DERECHO INTERNACIONAL HUMANITARIO

IUS AD BELLUM EN EL CIBERESPACIO: EL EJERCICIO DEL DERECHO A LA LEGÍTIMA DEFENSA

IUS AD BELLUM IN CYBERSPACE: THE EXERCISE OF THE RIGHT TO SELF-DEFENSE

Autor: *César Ramos Rojas*[1]

RESUMEN

El presente artículo pretende determinar cómo los Estados deben ejercer el derecho a la legítima defensa en el ciberespacio, debido a que es un tema vital para la paz y la seguridad global que ha adquirido relevancia en los últimos años.

Con este fin, el presente artículo parte de la introducción presentando las preguntas que pretende absolver, el propósito y el alcance de su contenido y su estructura. En el segundo capítulo, se analiza la regulación del uso de la fuerza en el derecho internacional para determinar su concepción actual, que permite su empleo mediante la legítima defensa. El tercer capítulo aborda este derecho inmanente de la legítima defensa detallando los requisitos que deben cumplirse para su correcto ejercicio conforme al derecho internacional, desde las condiciones que establece la Carta de las Naciones Unidas hasta las dispuestas por el derecho consuetudinario. Posteriormente, en el cuarto capítulo se presenta el ciberespacio y su relación con el uso de fuerza, brindando una definición de este entorno, examinando el uso militar que ha adquirido mediante los ciberataques y la aplicación del Derecho Internacional.

1) Cesar Ramos Rojas. Asistente de Investigación en derecho internacional en la Universidad del Pacífico. Lima, Perú. Bachiller en Derecho por la Pontificia Universidad Católica del Perú. Email: cesar.ramosr@pucp.edu.pe. 0009-0002-8625-4361.

En el capítulo 5 se analiza el ejercicio del derecho a la legítima defensa en el ciberespacio. A tal efecto, se analiza el cumplimiento de los requisitos establecidos en la Carta de las Naciones Unidas y en el derecho consuetudinario considerando las particularidades propias del ciberespacio, particularmente, de los ciberataques. Finalmente, el Capítulo 6 brinda las conclusiones del artículo y se formulan ciertas sugerencias por parte del autor para asegurar la aplicación del derecho internacional, particularmente las normas que regulan el uso de la fuerza, en el ciberespacio.

Palabras clave: Uso de la fuerza / Ius ad bellum / legítima defensa / ciberespacio, ciberataque.

ABSTRACT

This article aims to determine how States should exercise the right to self-defense in cyberspace, because it is a vital issue for global peace and security that has gained relevance in recent years.

To this end, this article starts from the introduction, presenting the questions it aims to answer, the purpose and scope of its content and its structure. In the second chapter, the regulation of the use of force in international law is analyzed to determine its current conception, which allows its use through self-defense. The third chapter addresses this inherent right of self-defense, detailing the requirements that must be met for its correct exercise in accordance with international law, from the conditions established by the Charter of the United Nations to those established by customary law. Subsequently, the fourth chapter presents cyberspace and its relationship with the use of force, providing a definition of this environment, examining the military use that it has acquired through cyberattacks and the application of International Law.

Chapter 5 analyzes the exercise of the right to self-defense in cyberspace. To this end, compliance with the requirements established in the Charter of the United Nations and in customary law is analyzed, considering the particularities of cyberspace, particularly cyberattacks. Finally, Chapter Six provides the conclusions of the article and certain suggestions are made by the author to ensure the application of international law, particularly the norms that regulate the use of force, in cyberspace.

Keywords: *Use of force, Ius ad bellum / self-defense / cyberspace / cyber attack.*

CAPÍTULO 1 - INTRODUCCIÓN

El 'ius ad bellum' es un concepto del derecho internacional que se refiere al derecho que tienen los Estados de emplear la fuerza de manera legítima en determinados casos. Asimismo, al fijar condiciones y restricciones, el "ius ad bellum" también limita el recurso indiscriminado de la fuerza contribuyendo a mantener la paz internacional.

Los dos supuestos por excelencia en los que un Estado puede utilizar la fuerza en el derecho internacional contemporáneo son la legítima defensa y cuando el Consejo de Seguridad de las Naciones Unidas autoriza el uso de la fuerza. Únicamente el primer supuesto permite a un Estado utilizar la fuerza bajo su propio criterio mediante un previo análisis del derecho internacional, al menos inicialmente, a diferencia del segundo supuesto[2] [3]. Este ejercicio unilateral es vital para garantizar la soberanía, la autodefensa y la seguridad de todos los Estados, por lo que es crucial comprender el derecho de la legítima defensa conforme al derecho internacional, a fin de evitar un uso inadecuado de la fuerza que atente contra la paz y la seguridad global.

Al respecto, a lo largo de la historia se ha considerado, estudiado y codificado el derecho a la legítima defensa de los Estados teniendo como base un ataque armado que implica únicamente el uso de recursos físicos, tales como soldados, armas convencionales, vehículos militares, entre otros; que tiene consecuencias únicamente en el espacio físico. Sin embargo, la participación del ciberespacio ha aumentado gradualmente en los conflictos armados modernos desde finales del siglo XX, como ocurrió en la Guerra Civil de Georgia y la Guerra ruso-georgiana (Zahra, Handayani, & Wulan, 2021, pp. 58-59), atrayendo la atención de la comunidad internacional.

A comienzos del siglo XXI ocurrió un incidente significativo que marcó un punto de inflexión en la percepción que se tenía de un ataque armado y el ciberespacio: los ciberataques en Estonia de 2007. Este acontecimiento conllevó una serie de ciberataques dirigidos a sitios web de diversas organizaciones en Estonia, en particular el parlamento estonio, ministerios, bancos y medios de comunicación (Roscini, 2014, p. 5). Estos ciberataques se desarrollaron en medio de una discrepancia con Rusia respecto a la reubicación del Soldado de Bronce en Tallin, la capital de Estonia, y las tumbas de la era soviética.

"Los dos supuestos por excelencia en los que un Estado puede utilizar la fuerza en el derecho internacional contemporáneo son la legítima defensa y cuando el Consejo de Seguridad de las Naciones Unidas autoriza el uso de la fuerza"

2) Conforme al artículo 49 de la Carta de las Naciones Unidas.

3) Además, es necesario que ninguno de los miembros permanentes ejerza su derecho de veto.

"En la cumbre de la OTAN de 2014 en Gales, los Estados miembros de dicha organización reconocieron que el derecho internacional es aplicable al ciberespacio donde pueden invocar la defensa colectiva en respuesta a un ciberataque equivalente a un ataque armado"

Al respecto, si bien el ciberespacio es un concepto que se popularizó en la década de 1980[4], lo ocurrido en Estonia en 2007 provocó que la comunidad internacional comenzará a considerar que un ciberataque puede ser tan perjudicial como un ataque convencional y, por lo tanto, al ciberespacio como un nuevo ambiente donde puedan producirse ataques armados. En consecuencia, a lo largo de la década del 2010, aumentó el debate sobre la aplicación del Derecho Internacional en el ciberespacio, particularmente sobre su posible uso militar. Se han desarrollado normas de soft law, como las del Manual de Tallin, que abordan la aplicación del derecho internacional a los conflictos armados en el ciberespacio, centrándose particularmente en el ius ad bellum e ius in bellum (Centro de Estudios Estratégicos CEEAG, 2018, 141-142).

Asimismo, en la cumbre de la OTAN de 2014 en Gales, los Estados miembros de dicha organización reconocieron que el derecho internacional es aplicable al ciberespacio donde pueden invocar la defensa colectiva en respuesta a un ciberataque equivalente a un ataque armado (North Atlantic Treaty Organization, 2014). Sin embargo, aún no existe una norma vinculante en el derecho internacional que precise y regule cómo se aplica la legítima defensa en el ciberespacio en concreto.

Es fundamental determinar la regulación del derecho de los Estados a recurrir a la fuerza en el ciberespacio, debido a que es un ámbito que ha desempeñado un papel cada vez más relevante en los conflictos armados y seguramente su importancia irá en aumento. A modo de ejemplo, durante la invasión rusa en Ucrania en 2022, se llevaron a cabo ciberataques que resultaron en la caída de múltiples servicios gubernamentales ucranianos (Redacción Ciencia, 2022). Mediante la comprensión de su regulación, se garantiza el empleo de la fuerza conforme al derecho internacional, fundamental para la defensa de los Estados y para prevenir su uso arbitrario.

Por lo tanto, al ser un tema vital para la paz y la seguridad global, el presente artículo analiza cómo se debe entender y ejercer el derecho a la legítima defensa por parte de los Estados en el ciberespacio, un entorno factible de ser una zona de conflicto.

4) https://www.jstor.org/stable/379040

1.1. Preguntas a responder

Durante el desarrollo del artículo se abordarán y responderán las siguientes preguntas:

- ¿Cómo se regula el derecho a la legítima defensa en el derecho internacional?

  A pesar de que no existen tratados que regulen en concreto el funcionamiento del "ius ad bellum" en el ciberespacio, sí existen normas que regulan el uso de la fuerza en general, sin importar el ámbito de aplicación. Por ende, la primera parte del artículo aborda el análisis de la regulación del "ius ad bellum" en el derecho internacional, en particular el derecho a la legítima defensa, a fin de poder implementar su aplicación en el ciberespacio.

- ¿Qué es el ciberespacio y cómo se utiliza la fuerza en este entorno?

  Entre las principales dificultades que enfrentan aquellos involucrados en el debate sobre el uso de la fuerza en el ciberespacio, se encuentra la comprensión de este entorno, los ciberataques y la función que pueden desempeñar en los conflictos armados. En consecuencia, la segunda sección del artículo proporciona una conceptualización del ciberespacio y su aplicación en las hostilidades.

- ¿Cómo se ejerce el derecho a la legítima defensa en el ciberespacio?

  La tercera parte del artículo aborda el análisis del ejercicio del derecho a la legítima defensa en el ciberespacio, considerando los requisitos que se deben cumplir para su ejercicio y cómo se cumplirían en este entorno.

