los efectos son identificables y cuantificables de forma objetiva, será más probable que la operación que los ha causado sea considerada uso ilegítimo de la fuerza (Schmitt, 2010, pág. 155);

- La presunción de legitimidad (*presumptive legitimacy* en inglés) implica aplicar la presunción de legalidad en ausencia de prohibición explicita (Schmitt, 2010, pág. 155); y

- La responsabilidad (r*esponsibility* en inglés) atribuida al ataque implica, según Schmitt, que cuanto más estrecho sea el nexo entre un Estado y las operaciones, más probable será que otros Estados caractericen dichas operaciones como usos de la fuerza, puesto que su atribución a un Estado concreto supone un mayor riesgo para la estabilidad internacional (Schmitt, 2010, pág. 156).

Estos siete factores componen los elementos de juicio propuestos por Michael N. Schmitt dirigidos a orientar la decisión de los Estados sobre la caracterización de un ciberataque como uso ilegítimo de la fuerza (Solano Díaz, 2014, pág. 43). El informe del Instituto de las Naciones Unidas de Investigación para el Desarme (UNIDIR) publicado en el año 2011 clasifica como

ejemplos de uso de la fuerza aquellas operaciones cibernéticas dirigidas a manipular los sistemas informáticos generando una crisis en una central nuclear o desactivar mecanismos de control aéreo de un aeropuerto concurrido en situaciones con malas condiciones meteorológicas, comportando estos ataques graves consecuencias en términos de víctimas y daños materiales (Melzer, 2011, pág. 12).

Para concluir, no existe un estándar especifico aplicable a todas las operaciones cibernéticas para determinar si traspasan el umbral del artículo 2.4 de la Carta (Solano Díaz, 2014) (Schmitt, 2010). Se trata, en palabras de Michael N. Schmitt, de una "decisión política de los Estados" que implicará llevar a cabo una valoración razonable los distintos parámetros establecidos para comparar de forma cualitativa y cuantitativa el ciberataque con aquellas medidas coercitivas físicas que constituyen una violación de la prohibición del artículo 2.4 de la Carta (Schmitt, 2010).

4.3. Modos de reacción de los Estados

La realidad internacional implica que en ocasiones los estados se vean inmersos en controversias internacionales entre ellos. Como explica el profesor Pastor Ridruejo, frente a una controversia entre estados el Derecho Internacional Contemporáneo no les impone una obligación de resultado; sino una obligación de comportamiento (Pastor Ridruejo, 2013, pág. 576). En otras palabras, los Estados no están obligados necesariamente a llegar a un arreglo de la controversia; la obligación impuesta por el Derecho Internacional consiste en que deben procurar llegar a una solución justa y rápida (Pastor Ridruejo, 2013, pág. 576). Prima el principio de la libertad de elección del medio de solución, que se encuentra limitado por la prohibición del uso de la fuerza, ya examinada en un apartado anterior. Las principales normas en Derecho Internacional que rigen en la cuestión de la solución de las controversias son: en primer lugar, la Carta de las Naciones Unidas recoge en su Capítulo VI las disposiciones relativas al arreglo pacífico de controversias; y en segundo lugar, la libertad de elección de medio confirmada por la jurisprudencia del Tribunal de la Haya (Pastor Ridruejo, 2013, pág. 576). Cuando un Estado es víctima de un ciberataque, este puede elegir el medio o mecanismo a emplear como respuesta. Los medios pacíficos de resolución de controversias buscan encontrar una solución entre ambos Estados sin llegar al uso de la fuerza. Además, y como se ha explicado, si el ciberataque en cuestión llegase a equipararse a un uso de la fuerza prohibido

por la Carta, el Estado víctima podría reaccionar amparándose en el artículo 51 de la Carta, empleando la fuerza como legítima defensa.

a. El empleo de medios pacíficos

La Carta de las Naciones Unidas establece como en su artículo 1.1 el primer propósito de la Organización de lograr el mantenimiento de la paz y seguridad internacionales, y para ello establece como labor la toma de medidas dirigidas a:

> Prevenir y eliminar amenazas a la paz, y para suprimir actos de agresión u otros quebrantamientos de la paz; y lograr por medios pacíficos, y de conformidad con los principios de justicia y del Derecho Internacional, el ajuste o arreglo de controversias o situaciones internacionales susceptibles de conducir a quebrantamientos de la paz (Organización de las Naciones Unidas, 1945).

Las competencias de la organización relativas al arreglo pacífico de controversias se recogen en el Capítulo VI de la Carta. Concretamente, en su artículo 33 se establece la idea de que los Estados parte de una controversia internacional "tratarán de buscarle solución, ante todo, mediante la negociación, la investigación, la mediación, la conciliación, el arbitraje, el arreglo judicial, el recurso a organismos o acuerdos regionales u otros medios pacíficos de su elección" (Organización de las Naciones Unidas, 1945). El artículo 33.2 establece que el Consejo de Seguridad tiene el poder de pedir a los Estados parte de una controversia internacional que la solucionen mediante el empleo de medios pacíficos (Organización de las Naciones Unidas, 1945). Asimismo, la Carta otorga al Consejo una serie de competencias consistentes en: la investigación de las controversias por iniciativa propia o a petición de un Estado; la labor de mediador en relación a dichas situaciones (artículo 36) e incluso de conciliador en caso de que las partes no logren poner fin a la controversia por medios pacíficos (artículo 37) (Organización de las Naciones Unidas, 1945).