1.2. Propósito y alcance del artículo

Considerando las preguntas a responder, el presente artículo tiene como finalidad aclarar cuándo un Estado tiene el derecho de usar la fuerza, mediante el derecho a la legítima defensa, en el ciberespacio. En ese sentido, no es el tema central analizar la faceta del ciberespacio como ambiente de conflictos armados. Esta cuestión es un tema relevante para la paz y seguridad internacional, dada la naturaleza restrictiva del uso de la fuerza entre Estados.

Asimismo, no será objeto de estudio la función que tiene el ciberespacio para beneficio de la humanidad durante conflictos, hostilidades o ciberoperaciones, pese a su importancia y a la breve mención que se puede formular al respecto.

1.3. Estructura del artículo

El presente Capítulo 1 tiene un carácter introductorio. Ofrece un breve contexto sobre el tema que se abordará en el artículo, presenta las principales preguntas que serán respondidas y define claramente su propósito y alcance.

"A pesar de que no existen tratados que regulen en concreto el funcionamiento del ius ad bellum en el ciberespacio, sí existen normas que regulan el uso de la fuerza en general, sin importar el ámbito de aplicación"

"*ius ad bellum*, entendido como el derecho al uso de la fuerza de los Estados, es fundamental para comprender como un Estado puede legalmente utilizar la fuerza en el ciberespacio"

El Capítulo 2 aborda el ius ad bellum. En este contexto, ofrece una breve descripción de la regulación de la fuerza con el objetivo de identificar y distinguir entre el *ius contra bellum*, el *ius ad bellum* y el *ius in bellum*.

El Capítulo 3 versa sobre la legítima defensa de los Estados, explica los requisitos que regula el ejercicio de este derecho, conforme a la Carta de las Naciones Unidas y el derecho internacional consuetudinario.

El Capítulo 4 trata sobre el ciberespacio como un entorno en el que los Estados también pueden utilizar la fuerza y verse afectados por su uso. En consecuencia, se brinda una concepción del ciberespacio como un ámbito sujeto al derecho internacional, se analiza su uso militar y se ilustra dos casos que ilustran dicho uso.

En el Capítulo 5, se conectan los requisitos abordados en el Capítulo 3 para ejercer el derecho a la legítima defensa con la concepción del ciberespacio presentada en el Capítulo 4. Por lo tanto, se analiza la correcta aplicación de este derecho en el ciberespacio conforme con el derecho internacional.

En el Capítulo 6, se presentan las conclusiones del artículo, la posición del autor sobre el tema y se proponen acciones a considerar en relación con la aplicación de la legítima defensa, en particular, y el uso de la fuerza, en general, en el ciberespacio.

CAPÍTULO 2 – EL IUS AD BELLUM

La comprensión del *ius ad bellum*, entendido como el derecho al uso de la fuerza de los Estados, es fundamental para comprender como un Estado puede legalmente utilizar la fuerza en el ciberespacio. En este contexto, es pertinente analizar la regulación de la fuerza en el derecho internacional, mediante la conceptualización del *ius* contra *bellum*, *ius ad bellum* e *ius in bellum* a fin de comprender la regulación actual de la fuerza en el derecho internacional.

2.1. La regulación de la fuerza

A lo largo de la historia, los Estados han tenido desacuerdos que a veces se han resuelto por medios pacíficos y otras veces mediante la violencia (Hernández, 2000, p. 162). Desde un punto normativo, el derecho internacional, que regula las relaciones entre los Estados y otros sujetos de derecho internacional, no ha pasado por alto la cuestión del uso de la fuerza (Valencia, 2013, p. 25). Son precisamente el derecho internacional consuetudinario y convencional las principales fuentes que regulan el uso de la fuerza por parte de los Estados. Mediante el ius contra bellum, ius ad bellum e ius in bellum el Derecho internacional aborda el uso de la fuerza. A continuación, se conceptualiza cada uno de estos términos.

2.1.1. Ius contra bellum

El *ius* contra *bellum* consiste en la prohibición de la amenaza o el uso de la fuerza entre Estados, un principio fundamental en el derecho internacional. La Carta de las Naciones Unidas, en su Artículo 2, inciso 4, plasma este principio estableciendo que los miembros de la organización "se abstendrán de recurrir a la amenaza o al uso de la fuerza contra la integridad territorial o la independencia política de cualquier Estado, o en cualquier otra forma incompatible con los Propósitos de las Naciones Unidas".

En la actualidad, el *ius* contra *bellum* estructura las relaciones entre Estados al abogar por la prevención del conflicto, la promoción de la resolución pacífica de disputas y la necesario sanción de los crímenes de agresión (Valencia, 2013, p. 26)[5]. Esta prohibición se reconoce como una norma fundamental del ius gentium, ya que su observancia asegura el cumplimiento de otros principios del derecho internacional. Asimismo, en posición de Kofi Annan, ningún principio que recoge o establece la Carta de las Naciones Unidas es más importante que el principio del no uso de la fuerza[6].

Sin embargo, los Estados no siempre actúan conforme al ius contra bellum, como ocurrió en 1974 cuando Turquía invadió el norte de Chipre y en 2022 cuando Rusia inició su invasión contra Ucrania. En el primer caso, Turquía justificó el uso de la fuerza argumentando la presunta necesidad de proteger a la minoría turca en Chipre y prevenir la anexión del Estado insular a Grecia. Asimismo, Rusia alegó la 'amenaza' de la creciente influencia de la OTAN en Europa del Este y un supuesto genocidio de los habitantes rusófonos en el Donbass. En este contexto, surge la incógnita sobre si el derecho internacional admite excepciones al ius contra bellum, respuesta que se encuentra en la propia Carta de las Naciones Unidas que menciona dos excepciones ala prohibición del uso de la fuerza, estableciendo así las bases del ius ad bellum.

2.1.2. Ius ad bellum

El *ius* ad *bellum*, o derecho a la guerra, implica los casos en los que es válido utilizar la fuerza por parte de los Estados en sus relaciones (1999, Nabulsi, s.f.). A lo largo de la historia, este concepto ha evolucionado. Inicialmente, el *ius ad bellum* concedía un poder absoluto y discrecional al soberano sobre el uso de la fuerza. Sin embargo, con el tiempo, este enfoque ha

"Sin embargo, los Estados no siempre actúan conforme al ius contra bellum, como ocurrió en 1974 cuando Turquía invadió el norte de Chipre y en 2022 cuando Rusia inició su invasión contra Ucrania"

5) Asimismo, la legítima defensa se sustenta en base a los principios de integridad territorial y soberanía estatal.

6) También afirmó que Los Secretarios Generales de las Naciones Unidas se ven desafiados y definidos por la gestión de situaciones que implican el uso de la fuerza, lo que pone a prueba su capacidad para aplicar y preservar este principio fundamental.

"El primer supuesto que justifica el uso de la fuerza es la autorización del Consejo de Seguridad de las Naciones Unidas"

cambiado hacia la instauración de normas destinadas a limitar el uso de la fuerza en las relaciones entre Estados.

Con la creación de las Naciones Unidas, la comunidad internacional buscó cambiar las dinámicas del ius ad bellum, estableciendo normas en el derecho internacional más estrictas y que limitan el uso de la fuerza, promoviendo la paz y la seguridad mediante la resolución pacífica de controversias y la cooperación internacional. En consecuencia, la Carta de las Naciones Unidas, en su Artículo 2, inciso 4, insta a los Estados a abstenerse de recurrir a la amenaza o al uso de la fuerza contra la integridad territorial o la independencia política de cualquier Estado.

No obstante, el derecho internacional contemporáneo concibe dos supuestos que permiten a un Estado recurrir al uso de la fuerza de manera legítima en circunstancias excepcionales y que están sujetos a una minuciosa evaluación por parte de la comunidad internacional. La misma Carta de las Naciones Unidas establece las dos excepciones a la prohibición del uso de la fuerza (Wood, 2013, pp. 351-352).

El primer supuesto que justifica el uso de la fuerza es la autorización del Consejo de Seguridad de las Naciones Unidas. De acuerdo con el artículo 42 de la Carta de las Naciones Unidas, el Consejo de Seguridad puede tomar medidas que impliquen el uso de la fuerza armada o su autorización por parte de miembros de las Naciones Unidas para mantener o restaurar la paz y la seguridad internacionales.

En segundo lugar, se permite el uso de la fuerza en casos de legítima defensa. Según el Artículo 51 de la Carta de las Naciones Unidas, un Estado tiene el derecho inherente de la autodefensa individual o colectiva si es objeto de un ataque armado.

Por lo mencionado, en la legítima defensa, la decisión de utilizar la fuerza inicialmente la toma únicamente el Estado. En cambio, la autorización del Consejo de Seguridad requiere del consenso de al menos 9 de sus 15 miembros[7]. Entonces, existe un mayor riesgo de que la fuerza sea utilizada erróneamente en base a la legítima defensa.

2.1.3. Ius in bellum

Las normas que rigen la conducción de las hostilidades una vez que ha estallado un conflicto armado son parte del "ius in bellum". El Comité Internacional de la Cruz Roja (CICR) denomina al ius in bellum como derecho internacional humanitario (DIH), en parte, para enfatizar su objetivo de mitigar los excesos de la guerra y proteger a los civiles y otros no combatientes (Bradi, 2023, pp. 146-147).[8]

Justamente, el propósito esencial del DIH es humanizar los conflictos arma-

7) Además, es necesario que ninguno de los miembros permanentes ejerza su derecho de veto.

8) Hay parte de la doctrina que enfatiza que el ius in bello debe denominarse como "las leyes de la guerra", alegando que es un cuerpo normativo que se deriva directamente de las costumbres y prácticas de la guerra misma y están destinadas a servir a los ejércitos de los Estados. No obstante, en el presente artículo se opta por utilizar el término DIH e ius in bellum indistintamente.

dos y reducir a lo estrictamente necesario los sufrimientos y daños causados por las acciones bélicas (Kareklas, 2022, p. 1). Mediante su cuerpo normativo, el DIH regula la conducta de las partes para proteger a quienes no participan de las hostilidades, restringe la utilización de ciertos medios y métodos de combate, establece un equilibrio entre el principio de humanidad y las necesidades militares, entre otras cuestiones.

El DIH entra en vigor una vez iniciado un conflicto armado y las partes tienen la obligación de aplicar sus normas, sin perjuicio de las razones de cómo o por qué comenzaron las hostilidades. De modo que el DIH no se centra en determinar la validez del uso inicial de la fuerza ni de la respuesta, a diferencia del ius ad bellum (Salmón, 2016, pp. 28-29).

2.2. Concepción actual

Entonces, en el derecho internacional vigente, la fuerza es una cuestión que se encuentra efectivamente regulada. El ius in bellum regula y limita la conducta de las partes en un conflicto armado (Benjamin, 2023).El ius ad bellum El ius ad bellum aborda la validez del uso excepcional de la fuerza, por lo que hay una proscripción al uso de la fuerza de manera general, tema que abarca el ius contra bellum.

La prohibición de la amenaza y del uso de la fuerza entre Estados se encuentra plasmada en la Carta de las Naciones Unidas y, debido a su carácter consuetudinario e universal[9], no solamente es vinculante con los Estados miembros de la organización. Incluso, la Comisión de Derecho Internacional ha señalado que la prohibición de la fuerza es un claro ejemplo de una norma imperativa de ius cogens[10] (Comisión de Derecho Internacional, 2001, p. 90)

No obstante, no todo uso de la fuerza se encuentra prohibido, debido a que la misma Carta de las Naciones también contempla dos salvedades a dicha proscripción: la legítima defensa y el uso de la fuerza por la autorización del Consejo de Seguridad. Ambos supuestos son excepciones, por lo que deben ser interpretados de manera restrictiva (Brownlie, 1963, p. 214). Entonces, actualmente el ius ad bellum e ius contra bellum son dos conceptos que buscan restringir el uso de la fuerza entre los Estados.

"El DIH entra en vigor una vez iniciado un conflicto armado y las partes tienen la obligación de aplicar sus normas, sin perjuicio de las razones de cómo o por qué comenzaron las hostilidades"

9) La Corte Internacional de Justicia (CIJ) en el caso Nicaragua de 1986 ha señalado que los principios del uso de la fuerza contenidos en la Carta de Naciones Unidas corresponden a los de la costumbre internacional.

10) Dicha afirmación se encuentra en el informe que elaboró la Comisión sobre la Convención de Viena sobre el Derecho de los Tratados.

"En las últimas décadas, se han iniciado diversos conflictos armados internacionales en los que diferentes Estados han alegado que se han cumplido con los requisitos para ejercer la legítima defensa mediante una interpretación flexible de la institución, por ejemplo, aplicando el uso de la fuerza frente a actores no estatale"

CAPÍTULO 3 LA LEGÍTIMA DEFENSA

En la comunidad internacional no hay debate sobre el derecho inmanente que tienen los Estados a la legítima defensa, debido a su vinculación con su derecho de sobrevivencia[11]. No obstante, han existido y persisten controversias con respecto a su interpretación. En las últimas décadas, se han iniciado diversos conflictos armados internacionales en los que diferentes Estados han alegado que se han cumplido con los requisitos para ejercer la legítima defensa mediante una interpretación flexible de la institución, por ejemplo, aplicando el uso de la fuerza frente a actores no estatales.

Sin embargo, es importante enfatizar que el ius ad bellum permite usar la fuerza de manera excepcional, en conformidad con la estricta prohibición establecida en el artículo 2, inciso 4, de la Carta de las Naciones Unidas. Por lo tanto, el ejercicio de la legítima defensa debe ser restrictivo y no flexible (Fuentes, 2015, p. 261). A continuación, se analizarán los requisitos que los Estados deben cumplir para el adecuado ejercicio de este derecho inmanente conforme al derecho internacional, específicamente, en la Carta de las Naciones Unidas y en el derecho consuetudinario.

3.1. Requisitos contenidos en la Carta

Como bien se ha mencionado, en el derecho internacional contemporáneo la legítima defensa se encuentra vinculado a un esquema institucional (Salmón, 2016, p. 158). De este modo, la comunidad internacional ha incorporado parte de su regulación en el artículo 51 de la Carta de las Naciones Unidas, con el objetivo de evitar que la decisión de emplear la fuerza quede exclusivamente en manos de un solo Estado y garantizar así que su uso sea conforme a derecho. En consecuencia, el ejercicio de legítima defensa está sujeto a la apreciación del Consejo de Seguridad a fin de salvaguardar la paz y la seguridad internacionales.

Entre las condiciones que establece el artículo 51 de la Carta de las Naciones Unidas se encuentran, a saber, la ocurrencia

11) Corte Internacional de Justicia "Legality of the Threat or Use of Nuclear Weapons." Opinión consultiva del 8 de julio de 1996, párrafo 96.

de un ataque armado, que la medida sea provisional y subordinada al Consejo de Seguridad y la debida comunicación de la legítima defensa.

3.1.1. Ataque armado

El artículo 51 de la Carta de las Naciones Unidas establece que todos los Estados tienen el derecho a la legítima defensa "en caso de un ataque armado" (Cocchini, 2018, p. 500). No obstante, la Carta no brinda una definición de ataque armado, posiblemente porque al momento de su redacción había consenso de qué supuestos subsume. Al respecto, en el asunto Actividades militares y paramilitares en Nicaragua y contra Nicaragua de 1986, la CIJ concluyó que las manifestaciones más severas del uso de la fuerza pueden ser calificadas como ataques armados que activen el derecho a la legítima defensa[12]. Este criterio se basó en la escala y en los efectos de tales manifestaciones (Max-Planck-Institut, s. f.). Según la doctrina, este criterio implica que acciones armadas cuyo efectos en otros Estado sean tan graves a las de un ataque armado "regular" y, por lo tanto, causen una destrucción sustancial de los elementos claves del Estado, son considerados ataques armados (Li y Zhang, 2022, p. 171).

Con la definición brindada por la Corte y la interpretación doctrinaria, no existe una tipificación estricta e inmutable de los criterios que debe cumplir un ataque armado, sino es una definición amplia que comprende los usos más graves de la fuerza. Esta definición es acorde con el hecho de que el desarrollo armamentístico sigue en constante avance, por lo que pueden ocurrir incidentes que no previstos explícitamente por la Carta, pero que formen parte de "los usos más graves de la fuerza" y, por ende, constituyan un ataque armado.

En suma, cualquier incidente que pueda ser calificado como uno de los usos más graves de la fuerza será un "ataque armado" y podrá activar el derecho a legítima defensa. Sin embargo, es importante destacar que pese a la amplitud de su definición, existen otros requisitos que debe cumplir un Estado para ejercer este derecho.

"Con la definición brindada por la Corte y la interpretación doctrinaria, no existe una tipificación estricta e inmutable de los criterios que debe cumplir un ataque armado, sino es una definición amplia que comprende los usos más graves de la fuerza"

12) La definición de "ataque" según el DIH o *ius in bellum* es distinta del concepto de "ataque armado" que establece la Carta de las Naciones Unidas, materia que abarca el *ius ad bellum*.

"El propósito del deber de informar es que, mediante su cumplimiento, el Consejo de Seguridad pueda tomar las medidas necesarias para preservar la paz y la seguridad internacionales, conforme al artículo 51 de la Carta"

3.1.2. Medidas temporales y sujetas a la decisión del Consejo de Seguridad

El artículo 51 de la Carta establece que la legítima defensa podrá ejercerse "hasta tanto que el Consejo de Seguridad haya tomado las medidas necesarias para mantener la paz y la seguridad internacionales". Asimismo, dispone que las medidas que se tomen ejerciendo este derecho "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" (Congressional Research Service, 2023, p. 1). En consecuencia, la legítima defensa debe cumplir con ser una medida temporal y subordinada a la decisión del Consejo de Seguridad.

Este requerimiento se funda en que el Consejo de Seguridad es el órgano que centraliza el uso de la fuerza, por lo que las medidas de los Estados deben ceder ante la decisión que tome. Incluso, el Consejo de Seguridad puede manifestar y tomar decisiones respecto a si el supuesto Estado víctima ha ejercido el derecho a la legítima defensa conforme con el derecho internacional.

No obstante, el Estado víctima aún puede seguir utilizando la fuerza, pese a que el Consejo haya tomado una decisión al respecto como el cese al fuego, si es que el Estado agresor continúa llevando a cabo actos hostiles (Kelsen, 1950, p. 801). Esta continuación de la legítima defensa es acorde al derecho internacional, debido a que se considera que no menoscaba la autoridad ni la responsabilidad del Consejo.

3.1.3. Informar al Consejo de Seguridad

El artículo 51 de la Carta de las Naciones Unidas establece que "las medidas tomadas por los Miembros en ejercicio del derecho de legítima defensa serán comunicadas inmediatamente al Consejo de Seguridad". En consecuencia, el Estado que ejerce la legítima defensa tiene la obligación de comunicar de inmediato al Consejo de Seguridad las acciones tomadas y las razones por las que se encuentra amparado en este derecho (Green, 2015, pp. 7-8).

El propósito del deber de informar es que, mediante su cumplimiento, el Consejo de Seguridad pueda tomar las medidas necesarias para preservar la paz y la seguridad internacionales, conforme al artículo 51 de la Carta. Al respecto, su incumplimiento no ha ocasionado que el uso de la fuerza en nombre de la legítima defensa haya sido considerado ilegal, por lo que es considerado un requisito procedimental y no sustantivo (Orakhelashvili, 2011, p. 280).