El principio relativo a la libertad de elección del medio de arreglo de la controversia implica que pesa sobre los Estados una obligación de comportamiento consistente en llegar a una solución de la controversia, lo que implica que no recae sobre ellos una obligación de resultado (Pastor Ridruejo, 2013, pág. 576). La vigencia de este principio en el Derecho Internacional Clásico fue corroborada por el Tribunal de la Haya en el asunto del Estatuto de Carelia Oriental en el año 1923, en el cuál estableció que dicha regla se constituía como "principio fundamental de Derecho Internacional" por el cual los Estados gozan de independencia en la elección de los medios de arreglo de controversias (Sentencia de 23 de julio de 1923 relativa al asunto del Estatuto de la Carelia Oriental, 1923). El artículo 33 de la Carta, como se ha expuesto en este

apartado, confirma la preservación de dicha norma en el Derecho Internacional Contemporáneo.

Tradicionalmente, los medios pacíficos de arreglo de controversia se clasifican en dos categorías, en virtud de la naturaleza de los mismos. En primer lugar, los Estados pueden acudir a los medios no jurisdiccionales, también llamados medios diplomáticos o políticos, de solución de controversias (Díez de Velasco, 2017). Estos incluyen las negociaciones diplomáticas, mediación, buenos oficios, investigación de los hechos y conciliación (Pastor Ridruejo, 2013, pág. 592). En segundo lugar, los Estados pueden recurrir a los medios jurisdiccionales de arreglo de controversias: el arbitraje y el arreglo judicial (Pastor Ridruejo, 2013, pág. 592).

En el contexto de la Unión Europea, frente a las amenazas de ciberataques impulsados por Estados, así como de otras formas de ciberdelincuencia, se han llevado a cabo esfuerzos dirigidos a afrontarlas a través de medios pacíficos. Desde la Unión Europea se ha llamado fuertemente a la coordinación entre los Estados Miembros; un ejemplo concreto se aprecia en el Informe emitido por la Comisión de Asuntos Exteriores del Parlamento Europeo, (Informe del 25 de mayo de 2018, de la Comisión de Asuntos Exteriores, sobre ciberdefensa). En dicho documento se pide a los Estados que impulsen "una mayor aplicación del enfoque común y global de la Unión en materia de ciberdiplomacia y de las normas existentes en relación con el ciberespacio" (Informe del 25 de mayo de 2018, de la Comisión de Asuntos Exteriores, sobre ciberdefensa). Además, en dicho informe se llama a los Estados a elaborar una serie de criterios y definiciones a escala de la Unión Europea en relación al concepto de ciberataque, con el fin de aumentar las capacidades de la Unión de elaborar respuestas rápidas y eficaces frente a los mismos (Informe del 25 de mayo de 2018, de la Comisión de Asuntos Exteriores, sobre ciberdefensa). El enfoque desde la Unión Europea en el instrumento de la ciber diplomacia se materializa en otras actuaciones tales como la aprobación de documentos como las "Conclusiones del Consejo sobre un marco para una respuesta diplomática conjunta de la UE a las actividades informáticas malintencionadas («conjunto de instrumentos de ciberdiplomacia»), de 19 de junio de 2017. También destaca el Reglamento del Consejo, de 17 de mayo de 2019, relativa a medidas restrictivas contra los ciberataques que amenacen a la Unión o a sus Estados miembros, por el cual se establece un marco de actuación que permite la puesta en marcha de una serie de medidas restrictivas como método de contrarrestar los ciberataques (Reglamento, de 17 de mayo de 2019, del Consejo de la Unión Europea, relativa

a medidas restrictivas contra los ciberataques que amenacen a la Unión o a sus Estados miembros, 2019).

Los mecanismos de ciber diplomacia se encuentran en una etapa temprana de desarrollo, y requieren una fuerte dimensión de cooperación interestatal, de concertación de compromisos diplomáticos (Chipana, 2019). Es necesario un esfuerzo por parte de los Estados dirigido a la firma de acuerdos relativos a la seguridad cibernética, con objeto de coordinar la normativa y armonizar el marco jurídico en ámbitos como la cooperación policial y judicial en casos de ataques a través del ciberespacio (Chipana, 2019). El primer tratado internacional dirigido a poner fin a los delitos informáticos es el Convenio sobre cibercriminalidad, o Convenio de Budapest, de 23 de noviembre de 2001, ratificado por España el 1 de octubre de 2010 (Instrumento de Ratificación del Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001 (BOE 17 de septiembre de 2010)). La respuesta institucional de la Unión incluye el establecimiento en el año 2013 de un Centro Europeo del Cibercrimen en Europol, como punto central en la lucha contra la cibercriminalidad y con el objetivo de reaccionar más rápidamente a los ciberataques en la red (Europol, 2013).

b. El empleo de la fuerza

La Carta de las Naciones Unidas establece dos excepciones a la prohibición del uso de la fuerza, expuestas en un apartado anterior. La primera se establece en el artículo 42; la segunda se encuentra en el artículo 51, y se trata del derecho a la legítima defensa individual o colectiva de los Estados (Organización de las Naciones Unidas, 1945). Cuando un ciberataque pueda clasificarse como una violación de la prohibición del uso de la fuerza establecida en el artículo 2(4) de la Carta, los Estados tienen la posibilidad de reaccionar ejerciendo su correspondiente Derecho a la legítima defensa (Organización de las Naciones Unidas, 1945).

El ámbito de aplicación de este artículo es sujeto de debate en la comunidad internacional (Barkham, 2001). Algunos autores se decantan por una interpretación estricta del artículo 51, argumentando que el derecho a la legítima defensa no se activa hasta que el Estado sufre un ataque armado (Condron, 2007, pág. 421). Siguiendo esta línea de pensamiento, un Estado no podría actuar antes de que tuviera lugar el ataque (ejerciendo la denominada legítima defensa preventiva) (Condron, 2007, pág. 421). La propia Corte Internacional de Justicia avaló esta interpretación en el Caso relativo a las actividades militares y paramilitares de Nicaragua y contra ella (1986), al establecer que “ya fuera individual o colectiva, la legítima defensa sólo

podía ejercerse como reacción a un ataque armado" (Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v United States), 1986, párr. 200). Asimismo, la interpretación más estricta del artículo 51 de la Carta fue reafirmada por la Corte en su fallo dictado en relación al asunto relativo a las plataformas petrolíferas (la República Islámica del Irán contra los Estados Unidos de América) el 6 de noviembre del año 2003. En este caso, Estados Unidos alegó su derecho a la legítima defensa para justificar el bombardeo a ciertas plataformas petrolíferas en Irán, y la Corte estableció lo siguiente:

> Ninguna disposición de esta Carta menoscabará el derecho inmanente de legítima defensa, individual o colectiva, en caso de ataque armado contra un Miembro de las Naciones Unidas, hasta tanto que el Consejo de Seguridad haya tomado las medidas necesarias para mantener la paz y la seguridad internacionales. Las medidas tomadas por los Miembros en ejercicio del derecho de legítima defensa serán comunicadas inmediatamente al Consejo de Seguridad, y no afectarán en manera alguna la autoridad y responsabilidad del Consejo conforme a la presente Carta para ejercer en cualquier momento la acción que estime necesaria con el fin de mantener o restablecer la paz y la seguridad internacionales (Case Concerning Oil Platforms (Islamic Republic Of Iran V. United States Of America), 2003).

Otros autores defienden la visión contraria, defendiendo que en determinadas circunstancias los Estados pueden utilizar el empleo de la fuerza antes de que se produzca un ataque armado (Arend & Beck, 2014, pág. 79) (Taft, 2005, pág. 659). El autor Thomas M. Franck apoya esta última postura y critica la interpretación estricta del artículo 2(4) de la Carta de las Naciones Unidas, estableciendo que una lectura literal de dicha disposición implicaría exigir que un Estado debe esperar a que se produzca un ataque nuclear real antes de emplear el uso de la fuerza como medida, y no es razonable esperar que un estado se disponga a cumplir con los términos de la Carta aun cuando ello suponga su destrucción total (Frank, 1970, pág. 809).

La creación de nuevas armas modernas, como las armas cibernéticas, ha creado nuevas complicaciones para los Estados en el contexto del cumplimiento relativo a la excepción de legítima defensa de la Carta (Gervais, 2012, pág. 543). El autor Gervais ilustra el argumento a favor de la legítima defensa preventiva con el siguiente ejemplo: cuando se redactó la Carta, todavía no se habían desarrollado armas de destrucción masiva, y los ataques no podían alcanzar la destrucción generalizada que permiten las armas modernas. Hoy en día, si los estados se ven obligados a un estricto cumplimiento del artículo 51, corren el riesgo de la aniquilación total (Gervais, 2012, pág. 453). ´

Aquellos autores que defienden esta postura se apoyan en las normas de Derecho consuetudinario para la determinación de aquellas situaciones en que puede invocarse la legitima defensa preventiva (Condron, 2007, pág. 412). El Derecho internacional

consuetudinario confiere a los Estados el derecho a la legítima defensa, abarcando un derecho de uso de la fuerza preventivos (Jennings, 2017, pág. 82). Dicha norma consuetudinaria comenzó a acuñarse en el llamado "incidente *Caroline*".

El incidente *Caroline* se remonta a principios del siglo XIX, cuando Canadá todavía se encontraba bajo dominio británico y los ataques contra los británicos se llevaban a cabo en todo el país. En el año 1837, un grupo de soldados británicos entraron en Estados Unidos desde Canadá, con el objetivo de destruir el barco americano *Caroline*. El barco fue incendiado, y los británicos justificaron sus acciones invocando el derecho a la defensa propia, argumentando que el barco *Caroline* continuaría proviniendo suministros a los rebeldes canadienses. El entonces Secretario de Estado estadounidense Daniel Webster declaró que para que el Estado británico pudiera reivindicar dicho derecho, debía probar la existencia de una "necesidad de autodefensa, instantánea, abrumadora, no dejando elección de los medios y no existiendo momento para deliberar" (Webster, 1842). Incluso cuando se cumplen dichos elementos, la fuerza empleada no puede ser "irrazonable o excesiva; ya que el acto, justificado por la necesidad de defensa propia, debe estar limitado por esa necesidad, y mantenerse de forma clara dentro de ella" (Webster, 1842).

El artículo 51 de la Carta establece cuatro condiciones necesarias para que se dé el derecho de legítima defensa. Si dichos requisitos no se cumplen, el derecho de legítima defensa no existe y el Estado podría incurrir en responsabilidad internacional por violación del artículo 2.4 de la Carta (Regueiro Dubra, 2012, pág. 94). Así, en virtud del artículo 51 debe existir un ataque armado previo; la legítima defensa ha de ser provisional y subsidiaria a la acción del Consejo de Seguridad; y el Estado tiene la obligación de informar al Consejo de Seguridad de las Naciones Unidas de las medidas tomadas (Organización de las Naciones Unidas, 1945).