No obstante, haber notificado es esencial para evaluar la buena fe del Estado en cuanto a su convicción de actuar de acuerdo con el derecho internacional (Orakhelashvili, 2011, p. 280). Al no informar se genera la presunción de que las acciones del supuesto Estado víctima no están amparadas por la figura de la legítima defensa, cuestión relevante en términos de alegar y/o probar la legalidad de su actuación. A modo de referencia, en el asunto *Actividades militares y paramilitares en Nicaragua y contra Nicaragua*, la CIJ afirmó que la falta de notificación al Consejo de Seguridad podría ser un elemento que genera incertidumbre acerca de si el Estado realmente está convencido de estar ejerciendo su derecho legítimo de defensa.

3.2. Requisitos consuetudinarios

Según la CIJ, el derecho consuetudinario establece requisitos para la legítima defensa que debe cumplir un Estado adicionales a los que dispone la Carta de Naciones Unidas, a saber, la proporcionalidad y la necesidad. Ambos requerimientos tienen su origen en el incidente conocido como Caroline Case o Caroline Affair de 1837, donde el entonces secretario de Estado de Estados Unidos, Daniel Webster, y el ex representante del gobierno británico, lord Ashburton, intercambiaron comunicaciones a propósito de la destrucción de un buque llamado "Caroline" por las fuerzas británicas en territorio estadounidense (Waxman, 2018, p.1).

La comunicación diplomática entre ambos funcionarios constituye un precedente en la aplicación de los criterios de necesidad y proporcionalidad en la legítima defensa e incorpora un tercer elemento, la inmediatez. Estos requisitos buscan asegurar que la legítima defensa se limite a repeler un ataque armado y prevenir sus consecuencias. De este modo, se pretende evitar que se utilice la fuerza punitivamente o como represalia. A continuación, se describirán los tres requisitos consuetudinarios.

3.2.1. Proporcionalidad

En el derecho internacional, la proporcionalidad desempeña un papel crucial en el *ius in bello* y en el *ius ad bellum*, aunque con significados distintos (McMahan, 2016, pp. 418-419). En el primer caso, es un principio rector del DIH que implica evaluar si los daños colaterales a civiles y bienes civiles, causados por un ataque contra un objetivo militar, son excesivos en comparación con la ventaja militar prevista. En el *ius ad bellum*, la proporcionalidad se emplea al momento de ejercer la legítima defensa abarcando tanto una perspectiva cuantitativa como cualitativa. La mayoría de los Estados considera que la legítima defensa es proporcional cuando se cumple con ambas perspectivas o dimensiones.

"La comunicación diplomática entre ambos funcionarios constituye un precedente en la aplicación de los criterios de necesidad y proporcionalidad en la legítima defensa e incorpora un tercer elemento, la inmediatez"

"La dimensión cuantitativa de la proporcionalidad se refiere a la comparación entre el nivel de fuerza empleada por el Estado agresor y la fuerza utilizada en la respuesta por parte del Estado que se defiende, considerando tanto su magnitud como alcance"

La dimensión cuantitativa de la proporcionalidad se refiere a la comparación entre el nivel de fuerza empleada por el Estado agresor y la fuerza utilizada en la respuesta por parte del Estado que se defiende, considerando tanto su magnitud como alcance. Según esta perspectiva, se busca que haya simetría entre el acto ofensivo y la reacción defensiva (Corn, 2020, pp. 99-100).

En cuanto a la dimensión cualitativa de la proporcionalidad, se centra en que el uso de la fuerza cumpla con el objeto de la legítima defensa, específicamente, repeler un ataque o prevenir que se materialice (Beer, 2018, pp. 186-188). Según esta perspectiva, la fuerza empleada por el Estado que ejerce la legítima defensa debe restringirse a la necesaria para contrarrestar el ataque armado, por lo que no se centra en la forma, sustancia y fuerza intrínseca de la acción en sí, sino en el resultado que se busca. Además, destaca que la reacción defensiva debe cumplir con los principios y reglas establecidos por el derecho internacional humanitario.

Ninguna de las dimensiones exige que la fuerza empleada en la defensa sea de la misma naturaleza que la del ataque armado inicial, pudiendo ser distinta (Roscini, 2014, pp. 90-91), únicamente el Estado debe cumplir un doble test de proporcionalidad: cualitativa y cuantitativa. El primero busca simetría y el segundo que el ataque defensivo cumpla con su finalidad. Es importante analizar la proporcionalidad en cada situación de forma individual, con el objeto de evitar que la fuerza sea utilizada con fines punitivos y que se desvirtúe así la legítima defensa.

3.2.2. Necesidad

La necesidad, en términos jurídicos, ofrece una justificación para una acción que generalmente estará prohibida cuando los medios convencionales son insuficientes para proteger un determinado interés jurídico. En la legítima defensa, la necesidad exige que el Estado utilice la fuerza como ultima ratio para hacer frente al ataque armado (Salmón, 2017, p. 159). Es decir, únicamente en situaciones donde las medidas que no involucren el uso de la fuerza hayan resultado ineficaces o sea altamente probable y razonable que resulten ineficaces. De existir otros medios que razonablemente puedan repeler el ataque armado, el Estado víctima deberá agotarlos previo a utilizar la fuerza vía legítima defensa.

El derecho internacional restringe el uso de la fuerza, y el requisito de la necesidad es una manifestación clara de esa limitación. Es obligatorio que un Estado recurra a la fuerza, vía legítima defensa,

únicamente en caso de que no haya otros medios pacíficos disponibles o no pueda ejecutarlos para defenderse de un ataque armado.

3.2.3. Inmediatez

Aunque el requisito de inmediatez no siempre se menciona explícitamente y a veces es asimilado con la necesidad, sigue siendo un elemento crucial establecido en el derecho consuetudinario para el ejercicio de la legítima defensa por parte de un Estado. De acuerdo con este requisito, para que un Estado pueda emplear la legítima defensa, se requiere que el ataque armado por parte del Estado agresor esté en desarrollo o que haya un intervalo de tiempo razonablemente breve entre dicho ataque y la respuesta defensiva (Consigli y Lavopa, 2006, pp. 34-35).

La inmediatez en la legítima defensa busca evitar que los Estados utilicen esta justificación como excusa para recurrir a la fuerza de manera ilegal. Esto se debe a que una reacción defensiva que ocurre en un lapso excesivo después de que los ataques armados hayan terminado podría ser calificado como una represalia o, incluso, una agresión, acción prohibida por el derecho internacional (Gill, 2015, p. 7). En consecuencia, este requisito permite distinguir entre la legítima defensa y el uso indebido de la fuerza. Subraya que el fin de la legítima defensa es repeler un ataque armado, no castigar al responsable.

Sin embargo, es importante aclarar que la inmediatez no implica que la respuesta defensiva sea instantánea, sino que se desarrolle en un plazo razonable (Roscini, 2014, p. 92). En consecuencia, la inmediatez no debe entenderse de manera inmediata, sino de forma razonable, debido a que la respuesta armada de un Estado agredido toma tiempo. Es importante considerar los plazos que conlleva la identificación del atacante por el Estado, la planificación de la respuesta militar, la necesidad de cumplir con el requisito de proporcionalidad y, de ser requerido, tomar otros medios pacíficos según el requisito de necesidad.

“La inmediatez en la legítima defensa busca evitar que los Estados utilicen esta justificación como excusa para recurrir a la fuerza de manera ilegal. Esto se debe a que una reacción defensiva que ocurre en un lapso excesivo después de que los ataques armados hayan terminado podría ser calificado como una represalia o, incluso, una agresión, acción prohibida por el derecho internacional”

"Entonces, el ciberespacio puede ser definido como un entorno compuesto por las telecomunicaciones, los sistemas informáticos, los sistemas interconectados mediante internet y redes interdependientes de tecnología de la información en general, definición que será utilizada en el presente artículo"

CAPÍTULO 4 EL CIBERESPACIO Y EL USO DE LA FUERZA

En la sociedad moderna, el ciberespacio se ha vuelto esencial en la vida diaria de las personas. La dependencia de las computadoras, sistemas informáticos y redes ha aumentado, convirtiéndose en una parte integral de las infraestructuras civiles e, incluso, de las fuerzas armadas de los Estados (Roscini, 2010, pp. 86-88).

La digitalización, sin embargo, presenta un dilema. A medida que un Estado se vuelve más dependiente digitalmente, también se vuelve más vulnerable a los ciberataques. Si las redes informáticas actualmente se consideran los 'canales vitales' de la sociedad, deshabilitarlas podría equivaler a una parálisis sistémica del Estado. En consecuencia, hemos observado una creciente participación del ciberespacio en conflictos armados desde finales del siglo XX (Gisel y Rodenhäuser, 2019).

4.1. Definición de ciberespacio

No hay un consenso internacional sobre el concepto del ciberespacio. No obstante, la Unión Internacional de Telecomunicaciones (UIT)[13] emplea este término para referirse a los sistemas y servicios que están directa o indirectamente conectados a Internet, así como a las telecomunicaciones y a los sistemas informáticos (Jamschon, 2021, p. 57). La mayoría de las definiciones se alinean a esta definición y concuerdan en que el ciberespacio se encuentra en una dimensión distinta a la física, debido a que se trata de un espacio intangible creado de forma artificial.

El Departamento de Defensa de los Estados Unidos define el ciberespacio como el dominio global del ambiente de información que consta de infraestructuras de tecnología de información en redes interdependientes y datos residentes(Roscini, 2014, pp. 9-10). Asimismo, mediante una declaración, el Reino Unido utiliza el concepto para referirse al ámbito de acciones y conductas llevadas a cabo utilizando la red interdependiente de infraestructuras de tecnología de la información (United Kingdom Mission to the United Nations, 2018, p. 2).

13) La Unión Internacional de Telecomunicaciones es el organismo especializado en telecomunicaciones de la Organización de las Naciones Unidas.

Entonces, el ciberespacio puede ser definido como un entorno compuesto por las telecomunicaciones, los sistemas informáticos, los sistemas interconectados mediante internet y redes interdependientes de tecnología de la información en general, definición que será utilizada en el presente artículo. Bajo este concepto, la ubicación del ciberespacio no es física, sino que se encuentra en todas y en ninguna parte al mismo tiempo, aunque requiere del entorno tangible para funcionar.