En virtud del artículo 51, el derecho de legítima defensa existe "hasta tanto que el Consejo de Seguridad haya tomado las medidas necesarias para mantener la paz y la seguridad internacionales" (Organización de las Naciones Unidas, 1945). Para determinar si el Consejo ha tomado las denominadas "medidas necesarias, es necesario remitirse a las competencias del Consejo de Seguridad como órgano encargado del mantenimiento de la paz y seguridad internacionales (Organización de las Naciones Unidas, 1945). En virtud de los artículos 39 y siguientes, el Consejo puede adoptar medidas provisionales (artículo 40); medidas que no implican el uso de la fuerza (artículo 41); y medidas que conllevan el uso de la fuerza armada (artículo 42) (Organización de las Naciones Unidas, 1945).

El derecho consuetudinario a la legítima defensa, ya sea preventiva o no, aparece para los Estados cuando se cumplen los requisitos de necesidad y proporcionalidad (Jennings, 2017, pág. 82). Para cumplir con el principio de necesidad, el Estado debe atribuir el ataque a una fuente específica, distinguir la intención del ataque, y sólo después, determinar el uso de la fuerza como respuesta apropiada al mismo (Condron, 2007, pág. 413). El requisito de necesidad implica que el uso de la fuerza invocado en virtud de la legítima defensa sea el único medio que el Estado tenga a su disposición para repeler la agresión (Regueiro Dubra, 2012, pág. 105). Este razonamiento fue empleado por la Corte en el asunto relativo a las actividades militares y paramilitares en Nicaragua y contra ello, estableciendo que el recurso a la fuerza debe ser la *ultima ratio* (Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v United States), 1986, párr. 237). La regla 14 del Manual de Tallin se refiere al requisito de la necesidad estableciendo que "la clave para el análisis de la necesidad en el contexto de un ciberataque es la imposibilidad o falta de remedios alternativas que no impliquen el uso de la fuerza" (Schmitt, Tallinn Manual on The International Law Applicable to Cyber Warfare, 2013, pág. 59).

En segundo lugar, el requisito de proporcionalidad debe proyectarse tanto en los medios como en los fines (Regueiro Dubra, 2012, págs. 106-108). En palabras del profesor Remiro Brotóns, la acción del Estado debe ser proporcionada a la "naturaleza e intensidad del ataque sufrido, y suficiente para desactivarlo" (Remiro Brotons, 2010, pág. 679). En esta línea, la profesora Raquel Regueiro Dubra, establece que es necesario asimismo evaluar la proporcionalidad en los resultados del ataque defensivo (Regueiro Dubra, 2012, págs. 106-108). El criterio de la proporcionalidad se incluye en la Regla 14 del Manual de Tallin en el cuál se establece que limita la escala, el ámbito, la duración y la intensidad de la respuesta del Estado necesaria para poner fin al ciberataque que dio lugar al derecho de la legítima defensa (Schmitt, Tallinn Manual on The International Law Applicable to Cyber Warfare, 2013, pág. 59).

En tercer lugar, el requisito de la inmediatez se trata del elemento distintivo existente la legitima defensa como respuesta a un ataque armado y las represalias, prohibidas por el Derecho Internacional (Ortega Carcelén, 1991, pág. 81). En palabras de Ortega Carcelén, "todo uso de la fuerza que se lleve a cabo sin conexión temporal con el ataque armado previo deberá siempre ser catalogado como represalia" (Ortega Carcelén, 1991, pág. 82). En la misma línea, la regla 15 del Manual de Talín establece que a pesar de que el artículo 51 de la Carta no incluye expresamente la legítima defensa anticipatoria, un Estado puede defenderse una vez el ataque

es “inminente” (CCDCOE, 2013, pág. 60). Dicha postura se base en el standard de inminencia originado en el incidente *Caroline,* explicado anteriormente.

El derecho de los Estados a la legítima defensa individual o colectiva consagrado en el artículo 51 de la Carta tan sólo puede ser alegado frente a ataques armados efectuados por otro Estado. El ejercicio del derecho de la legítima defensa tan sólo puede ser invocado y ejecutado frente a un ente estatal, por lo que necesariamente el ataque armado que se produzca debe ser atribuible a un Estado concreto (Regueiro Dubra, 2012, pág. 95). Ello implica que frente a un ciberataque llevado a cabo por un individuo de otro Estado, el atacado debe solicitar al gobierno del que el sujeto es nacional para que ponga fin a dicha conducta, a no ser que la provocación pueda atribuirse a un agente del Estado en cuestión (U.S Department of Defense, 1999, pág. 22). Dadas las oportunidades que el ciberespacio ofrece para la comisión de ataques en remoto y el anonimato de los atacantes, la probabilidad de que los autores de los ciberataques no sean identificados es alta (Brenner, 2007, pág. 380)

La cuestión de la atribución cobra importancia en este contexto ya que las normas relativas a la respuesta permitida a los Estados varían dependiendo de si el atacante es un actor estatal o un actor no estatal (Condron, 2007, pág. 414) (Jensen, 2002, págs. 232-233). El artículo 2(4) de la Carta de las Naciones Unidas se aplica a los Estados, y no a individuos (Jensen, 2002, pág. 232). Por consiguiente, el Derecho internacional impide a los Estados amenazar o utilizar la fuerza entre sí, mientras que los actos realizados por los individuos caen dentro del ámbito doméstico de cada Estado (Jensen, 2002, págs. 232-233). Siguiendo la visión de los autores Condron y Creekman, el marco jurídico internacional actual limita las opciones de respuesta de los Estados, dificultando la elaboración de una respuesta eficaz que no implique una violación del Derecho internacional (Condron, 2007, pág. 415) (Creekman, 2002, págs. 668-669).

Toda vez que un Estado víctima de un ataque se ampara en el derecho a la legítima defensa, este puede ejercer su poder en el territorio del Estado atacante. Los principios que actúan como límites al principio de soberanía quedan, en estas situaciones, suspendidos puesto que el Estado puede usar la fuerza para defenderse del ataque sufrido, violando la soberanía de aquel que atacó primero. Ello ocurre también en el ámbito del ciberespacio, donde los Estados pueden actuar sobre el dominio de otro Estado a través de operaciones cibernéticas.

En todo caso, actualmente no existe acuerdo en relación al umbral a partir del cual una operación cibernética se considera ataque armado, dando lugar a la activación de la excepción a la prohibición del uso de la fuerza contemplada en el artículo 51 de la Carta de las Naciones Unidas (Solano Díaz, 2014). Como establece el autor Michael N. Schmitt, se trata de una decisión política del Estado víctima, decisión que debe ser razonable a la luz de los modelos que se han explicado en este apartado (Schmitt, 2010).

5. CONCLUSIONES

El presente documento de investigación ha realizado un recorrido por el principio de soberanía como norma *ius cogens* en Derecho internacional, y se ha detenido especialmente en los principios de igualdad soberana y no injerencia en los asuntos internos de otros Estados. La fórmula tradicional de la soberanía estatal históricamente se apoyaba en una serie de elementos (territorio delimitado, gobierno, población determinada y capacidad de entrar en relación con otros Estados) que se sumaban para dar lugar a un Estado, sujeto de Derecho internacional, con poderes soberanos inherentes a él. Sin embargo, nuevos factores han entrado en el escenario en que el Derecho internacional se proyecta, y de ellos emanan nuevos desafíos para esta disciplina. El rápido desarrollo de las nuevas tecnologías, sumado a la globalización y al acceso universal a internet han dado lugar al desarrollo de un nuevo espacio relacional, el ciberespacio. El ciberespacio como nuevo dominio del Estado supone la extensión de su soberanía, y a través del recorrido por distintos artículos y opiniones doctrinales, en el presente apartado se presentan una serie de conclusiones finales.

En primer lugar, el principio de soberanía, que ha encontrado tradicionalmente su máxima expresión en el territorio de cada Estado, en la actualidad se proyecta también sobre el ámbito del ciberespacio. Existe un consenso doctrinal sobre la aplicación de la soberanía en el ciberespacio, relativa a la existencia de una prohibición impuesta a los Estados de llevar a cabo operaciones cibernéticas que violen la soberanía de otro Estado. El carácter innovador de la tecnología que subyace tras el ciberespacio no obstaculiza la aplicabilidad del principio de soberanía a los componentes y a las actividades de este. En la misma línea, la gran mayoría de normas y principios del Derecho internacional consuetudinario se aplican al ciberespacio y a las actividades cibernéticas.

Los Estados pueden ejercer sus competencias soberanas en el ciberespacio, sin embargo, deben aceptar las correspondientes obligaciones que ello conlleva. Se trata de los límites tradicionales

del principio de soberanía: la igualdad soberana y el principio de no injerencia en asuntos internos. La extensión del principio de soberanía aplicado en el ciberespacio implica que los Estados tienen derecho a proyectar su poder en este ámbito de acuerdo con sus propios objetivos y recursos. El principio de no intervención viene de la mano con su soberanía: de este modo, los Estados están obligados a reconocer la soberanía del resto de Estados y no interferir con las decisiones tomadas por estos en su ámbito doméstico en relación con operaciones cibernéticas. De este modo, un Estado no puede tratar de restringir o limitar los poderes de otro Estado en el ciberespacio, o tratar de disminuir sus capacidades.

Sin perjuicio de la plena eficacia del principio de no intervención en asuntos internos de otros Estados en el ámbito cibernético, los Estados pueden establecer acuerdos entre ellos para establecer límites en el desarrollo de sus capacidades. A través de acuerdos bilaterales o multilaterales entre Estados, estos pueden cooperar para elaborar unas líneas de actuación comunes en el ámbito del ciberespacio. En este contexto de cooperación, como en todo tratado internacional, impera la obligación de negociar de buena fe y cumplir con los compromisos internacionales de los que los Estados son parte.

En segundo lugar, el principio de igualdad soberana mantiene su eficacia en el ciberespacio, en el cual cada Estado ejerce sus competencias en un plano de igualdad con respecto al resto de Estados. Sin perjuicio de las diferencias en las capacidades de cada Estado, todos poseen el mismo poder soberano sobre su territorio. Las operaciones cibernéticas que los Estados pueden llevar a cabo deben respetar los derechos derivados del carácter soberano de los demás Estados. El principio de igualdad soberana plantea cuestiones que requieren la atención de la comunidad internacional. Se ha concluido que cada Estado puede decidir libremente las operaciones cibernéticas que decide realizar, siempre que no constituya una violación de la soberanía de otro Estado. Sin embargo, la cuestión de la cooperación en el ámbito del ciberespacio cobra especial importancia, en especial con relación a Estados con menos capacidades tecnológicas. Se trata de una labor pendiente para la comunidad internacional: hallar el balance entre el respeto al principio de soberanía estatal en el ciberespacio y los beneficios que se obtendrían del intercambio de información y sistemas de seguridad en la red. No existe hoy en día obligación respecto a colaborar activamente en dichos mecanismos de cooperación.

En tercer lugar, esta investigación se ha centrado en el estudio de una particular amenaza que se cierne sobre los Estados en el ciberespacio: los ciberataques. Las acciones dirigidas a lesionar o casuar daños en forma de ciberataques pueden llevarse a cabo de distintas formas.

En este documento se han recogido los distintos criterios empleados por los Estados para determinar si un ciberataque puede considerarse un uso de la fuerza, constituyendo una violación a la prohibición del uso de la fuerza consagrada en el artículo 2.4 de la Carta de las Naciones Unidas. En este aspecto, concluimos que actualmente no existe acuerdo en relación con el umbral a partir del cual una operación cibernética se considera ataque armado. Se trata de una decisión política del Estado víctima, y esta debe ser razonable a la luz de los criterios expuestos.