Es la sociedad la que posee la capacidad de modificar o evolucionar el entorno difuso del ciberespacio, que proporciona posibilidades ilimitadas a diferencia de otros espacios. Esta característica ha permitido que civiles, corporaciones, Estados y otros actores utilicen este entorno para llevar a cabo sus actividades diarias

4.2. Uso militar del ciberespacio

Desde hace ciento cincuenta años, los avances tecnológicos han sucedido con tal rapidez que cada conflicto armado se diferencia notablemente de los anteriores (Crawford, 2010, p. 7). Actualmente, uno de los ámbitos donde se evidencian estos cambios de manera destacada es el ciberespacio. A medida que los Estados se vuelven más digitalizados, la importancia del desarrollo militar en este dominio aumenta para enfrentar posibles vulnerabilidades y, al mismo tiempo, para aprovecharlo contra el adversario. Como resultado, el ciberespacio se ha convertido en un terreno en el que se realizan actividades tanto de índole civil como militar.

Este fenómeno ha llevado a que el ciberespacio sea considerado un escenario activo en los conflictos armados, donde los objetivos militares pueden ser alcanzados en cuestión de segundos, debido a que las distancias geográficas y las fronteras resultan irrelevantes. Al respecto, el reporte del Grupo de Expertos Gubernamentales de las Naciones Unidas (GGE) de 2010 detalla el uso militar del ciberespacio (Tiirmaa-Klaar, 2021, p. 5) y resalta que hay cada vez más informes que indican que los Estados están desarrollando tecnologías de la información y las comunicaciones como instrumentos de guerra e inteligencia.

En este contexto, varios Estados han iniciado la creación de unidades cibernéticas dentro de sus fuerzas armadas. En Sudamérica, Colombia ha establecido el Comando Cibernético Conjunto de las Fuerzas Armadas. En Norteamérica, Estados Unidos ha formado un Comando Cibernético militar. En Europa, Francia se ha creado un Comando de Ciberdefen-

“Este fenómeno ha llevado a que el ciberespacio sea considerado un escenario activo en los conflictos armados, donde los objetivos militares pueden ser alcanzados en cuestión de segundos, debido a que las distancias geográficas y las fronteras resultan irrelevantes”

"Un ciberataque o ataque cibernético se refiere a cualquier maniobra o acto ofensivo deliberado que tiene como objetivo tomar el control, desestabilizar o dañar un sistema informático"

sa, llamado ComCyber, para coordinar las operaciones cibernéticas militares. En Asia, China ha establecido batallones y regimientos en el ciberespacio. En la actualidad, la mayoría de los ejércitos de los Estados, especialmente los desarrollados, han incorporado el ciberespacio en el ámbito militar.

De hecho, parte del conflicto entre Rusia y Ucrania se ha desarrollado en el ciberespacio (Duguin y Pavlova, 2023, pp. 6-7), donde en ciertos momentos se han interrumpido los sistemas militares de mando, control y comunicación (Burkhalter, 2022)[14], además de paralizarse los sistemas bancarios. Un ciberataque o una ciberoperación tiene la capacidad de desactivar generadores de energía, provocar el descarrilamiento de trenes, la caída de aviones, la fusión de reactores nucleares, entre otros eventos.[15] Son precisamente los ciberataques las acciones más graves que realizan los Estados en el ciberespacio para perjudicar al enemigo, y el siguiente apartado aportará con mayor precisión en qué consisten.

4.2.1. Ciberataque

A diario, se llevan a cabo innumerables operaciones maliciosas en el ciberespacio, con variados niveles de daño. Estas acciones abarcan desde el robo o la destrucción de información hasta el ciberespionaje y la destrucción física. Para clasificarlas, aquellas de baja intensidad se denominan como "incidentes", mientras que las de mayor intensidad, en términos de escala y efectos, se consideran como "ciberataques" o "ataque cibernético" (Jamschon, 2021, p. 60).

Un ciberataque o ataque cibernético se refiere a cualquier maniobra o acto ofensivo deliberado que tiene como objetivo tomar el control, desestabilizar o dañar un sistema informático. Esta actividad maliciosa es considerada una categoría restringida aplicable a operaciones cibernéticas hostiles particularmente atroces, lo que permite la más enérgica de las respuestas por parte del Estado. La gravedad de las consecuencias resulta característica de este tipo de acciones, más que el acto en sí.

En el marco de un conflicto armado internacional, un ciberataque implica la acción deliberada que vulnera un sistema vital para la seguridad nacional, independencia política o integridad territorial de un Estado. Actualmente, son comunes en los conflictos junto con operaciones mili-

14) El 24 de febrero, simultáneamente con la invasión de Ucrania por parte de Rusia, se llevó a cabo un ciberataque contra el satélite de comunicaciones KA-SAT, resultando en la interrupción de las redes de comunicación militar ucranianas.

15) Acciones que pueden ser contrarias al DIH.

tares cinéticas, tal como ocurrió durante la invasión de Rusia a Ucrania en 2023. De hecho,el Foro Económico Mundial ha señalado en su informe de riesgo de 2023 que los ciberataques son el quinto riesgo más grave que confrontan los Estados actualmente (Matalobos, 2023).

En cuanto a sus efectos, los ciberataques pueden causar daños tanto materiales como inmateriales, ya sea de forma inmediata o a largo plazo, de manera directa o indirecta. Un ejemplo ilustrativo es la vulnerabilidad de los sistemas de salud de los Estados, que, a pesar de estar cada vez más digitalizados, suelen carecer de una protección adecuada contra ciberataques. Durante el desarrollo de conflictos armados internacionales, es común que las infraestructuras esenciales de los hospitales sufran daños por bombardeos, y si a eso le sumamos un ciberataque a gran escala, las consecuencias podrían ser aún peores (CICR, 2021).

A continuación, se expondrán dos casos que demuestran los graves efectos de los ciberataques para los Estados, uno en un contexto sin violencia armada prolongada y el otro en el marco de un conflicto armado internacional reciente.

4.2.2. Ciberataques contra Estonia de 2007

En abril de 2007, en el marco de la decisión del gobierno estonio de retirar un monumento a los caídos soviéticos, el Soldado de Bronce de Tallin y tumbas de guerra, Estonia sufrió un ataque cibernético a gran escala. Este ciberataque fue el primero que logró afectar significativamente la infraestructura de un Estado. El incidente consistió en un masivo ciberataque de denegación de servicio distribuido (DDoS)[16] que duró tres semanas. Más de un millón de computadoras ubicadas en más de 100 Estados, conectadas mediante el uso de botnets, dirigieron solicitudes hacia las infraestructuras críticas de Estonia, impactando áreas como la economía, el comercio y las comunicaciones a nivel nacional.

Como resultado, la población estonia enfrentó dificultades para realizar operaciones bancarias, recibir noticias y comunicarse a través de los canales normales. El ataque llevó a Estonia a considerarlo un acto de guerra, solicitando ayuda a la OTAN. Este incidente marcó un hito, ya que condujo al establecimiento del Centro de Excelencia de Ciberdefensa de la OTAN en Tallin, capital de Estonia (Añover, 2021).

Expertos en ciberseguridad rastrearon la actividad cibernética hasta Rusia, quien negó cualquier implicación y acusó de falsificación en su contra. Asimismo, la falta de cooperación en la investigación y el rechazo de una solicitud de investigación bilateral aumentaron la tensión entre Estonia y Rusia. Si bien el incidente no ocasionó el inicio de un conflicto armado, dejó en claro el potencial disruptivo de los ciberataques a nivel estatal. Al respecto, la OTAN ha reconocido que ataques cibernéticos similares a los que experimentó Estonia en 2007 podrían llevar actualmente a la invocación del Artículo 5 (Prucková, 2022)[17].

16) Un ataque distribuido de denegación de servicio (DDoS) implica el empleo de varios sistemas informáticos comprometidos para dirigirse a un objetivo específico, como un servidor, un sitio web u otro recurso de red. Este tipo de ataque tiene como resultado la denegación del servicio para los usuarios que intentan acceder al recurso de destino.

17) La OTAN no ha detallado las características específicas que un ciberataque debe tener para provocar la activación del Artículo 5. La organización argumenta que evita conceder a posibles adversarios el privilegio de definir las circunstancias exactas en las que se desencadenaría la legítima defensa colectiva.

"En suma, desde el inicio del conflicto armado contra Rusia, Ucrania ha sido objeto de una gran serie de ciberataques. Estos incidentes han abarcado operaciones dirigidas a la infraestructura energética de Ucrania, servicios postales, y telecomunicaciones"

4.2.3. Ciberataques contra Ucrania en 2022

Es importante precisar que incluso antes de la invasión rusa en 2022, Ucrania ya había enfrentado ciberataques vinculados a Rusia. En marzo de 2014, en el marco de la anexión rusa de Crimea, hubo un significativo ataque cibernético que afectó sitios web ucranianos. En 2015, la red eléctrica ucraniana sufrió un ataque que causó la pérdida de energía para más de 230,000 consumidores. En junio de 2017, entidades y empresas en Ucrania fueron afectadas por el malware "NotPetya", causando pérdidas estimadas de más de 10 mil millones de dólares (Sari, 2023, pp. 3-4).

El 14 y 15 de febrero de 2022, se llevaron a cabo una serie de ciberataques, dirigidos hacia redes y sitios web tanto privados como gubernamentales en Ucrania(Lin, 2022, p. 33). El 18 de febrero, el Ministerio de Relaciones Exteriores y de la Mancomunidad de Naciones del Reino Unido afirmó que había gran probabilidad de que la Dirección Principal de Inteligencia rusa (GRU) estuviera implicada en estos ciberataques.

Después del inicio de la invasión rusa a gran escala en febrero de 2022, Ucrania continuó siendo blanco de ciberataques vinculados a Rusia. Uno de los incidentes más perjudiciales fue el ataque a Viasat, que causó interrupciones significativas en los servicios de Internet en todo el Estado. Este ataque dejó inoperativos miles de módems de banda ancha, incluyendo aquellos utilizados por el gobierno y el ejército ucranianos (Canadian Centre for Cybersecurity, 2022, pp. 2-4).