Cuando se equipara un ciberataque a un uso de la fuerza que viola la prohibición consagrada en el artículo 2.4, la propia Carta establece los modos de reacción de los Estados, aplicables a su vez en el contexto del ciberespacio. Ellos son, como se explica a lo largo del trabajo: la solución de controversias a través del empleo de medios pacíficos; la autorización del Consejo de Seguridad bajo el amparo del artículo 42 de la Carta; y el ejercicio al derecho de la legítima defensa amparado en el artículo 51 de la Carta.

En relación con la solución de controversias, la obligación impuesta por el Derecho Internacional consiste en que deben procurar llegar a una solución justa y rápida es aplicable al ámbito del ciberespacio. La resolución del conflicto por medios pacíficos debe priorizarse frente al recurso al uso de la fuerza, como consagra el artículo 33 de la Carta. En este sentido, en el ámbito del ciberespacio cobran importancia la realización de acuerdos relativos a la seguridad cibernética y el compromiso por parte de los estados de apoyar iniciativas de cooperación en el desarrollo de mecanismos como la ciber diplomacia.

El derecho a la legítima defensa de los Estados constituye otro de los medios de reacción de los Estados frente a un ciberataque que pueda equipararse a un uso de la fuerza frente a un Estado. En esta investigación se establece la conexión entre el derecho a la legítima defensa de un Estado y la lesión de su soberanía en el ciberespacio. Un Estado cuya soberanía ha sido violada a través del uso de la fuerza en el ciberespacio, tiene derecho a responder a dicho ciberataque empleando la fuerza en virtud de su derecho a la legítima defensa, sin perjuicio de los requisitos que deben cumplirse para que este tenga lugar y no sea considerado represalia. Así las cosas, una vez se cumplen los requisitos descritos en este documento de trabajo, y el Estado víctima puede ampararse en su derecho a la legítima defensa y ejercer la fuerza frente al Estado atacante, parece ser que los límites de su soberanía se disipan, pudiendo el Estado víctima del ciberataque ejercer su poder en el territorio del Estado atacante. Los límites derivados del Derecho internacional consuetudinario en relación con el derecho a la legítima

defensa cobrarían eficacia en ese momento: la proporcionalidad, necesidad e inmediatez. De este modo, en el ámbito de la legítima defensa en el ciberespacio podríamos concluir que los principios que limitan la soberanía estatal se difuminan, y el Estado puede usar la fuerza para defenderse del ataque sufrido, violando la soberanía de aquel que atacó primero.

Para concluir, la presente investigación muestra los desafíos legales que presenta la aparición del ciberespacio como nuevo dominio estatal. La soberanía de los estados constituye un ámbito vulnerable a las incertidumbres que existen con respecto a las operaciones cibernéticas. A lo largo de la presente investigación se ha arrojado luz sobre la cuestión de la soberanía estatal en el ciberespacio, estableciendo que los límites tradicionales del principio de soberanía se mantienen firmes en este nuevo espacio relacional, y las posibles respuestas de los estados frente a una violación de la soberanía a través del uso de la fuerza en forma de ciberataque. Asimismo, se ha subrayado la importancia de la cooperación interestatal dirigida a la elaboración de directrices y criterios claros en relación con el régimen legal aplicable en el ciberespacio, así como al establecimiento de acuerdos en relación con la solución de controversias que tengan lugar en dicho dominio.

6. BIBLIOGRAFÍA

I. Doctrina

- Arend, A. C., & Beck, R. J. (2014). International Law and the Use of Force: Beyond the UN Charter Paradigm. Routledge.

- Barberis, J. A. (1973). Nouvelles questions concernant la personnalité juridique internationale. Ginebra: Recueil des cours.

- Barboza, J. (1999). Derecho Internacional Público. Buenos Aires: Zavalía. Recuperado el 1 de Febrero de 2020

- Barkham, J. (2001). Information Warfare and International Law on the Use of Force. New York University Journal of International Law and Politics.

- Black, H. (2009). Black´s Law Dictionary (9º ed.). St. Paul: West Group.

- Bodin, J. (1576). De la República I.

- Brenner, S. (2007). 'At Light Speed' - Attribution and Response to Cybercrime/Terrorism/Warfare. Journal of Criminal Law and Criminology , 97, 350-400.

- Brotons, A. R. (1982). Derecho Internacional Público: Principios Fundamentales. Madrid: Tecnos.

- Brownlie, I. (2002). International Law and the Use of Force by States: Revisited. Ginebra: Chinese Journal of International Law. Recuperado el 3 de Marzo de 2020, de https://doi.org/10.1093/oxfordjournals.cjilaw.a000415

- Carrillo Salcedo, J. A. (1991). Curso de derecho internacional público. Madrid: Tecnos.

- CCDCOE. (2013). Tallinn Manual on The International Law Applicable to Cyber Warfare. NATO

- Condron, S. M. (2007). Getting it Right: Protecting American Critical Infrastructure in Cyberspace. Harvard Journal of Law & Technology, 20(2), 404-421. Recuperado el 2 de Marzo de 2020, de http://jolt.law.harvard.edu/articles/pdf/v20/20HarvJLTech403.pdf

- Cornish, P., Livingstone, D., Clemente, D., & Yorke, C. (2010). On Cyber Warfare. Londres: Chatam House (The Royal Institute of International Affairs). Recuperado el 15 de Febrero de 2020, de https://www.chathamhouse.org/sites/default/files/public/Research/International%20Security/r1110_cyberwarfare.pdf

- Creekman, D. M. (2002). A Helpless America? An Examination of the Legal Options Available to the United States in Response to Varying Types of Cyber-Attacks from China. American University International Law Review, 17(2), 641-681.

- Díez de Velasco, M. (2017). Instituciones de derecho internacional público. Madrid: Tecnos. Recuperado el 3 de Enero de 2020.

- Publicación Doctrinal Conjunta PDC-01(A) de 2008 [Ministerio de Defensa]. Doctrina para el empleo de las Fuerzas Armadas.

- Frank, T. M. (1970). Who Killed Article 2(4)? or: Changing Norms Governing the Use of Force by States. The American Journal of International Law, 809-820.

- Franzese, P. W. (2009). Sovereignty in Cyberspace: can it exist? Air Force Law Review, 64, 1-26. Recuperado el 2 de Febrero de 2020, de

https://www.law.upenn.edu/live/files/3473-franzese-p-sovereignty-in-cyberspace-can-it-exist

- Gervais, M. (2012). Cyber Attacks and the Laws of War. Berkeley Journal of International Law, 525-579.

- Giraldo, S. M. (2017). Análisis de las infraestructuras críticas en la era de las ciberguerras en búsqueda del delicado equilibrio entre libertad y seguridad. Universidad Militar Nueva Granada.

- González, M. P. (1995). Las Naciones Unidas y el mantenimiento de la paz: cincuenta años de esfuerzos. Cuadernos de Historia Contemporánea(17), 61-78. Recuperado el 10 de febrero de 2020, de https://revistas.ucm.es/index.php/CHCO/article/view/CHCO9595110061A

- Heinegg, W. H. (2012). Legal Implications of Territorial Sovereignty in Cyberspace. 4th International Conference on Cyber Conflict (págs. 7-19). Tallinn: NATO CCD COE Publications. Recuperado el 3 de Febrero de 2020, de https://www.ccdcoe.org/uploads/2012/01/1_1_von_Heinegg_LegalImplicationsOfTerritorialSovereigntyInCyberspace.pdf

- Jennings, R. Y. (2017). The Caroline and McLeod Cases. Cambridge University Press.

- Jensen, E. T. (2002). Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right to Self-Defense. Stanford Journal of International Law, 38, 207-240.

- Joyner, C. C., & Lotrionte, C. (2001). Information Warfare as International Coercion: Elements of a Legal Framework. European Journal of International Law, 825-865.

- Khanna, P. (2018). State Sovereignty and Self-Defence in Cyberspace. Brics Law Journal, 5(4), 139-154. Recuperado el 20 de Febrero de 2020, de https://www.bricslawjournal.com/jour/article/view/197/131

- Lessig, L. (2001). El código y otras leyes del ciberespacio. Madrid: Taurus.

- Libicki, M. C. (2009). Cyberdeterrance and Cyberwar. Santa Monica, California: RAND Corporation. Recuperado el 12-28 de Enero de 2020, de https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf

- Machín, N., & Gazapo, M. (2016). La ciberseguridad como factor crítico en la seguridad de la Unión Europea. UNISCI, 47-68.

- McWhinney, E. (1979). nternational Law Antinomies And Contradictions Of An Era Of Historical Transition: Retrospective On The Nato Armed Intervention In Kosovo. En E. McWhinney, Estudios de Derecho Internacional. Homenahe al Profesor Miaja de la Muela (pág. 407). Madrid: Tecnos.

- Montgomery, M. (2019). Proliferation of cyberwarfare under international law: virtual attacks with concrete consequences. Southern California Interdisciplinary Law Journal, 28(2), 499-521.

- N. R. Council, Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy (págs. 151-178). Washington, D.C: The National Academies Press.

- Oppenheim, L., & Lauterpacht, H. (1944). International Law. A Treatise. Londres: Longmans, Green & Co.

- Ortega Carcelén, M. (1991). La legítima defensa del territorio del Estado. Requisitos para su ejercicio. Madrid: Tecnos.

- Owens, W. A., Dam, K. W., & Lin, H. S. (2009). Technology, Policy, Law, and Ethics Regarding U. S. Acquisition and Use of Cyberattack Capabilities. National Academies Press.

- Pastor Ridruejo, J. A. (2013). Curso de Derecho Internacional Público y Organizaciones Internacionales. Madrid: Tecnos.

- Raboin, B. (2011). Corresponding Evolution: International Law and the Emergence of Cyber Warfare. Journal of the National Association of Administrative Law Judiciary. Recuperado el 10 de Febrero de 2020, de https://books.google.es/books/about/Corresponding_Evolution_International_La.html?id=n0zAoQEACAAJ&redir_esc=y

- Regueiro Dubra, R. R. (2012). La legítima defensa en Derecho Internacional. Instituto Universitario General Gutiérrez Mellado - UNED.

- Reisman, M., & Baker, J. (2011). Regulating Covert Action: Practices, Contexts, and Policies of Covert Coercion Abroad in International and American Law. Yale University Press.

- Remiro Brotons, A. R. (2010). Derecho Internacional. Curso General. Tirant Lo Blanch.

- Ress, G. (2002). Interpretation of the Charter. En B. Simma, H. Hermann Mosler, & A. Randelzhofer, The Charter of the United Nations: A Commentary. Nueva York: Oxford University Press.

- Salinas Macías, J. A. (2015). El Uso de la Fuerza en el Ciberespacio. Revista Perspectiva Jurídicas, 229-257.

- Schmitt, M. N. (2007). Grey Zones in the International Law of Cyberspace. The Yale Journal of International Law, 1-21.