En suma, desde el inicio del conflicto armado contra Rusia, Ucrania ha sido objeto de una gran serie de ciberataques. Estos incidentes han abarcado operaciones dirigidas a la infraestructura energética de Ucrania, servicios postales, y telecomunicaciones. Asimismo, se han observado mensajes falsos dirigidos al público en general, ataques de phishing contra funcionarios gubernamentales y ciudadanos, así como diversas actividades de inteligencia y vigilancia llevadas a cabo a través de medios cibernéticos. Si bien muchos de estos ciberataques han sido atribuidos a grupos con afinidad prorrusa, así como a autoridades rusas (National Cyber Security Centre, 2022), es importante señalar que el Gobierno ruso ha negado su participación.

Estos eventos evidencian la creciente importancia de los ciberataques en los conflictos armados actuales, utilizándose de manera conjunta con las operaciones militares que se desarrollan en el espacio físico. En abril de 2022, David Cattler y

Daniel Black, funcionarios de la OTAN, argumentaron que las acciones en el ciberespacio representan el mayor éxito militar de Rusia hasta la fecha en el conflicto armado contra Ucrania (Mueller, Jensen, Valeriano, Maness y Macias, 2023).

4.3. La vigencia y aplicación del Derecho Internacional en el ciberespacio

Los ciberataques previamente mencionados son ejemplos ilustrativos que explican la creciente preocupación de los Estados respecto a proteger las infraestructuras y las actividades cibernéticas de las que dependen, dependencia que de hecho va en aumento. En consecuencia, la aplicación del derecho internacional en este entorno es fundamental para garantizar su seguridad y estabilidad.

Parte de la comunidad internacional está de acuerdo en que el Derecho Internacional se aplica en el ciberespacio. En el informe del Grupo de Trabajo Especial de Composición Abierta (OEGW) de 2021, los Estados reiteraron su comprensión al respecto, afirmando que su aplicación, particularmente la Carta de las Naciones Unidas, es esencial para preservar la paz y la estabilidad (Schmitt, 2021).

Mediante diversas declaraciones, la mayoría de los Estados y algunas organizaciones internacionales han dejado en claro su posición respecto a la aplicación del derecho internacional en el ciberespacio. Dinamarca, por ejemplo, sostiene que las obligaciones de los tratados, el derecho consuetudinario y los principios generales del derecho internacional tienen aplicación en todas las áreas, incluyendo las operaciones realizadas en el ciberespacio (Kjelgaard y Melgaard, 2023, pp. 447-448). Canadá, por su parte, asegura que el derecho internacional se extiende a las actividades de todos los Estados en este entorno, abarcando la totalidad de la Carta de las Naciones Unidas y el derecho internacional consuetudinario (Government of Canada, 2022).

Es importante señalar que, aunque la gran mayoría de las normas del derecho internacional fueron concebidas considerando situaciones físicas, no hay impedimento para su aplicación en el ciberespacio. El marco existente del derecho internacional proporciona disposiciones que no se limitan a un conjunto específico de escenarios, sino que permiten abordar los nuevos desafíos que surgen debido al rápido avance tecnológico. En consecuencia, sigue siendo válido, aunque su aplicación en el ciberespacio debe adaptarse a este entorno considerando sus características.

4.3.1. La aplicación del *ius ad bellum, ius contra bellum* y el *ius in bellum*

Entre los principales tratados relacionados con el *ius ad bellum*, *ius contra*

“Es importante señalar que, aunque la gran mayoría de las normas del derecho internacional fueron concebidas considerando situaciones físicas, no hay impedimento para su aplicación en el ciberespacio”

"La posibilidad de realizar una interpretación dinámica de las disposiciones de ius ad bellum, ius contra bellum y ius in bello para abarcar el ciberespacio se respalda en el hecho de que numerosos miembros de la comunidad internacional han aplicado normas existentes en el derecho internacional a las operaciones cibernéticas"

bellum y *ius in bello* se encuentran la Carta de las Naciones Unidas de 1945, las Convenciones de La Haya de 1899 y 1907, los cuatro Convenios de Ginebra de 1949 y sus dos Protocolos adicionales de 1977. Cabe destacar que ninguno de estos instrumentos hace referencia al ciberespacio. No obstante, según la Corte Internacional de Justicia (CIJ)[18], mediante la interpretación dinámica o evolutiva[19], todo tratado debe ser interpretado y aplicado en consonancia con el marco del ordenamiento jurídico vigente en el momento de la interpretación (Roscini, 2014, pp. 20-21).

La posibilidad de realizar una "interpretación dinámica" de las disposiciones de *ius ad bellum, ius contra bellum y ius in bello* para abarcar el ciberespacio se respalda en el hecho de que numerosos miembros de la comunidad internacional han aplicado normas existentes en el derecho internacional a las operaciones cibernéticas. Entre los Estados y organizaciones internacionales que están de acuerdo al respecto se encuentran Australia, Canadá, China, Cuba, Dinamarca, la Unión Europea, Hungría, Irán, Italia, Malí, Países Bajos, Qatar, la Federación de Rusia, el Reino Unido, entre otros. En consecuencia, en base a una "interpretación dinámica", la aplicación del derecho internacional que regula el uso de la fuerza puede extenderse al ciberespacio y, en particular, a los ciberataques.

Entonces, el empleo de ciberataques que equivalen al uso de la fuerza se encontraría prohibidos entre Estados (i*us contra bellum*), su empleo debe ser acorde a las excepciones que establece el derecho internacional (*ius ad bellum*), y obedecer al Derecho Internacional Humanitario durante un conflicto armado (*ius in bello*). En el caso del ius contra bellum, Dinamarca ha afirmado que los ciberataques pueden vulnerar la prohibición de la amenaza o el uso de la fuerza contenida en el artículo 2, inciso 4, de la Carta de

18) Este método de interpretación fue utilizado por la CIJ en la Opinión Consultiva de 21 de junio de 1971 y en el fallo del 13 de julio de 2009, en el asunto "Controversia sobre derechos de navegación y derechos conexos".

19) Este método de interpretación se encuentra también implícito en el artículo 31 de la Convención de Viena sobre el Derecho de los Tratados.

las Naciones Unidas, dependiendo de la escala física y los efectos de la operación cibernética (Kjelgaard y Melgaard, 2023, pp. 450-452).

En este sentido, si bien su existencia tiene décadas, el ciberespacio fue reconocido por determinados Estados como un nuevo dominio potencial de conflictos armados en la Cumbre de la OTAN de 2016 en Varsovia (Schmitt, 2020), donde las actuaciones estatales deben ser acordes al *ius ad bellum*, *ius contra bellum e ius in bello*. Un año después, en el 2017, se publicó el famoso Manual de Tallin 2.0, norma de soft law elaborada por un grupo internacional de aproximadamente veinte expertos por invitación del Centro de Excelencia Cooperativa de Ciberdefensa de la OTAN. Es la segunda edición de un documento sobre cómo se debe aplicar el derecho internacional en conflictos cibernéticos, ciberataques y ciberseguridad. Si bien no es vinculante, es un referente en el uso de la fuerza en el ciberespacio de los Estados.

CAPÍTULO 5 EL EJERCICIO DE LA LEGÍTIMA DEFENSA EN EL CIBERESPACIO

Los ciberataques representan un problema cada vez más grave para la comunidad internacional, por lo que el ejercicio del derecho de legítima defensa en el ciberespacio se ha convertido en una cuestión importante para la seguridad y paz global. Al respecto, si bien los Estados no han regulado en concreto cómo se regula la legítima defensa en este entorno, lo cierto es que existen normas generales en el derecho internacional que regulan este derecho y que son aplicables en el ciberespacio. En consecuencia, los Estados siempre deben cumplir con los requisitos establecidos en la Carta de las Naciones Unidas y el derecho consuetudinario independientemente del entorno donde ejerzan la legítima defensa.

No obstante, la aplicación del derecho internacional en este entorno debe tener en consideración la naturaleza de las actividades cibernéticas (Melzer, 2011, p. 5). Es decir, la reacción defensiva de los Estados en el ciberespacio debe cumplir con los requisitos de necesidad, proporcionalidad e inmediatez, conforme a lo dispuesto en el Manual de Tallin 2.0, considerando las características propias de este entorno.

En este capítulo, examinaremos cuándo un Estado puede ejercer su derecho a la legítima defensa en el ciberespacio, evaluando cómo se cumplen los requisitos establecidos por el derecho internacional. La primera parte se enfocará en analizar la aplicación de los requisitos de la Carta de las Naciones Unidas, mientras que la segunda parte se centrará en aquellos establecidos por la costumbre internacional.

“En este sentido, si bien su existencia tiene décadas, el ciberespacio fue reconocido por determinados Estados como un nuevo dominio potencial de conflictos armados en la Cumbre de la OTAN de 2016 en Varsovia ”

"Como se mencionó anteriormente, la Corte Internacional de Justicia (CIJ) en el caso de las Actividades militares y paramilitares en Nicaragua y contra Nicaragua de 1986 identificó que las formas más graves o severas del uso de la fuerza, según su escala y efectos, constituyen ataques armados"

5.1. Cumplimiento de los requisitos establecidos en la Carta de las Naciones Unidas

5.1.1. ¿El ciberataque es un ataque armado?

Según el Artículo 51 de la Carta de las Naciones Unidas, un Estado tiene el derecho de ejercer la legítima defensa ante un ataque armado, por lo tanto en el ciberespacio, un Estado puede reaccionar en defensa propia frente a un ciberataque cuando pueda ser calificado como un 'ataque armado'. Es pertinente destacar que se hace referencia a ciberataques por ser las operaciones maliciosas que se desarrollan en el ciberespacio de mayor intensidad en términos de escala y efectos.