- Schmitt, M. N. (2010). Cyber Operations in International Law: The Use of Force, Collective Security, Self Defense and Armed Conflicts.

- Schmitt, M. N. (2011). Cyber Operations and the Jus ad bellum Revisited. Villanova Law Review, 578-581.

- Schmitt, M. N. (2013). Cyberspace and International Law. Harvard Law Review Forum, 178.

- Schmitt, M. N. (2014). The law of cyber warfare: quo vadis? Standford Law & Policy Review, 25. Recuperado el 15 de Debrero de 2020, de https://law.stanford.edu/publications/law-cyber-warfare-quo-vadis/

- Schmitt, M. N. (Ed.). (2017). Tallin Manual 2.0 on the International Law Applicable to Cyber Operations. Newport, Rhode Island: Cambridge University Press.

- Sebenius, A. (28 de Junio de 2017). Writing the rules of cyberware. The Atlantic. Recuperado el 5 de Febrero de 2020, de https://www.theatlantic.com/international/archive/2017/06/cyberattack-russia-ukraine-hack/531957/

- Shackelford, S. J. (2009). From Nuclear War to Net War: Analogizing Cyber Attacks in International Law. Berkeley Journal of International Law, 202-208.

- Sharp, W. G. (1999). Cyberspace and the Use of Force. Aegis Research Corporation.

- Stone, J. (1958). Agression and World Order: A Critique of United Nations theories of agression. The American Journal of International Law, 364-366.

- Taft, W. H. (2005). International Law and the Use of Force. Georgetown Journal of International Law, 650-660.

- Tamkin, E. (27 de Abril de 2017). 10 Years After the Landmark Attack on Estonia. Is the World Better Prepared for Cyber Threats? Foreign Policy. Recuperado el 2 de Febrero de 2020, de https://foreignpolicy.com/2017/04/27/10-years-after-the-landmark-attack-on-estonia-is-the-world-better-prepared-for-cyber-threats/

- Truyol y Serra, A. (1999). Theorie du droit international public. Paris: Recueil des Cours. Recuperado el 7 de Enero de 2020

- Waldock, C. Y. (1952). The regulation of the use of force by individual States in International Law. Paris: R. des C.

II. Normativa y jurisprudencia

- *Island of Palmas Case (Netherlands v USA*) [1928] ICJ Rep 2.

- *Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v United States),* [1986] ICJ Rep 14.

- *Case Concerning Oil Platforms (Islamic Republic Of Iran V. United States Of America),* [2003] ICJ.

- *Corfu Channel Case (United Kingdom v Albania),* Merits, [1949] ICJ Rep 4.

- Convención de Viena sobre el Derecho de los Tratados, 23 de Mayo de 1969.

- Estatuto de Roma de la Corte Penal Internacional. 17 de Julio de 1998. Recuperado el 20 de Marzo de 2020, de https://www.boe.es/buscar/doc.php?id=BOE-A-2002-10139

- Ley 8/2011 de 2011. Por la que se establecen medidas para la protección de las infraestructuras críticas. 28 de abril de 2011. BOE-A-2011-7630.

- Orden Ministerial 10/2013 de 2013 [Ministerio de Defensa del Reino de España]. Por la que se crea el Mando Conjunto de Ciberdefensa de las Fuerzas Armadas. 19 de febrero de 2013. BOE-A-2015-1232

- Organización de las Naciones Unidas. (1945). Carta de las Naciones Unidas. San Francisco.

- Protocolo Adicional a los Convenios de Ginebra de 1949, relativo a la protección de las víctimas de los conflictos armados internacionales (1977).

III. Documentos Oficiales

- A/RES/2625(XXV) de 24 de octubre de 1970.

- A/RES/29/3314 de 14 de diciembre de 1974.

- A/RES/53/70 de 4 de enero de 1999.

- A/RES/56/83 de 12 de diciembre de 2001.

- Asamblea General de las Naciones Unidas. (2000). Nosotros Los Pueblos: la Función de las Naciones Unidas en el Siglo XXI. Informe del Secretario General Kofi Annan presentado para La Cumbre del Milenio. Resolución A/54/2000.

- Cartwright, J. E. (2011). Joint terminology for cyberspace negotiations. Washington, D.C.: U.S. Department of Defense.

- Department of Defense Dictionary of Military and Associated Terms. (2010). Joint Publication (JP) 1-02. Recuperado el 20 de enero de 2020, de http://www.dtic.mil/doctrine/dod_dictionary

- International Strategy for Cyberspace. (2011). Washington, D.C.: United States. White House Office. Recuperado el 3 de enero de 2020, de https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

- Opinión consultiva de 8 de julio de 1996 sobre legalidad de la amenaza y uso de armas nucleares, A/51/218 (Corte Internacional de Justicia 8 de Julio de 1996).

- Reglamento sobre la ciberseguridad, 2019/881 (Parlamento Europeo y Consejo Europeo 17 de abril de 2019).

- Secretaria General del Consejo de la Unión Europea. (2013). Conclusiones del Consejo sobre la comunicación conjunta de la Comisión y de la Alta Representante de la Unión para Asuntos Exteriores y Política de Seguridad. Bruselas.

- Summary Report of Eleventh Meeting of Committee I/1. U.N.C.I.O. (1945).

- U.S Department of Defense. (1999). An Assesment of International Legal Issues in Information Operations. U.S Department of Defense.

- Webster, D. (1842). Letter from Mr. Webster to Lord Ashburton, August 6, 1842. En R. Y. Jennings, The Caroline and McLeod Cases (Vol. 32, págs. 82-99). Cambridge University Press.