Ahora bien, es relevante determinar si los ciberataques pueden considerarse 'ataques armados'. Como se mencionó anteriormente, la Corte Internacional de Justicia (CIJ) en el caso de las Actividades militares y paramilitares en Nicaragua y contra Nicaragua de 1986 identificó que las formas más graves o severas del uso de la fuerza, según su escala y efectos, constituyen ataques armados. Por lo tanto, un ciberataque puede ser considerado como un ataque armado cuando su escala y los efectos generados son comparables a los de una acción tradicionalmente reconocida como una forma grave del uso de la fuerza (Ambos, 2015, pp. 24-25). Conforme con la regla 30 del Manual de Tallin, entre tales efectos se encuentran la destrucción física de la propiedad, así como el daño o la muerte de personas de un Estado.

Es decir, si un ciberataque causa lesiones o la muerte de personas, o que resulte en la destrucción de bienes, cumplirá con el criterio de escala y efectos de un ataque y podrá ser considerado como tal (Shandler, Gross y Canetti, 2023, p. 12). En términos generales, si el daño causado por un ciberataque es comparable a la destrucción buscada mediante el ejercicio de operaciones militares convencionales, podemos considerarlo como un ataque armado que active el derecho a la legítima defensa del Estado, tal como reconoce el artículo 51 de la Carta de las Naciones Unidas.

En relación con la idea de que un 'ataque armado' debe implicar necesariamente el uso de medios en el espacio físico, la CIJ dejó claro que el artículo 51 se aplica a cualquier uso de la fuerza, independientemente de las armas empleadas, (Corte Internacional de Justicia, 1996). Por lo tanto, el hecho de que los ciberataques no sean armas cinéticas no impide su calificación como ataques armados.

No obstante no todos los ciberataques pueden considerarse como una de las

formas más graves o severas del uso de la fuerza y, por lo tanto, no serían considerados como un ataque armado (Barber, 2023, p. 21). De hecho, la mayoría de los ciberataques ejecutados diariamente no ocasionan, ni buscan ocasionar, un daño equiparable al de un ataque armado tradicional (Hathaway et al., 2012, pp. 836-837), aunque sí pueden generar severas consecuencias, como el posible robo de información bancaria o de gobiernos. En estos casos, no es posible afirmar que dichas operaciones sean ataques armados y que den lugar al derecho a la legítima defensa.

Sin embargo, pueden haber casos en los que diversos ciberataques aisladamente no pueden ser clasificados como un ataque armado por no alcanzar el umbral requerido, pero el conjunto de sus efectos puede ser comparable a los de una acción tradicionalmente reconocida como una forma grave del uso de la fuerza. También en estos casos se puede considerar que el Estado ha sido víctima de un ataque armado y, por ende, puede actuar conforme con el derecho a la legítima defensa.

En ese sentido, los ciberataques pueden proceder de diferentes entidades que actúan de manera concertada y el Estado víctima tendrá el derecho a actuar defensivamente, similar a cómo ocurre frente a un ataque armado convencional. Una interpretación contraría validaría este tipo de acciones concertadas, poniendo así en riesgo la sobrevivencia del Estado agraviado, la paz y la seguridad internacionales, y dejaría sin efecto la prohibición al uso de la fuerza que establece el artículo 2, inciso 4, de la Carta de las Naciones Unidas. Por lo tanto, se debe examinar cada caso individualmente a fin de determinar cuándo un ciberataque o un conjunto de ciberataques será considerado un ataque armado.

A modo de recapitulación, si la escala y los efectos de un ciberataque son similares a los de una operación militar convencional, ya sea por la destrucción de bienes o por el daño y la muerte de personas, se consideraría una forma grave de uso de la fuerza, constituyendo así un ataque armado. Asimismo, un ataque armado no implica necesariamente que provenga del espacio físico. Finalmente, pueden haber ciberataques que individualmente no alcancen el umbral de ataque armado, pero cuyo conjunto tenga efectos similares, por lo que el Estado víctima podrá defenderse independientemente de si la operación provino de uno o más Estados. En tales casos, el Estado afectado podrá ejercer su derecho a la legítima defensa.

5.1.2. La temporalidad de las medidas y su subordinación al Consejo de Seguridad

En el ciberespacio, la aplicación de este requisito implica que el Estado víctima de

"En ese sentido, los ciberataques pueden proceder de diferentes entidades que actúan de manera concertada y el Estado víctima tendrá el derecho a actuar defensivamente, similar a cómo ocurre frente a un ataque armado convencional"

"En el ciberespacio, la aplicación de este requisito implica que el Estado víctima debe informar de inmediato al Consejo de Seguridad sobre las acciones tomadas para defenderse frente a un ciberataque que constituya un ataque armado y proporcionar las razones que respaldan la validez de su accionar."

un ciberataque, que constituya un ataque armado, podrá ejercer su derecho a la legítima defensa hasta que el Consejo de Seguridad tome las medidas para mantener o restablecer la paz y la seguridad internacionales.

En tales casos, el Consejo de Seguridad tendrá la facultad para determinar si el o los ciberataques han constituido efectivamente un ataque armado mediante la evaluación de si ha implicado una amenaza a la paz, quebrantamiento de la paz o acto de agresión, conforme al artículo 39 de la Carta de las Naciones. De esta forma, la evaluación de si un ciberataque ha constituido un ataque armado no quedará únicamente en manos del supuesto Estado víctima. En su lugar, nueve de los quince miembros del Consejo de Seguridad analizarán y votarán por si efectivamente ha sido así, conforme al artículo 27 de la Carta de las Naciones Unidas[20].

Asimismo, si los ciberataques persisten aún con la decisión del Consejo, el Estado víctima puede seguir ejerciendo válidamente su derecho a la legítima defensa.

Mediante este proceso, el Consejo de Seguridad tiene las herramientas para garantizar que el uso de la fuerza sea válido, ya sea si el Estado víctima ha sufrido daños por un ataque armado convencional o un ciberataque. Sin embargo, si bien este requisito contribuye a que los Estados actúen conforme al derecho internacional, cabe aclarar que este órgano de Naciones Unidas ha sido objeto de críticas por haber actuado en determinados supuestos en base a cuestiones políticas más que jurídicas.

5.1.3. Necesidad de informar al Consejo de Seguridad

En el ciberespacio, la aplicación de este requisito implica que el Estado víctima debe informar de inmediato al Consejo de Seguridad sobre las acciones tomadas para defenderse frente a un ciberataque que constituya un ataque armado y proporcionar las razones que respaldan la validez de su accionar. Dichas razones son finalmente los argumentos del Estado agraviado respecto a por qué considera

20) Cabe precisar que adicionalmente a los nueves votos que se requieren para decidir en el Consejo de Seguridad que un ciberataque finalmente constituye un ataque armado, es necesario que ninguno de los cinco miembros permanentes ejerza su derecho de veto: China, Estados Unidos, Francia, Reino Unido y Rusia. De esta forma, será más riguroso en principio determinar que el Estado víctima actuó defensivamente acorde al derecho internacional.

que los efectos del ciberataque o ciberataques han alcanzado el umbral suficiente para considerar a la operación como un ataque armado. Más aún, considerando que es la víctima quien está en mejor posición para acceder a la información sobre los daños que ha sufrido y demostrar así que actuó conforme al derecho internacional. De esta forma, el Consejo de Seguridad contará con mayores datos para evaluar más efectivamente si se han cumplido los requisitos de la legítima defensa.

Asimismo, no es necesario que las medidas defensivas que tome y debe informar el Estado al Consejo de Seguridad compartan la misma naturaleza que el ataque armado inicial del que ha sido víctima. Es decir, pueden implicar operaciones militares en el espacio físico y/o en el ciberespacio. Sobre ello se analizará con mayor detalle en el apartado "el análisis de la proporcionalidad".

De esta manera, el Consejo de Seguridad podrá tomar las medidas necesarias para preservar la paz y la seguridad internacionales. Si bien es importante enfatizar que el incumplimiento de este requisito no convierte ilegal el uso de la fuerza per se (Orakhelashvili, 2011, p. 280), su observancia brinda mayores garantías al respeto del derecho internacional. Se evita que cualquier operación maliciosa en el ciberespacio sea calificada como un ataque armado, ya que el Estado debe justificar su razonamiento, impidiendo así que se distorsione el derecho a la legítima defensa.

5.2. Cumplimiento de los requisitos consuetudinarios

5.2.1. El análisis de la proporcionalidad

La dimensión cuantitativa del requisito de proporcionalidad exige que el derecho a la legítima defensa se ejerza buscando simetría en el nivel de fuerza entre el ataque armado del Estado agresor y la respuesta defensiva por el Estado víctima.

En el ciberespacio, el cumplimiento de esta premisa implica que la magnitud de la respuesta, ya sea mediante un ciberataque o un ataque físico, deba ser proporcional a la escala y los efectos del ataque armado. Es decir, si el ciberataque ocasionó que diversas instalaciones del Estado explosionen, como puede ocurrir con un reactor nuclear el ejercicio de la legítima defensa puede implicar detonaciones. Al respecto, no se requiere que la respuesta sea de la misma naturaleza que el ataque armado, por lo tanto, un Estado agredido puede usar la fuerza en el espacio físico como respuesta a un ciberataque o iniciar una serie de ciberataques frente a un bombardeo, incluso puede desarrollar tanto operaciones en el espacio físico como en el ciberespacio.

"Dichas razones son finalmente los argumentos del Estado agraviado respecto a por qué considera que los efectos del ciberataque o ciberataques han alcanzado el umbral suficiente para considerar a la operación como un ataque armado"

"Dichas razones son finalmente los argumentos del Estado agraviado respecto a por qué considera que los efectos del ciberataque o ciberataques han alcanzado el umbral suficiente para considerar a la operación como un ataque armado"

De hecho, en determinadas situaciones una respuesta en el ciberespacio contra un ciberataque puede no ser posible o efectiva, ya sea porque el Estado víctima carece de la tecnología necesaria para responder en el ciberespacio o porque el agresor es un Estado sin infraestructura digital vital que pueda ser atacada (Roscini, 2014, pp. 90-91). En estos casos, requerir necesariamente que la respuesta sea de la misma naturaleza impedirá finalmente que el Estado se proteja y que continúe siendo objeto de ciberataques. Entonces, el Estado víctima podrá utilizar el medio más adecuado a fin de defenderse de la agresión, siempre y cuando la respuesta se ajuste a la magnitud y efectos del ataque armado inicial, para garantizar la proporcionalidad.

Asimismo, determinar la proporcionalidad en el ciberespacio puede presentar serios desafíos. El Estado puede no tener conocimiento de todas las características o efectos del ciberataque del que ha sido víctima. (Fenton, 2019, pp. 351-352). Al ser el daño causado por un ciberataque imprevisible de forma inmediata, podría resultar complicado establecer su magnitud y consecuencias. Incluso, puede que un ciberataque que inicialmente se consideró que no constituye un ataque armado, con el tiempo sus efectos causen la muerte de miles de personas o la pérdida de bienes. Por lo tanto, se requiere una mayor investigación informática por parte de los Estados a fin de que tomen las acciones para poder cumplir con el elemento de proporcionalidad.

Asimismo, el Estado víctima puede no tener conocimientos sobre la infraestructura digital del Estado agresor al momento de defenderse mediante un ciberataque. En estos casos, al requerir una respuesta defensiva en un tiempo breve, el Estado deberá intentar cumplir con la proporcionalidad y demostrar que tomó acciones a fin de cumplir con dicho requisito. Al respecto, es preciso mencionar que este problema es similar a los inconvenientes que pueden surgir cuando el ataque armado y la respuesta defensiva ocurren en el espacio físico, por ejemplo, con las armas biológicas o químicas[21], cuyos efectos tienden a ser indeterminables.

En relación con la dimensión cualitativa del requisito de proporcionalidad, se establece que la legítima defensa debe orientarse a repeler un ataque armado o prevenir su perpetración. Este aspecto guarda relación con la observancia del DIH (Salmón, 2017, p. 159). A manera

21) Ambas armas se encuentran prohibidas en el Derecho Internacional Humanitario, conforme a las normas consuetudinarias que ha listado el Comité Internacional de la Cruz Roja (CICR).

de ejemplo, en el caso de que un Estado se vea amenazado por un ciberataque a gran escala que pueda ocasionar numerosas pérdidas de vidas humanas, no sería admisible por el derecho internacional que inicie una operación contra los hospitales del Estado agresor. Tal medida, en principio, no se centraría en repeler el ciberataque ni prevenir su consumación. En cambio, el derecho internacional sí permite que el Estado víctima puede utilizar la fuerza mediante armas tradicionales o con operaciones en el ciberespacio para atacar la infraestructura cibernética del atacante, como bombardeando los servidores desde los que se originan los ciberataques. En todo caso, es necesario analizar la proporcionalidad en cada situación de forma individual, más aún considerando que su cumplimiento en el ciberespacio es esencialmente una cuestión técnica.

5.2.2. Necesidad

El requisito de necesidad exige que el Estado ejerza la legítima defensa como ultima ratio, es decir, cuando el uso de la fuerza es la única opción disponible para hacer frente o repeler el ataque armado considerando todas las circunstancias. Este requisito es conforme con el Artículo 2, inciso 3, y las disposiciones del Capítulo VI de la Carta de las Naciones Unidas que establecen la solución pacífica de controversias, obligación que también deben cumplir los Estados en las actividades que realizan en el ciberespacio (United Kingdom Mission to the United Nations, 2018, p. 3).

En consecuencia, antes de recurrir al uso de la fuerza, el Estado víctima debe verificar que el asunto no pueda resolverse por medios pacíficos o menos hostiles (Blank, 2020, pp. 256-257). Frente a un ciberataque de un Estado carente de tecnología, es más probable que un Estado considerado potencia en el sector de la informática pueda hacer frente al ataque armado sin necesidad de utilizar la fuerza. A modo de ejemplo, podría impedir que el ciberataque acceda a las redes mediante la implementación de ciber defensas pasivas o llevar a cabo una contra operación cibernética que no equivalga a un ataque armado. Al contrario, si el Estado víctima se encuentra desprovisto de dichas tecnologías, puede intentar dialogar directamente con el Estado agresor para que cancele el ciberataque antes de que produzca efectos.

Sin embargo, es importante considerar que los ciberataques pueden causar daños de forma inmediata, ya que en el ciberespacio los objetivos pueden ser alcanzados en cuestión de segundos (Government of the Kingdom of the Netherlands, 2019, p. 1). En tales circunstancias, el Estado víctima no contaría con el tiem-

“Frente a un ciberataque de un Estado carente de tecnología, es más probable que un Estado considerado potencia en el sector de la informática pueda hacer frente al ataque armado sin necesidad de utilizar la fuerza”

po suficiente para poder analizar o tomar medidas que no impliquen el uso de la fuerza. Es así que el derecho internacional establece que si el peligro es abrumador y el tiempo para que se produzca el daño es demasiado corto para deliberar o tomar otras acciones, entonces el Estado puede invocar su derecho a la legítima defensa con el fin de repeler o evitar el ciberataque. Esta acción es conforme al principio de necesidad, debido a que el breve plazo para que el daño se produzca hace analizar o ejecutar otras medidas resulten insuficientes o inútiles para afrontar el ataque armado.

En resumen, la aplicación del requisito de necesidad en el ciberespacio implica que el uso de la fuerza por parte del Estado víctima, incluso a través de ciberataques, deba ser fundamental para repeler o prevenir con éxito un ataque armado, en vista de que las medidas menos hostiles o pacíficas no resultaron o no resultan efectivas.

5.2.3. Inmediatez

En el ciberespacio, el ejercicio de la legítima defensa está sujeto a la condición de inmediatez, de acuerdo con la regla 15 del Manual de Tallin (Tsagourias, 2012, pp. 35-36). Este requisito supone que el Estado víctima debe recurrir a la fuerza cuando el ciberataque esté en desarrollo o haya transcurrido un tiempo razonablemente corto entre su ocurrencia y la respuesta defensiva. En este análisis se debe considerar factores relevantes como la proximidad temporal entre el ciberataque y la reacción defensiva, el plazo necesario para identificar al atacante considerando las características del ciberespacio y el tiempo necesario para preparar una respuesta, ya sea mediante operaciones en el espacio virtual o físico. En consecuencia, la inmediatez brinda un período razonable para que el Estado actúe en legítima defensa.

A fin de cumplir con la inmediatez, resulta crucial considerar que en numerosas ocasiones la identificación de un ataque armado en el ciberespacio no se produce de manera inmediata; incluso podría presentar la apariencia de una operación no maliciosa durante días o más tiempo. Este periodo debe contemplarse dentro del plazo que tiene el Estado para defenderse a fin de garantizar su derecho. Asimismo, un ciberataque puede consistir en múltiples operaciones que se llevan a cabo con frecuencia semanal o mensual. Por lo tanto, el Estado víctima aún puede recurrir al uso de la fuerza en legítima defensa, incluso después de la finalización de una operación sin necesidad de esperar el inicio de la siguiente a fin de impedir que se lleve a cabo, pues se considera que el ataque armado en su conjunto no ha finalizado.

Asimismo, como se ha mencionado previamente, pueden haber ciberataques cuyos efectos recién se produzcan semanas o meses después de su ejecución. En estos casos, el Estado víctima deberá determinar cuándo se produjo la operación, si el Estado agresor puede cesar los efectos de la misma y cuál es su origen, a fin de poder ejercer la legítima defensa conforme al derecho internacional. Por ejemplo, en principio no sería válido utilizar la fuerza si la operación en el ciberespacio se llevó a cabo hace más de diez años y el Estado agresor no puede detener sus efectos[22].

22) Esta cuestión no excluye la responsabilidad internacional y las reparaciones que deba cumplir el Estado agresor por vulnerar la prohibición del uso de la fuerza y otras normas de derecho internacional.

En general, ya sea en el ciberespacio o en el entorno físico, el requisito de inmediatez implica evaluar de manera razonable las circunstancias para establecer un plazo que permita distinguir entre el ejercicio de la legítima defensa y el uso ilegal de la fuerza.

CAPÍTULO 6 CONCLUSIONES Y SUGERENCIAS

El ciberespacio es un entorno relativamente nuevo en comparación con las normas que regulan y limitan el uso de la fuerza, aún así, ha adquirido gran importancia para las acciones de los Estados de carácter militar. Si bien el ius contra bellum, el ius ad bellum y el ius in bellum se han concebido considerando el uso de la fuerza por los Estados en el espacio físico, actualmente la comunidad internacional es consciente del peligro que representa los ciberataques para su seguridad, pudiendo ser considerados como "ataques armados" y jugando un papel clave en varios conflictos armados. Diversos incidentes han demostrado este hecho, desde los ciberataques en Estonia de 2007 hasta la invasión rusa en Ucrania que inició el 2022 y perdura en la actualidad[23].

En consecuencia, el derecho internacional se aplica también en el ciberespacio, imponiendo la obligación a cualquier Estado que contemple el uso legítimo de la fuerza en este entorno de ajustarse a las normas del ius ad bellum. En el caso de la legítima defensa, como se ha analizado, es importante que el Estado realice una evaluación meticulosa del cumplimiento de los requisitos establecidos por el derecho internacional considerando las características particulares del ciberespacio.

De este modo, es necesario que los Estados cumplan con los requisitos dispuestos en la Carta de las Naciones Unidas y los que establece la costumbre internacional para poder garantizar la seguridad y la paz global en el ciberespacio. Los Estados deben determinar si un ciberataque constituye un ataque armado antes de reaccionar defensivamente, informar al Consejo de Seguridad por qué consideran que el ciberataque constituye un ataque armado, evaluar si es posible repeler el ciberataque mediante medios que no impliquen el uso de la fuerza, entre otras cuestiones. Una interpretación errónea de los requisitos de la legítima defensa pueden ocasionar situaciones lamentables para los Estados y la comunidad internacional en general.

Es importante señalar que la regulación de la legítima defensa brinda una respuesta satisfactoria para su aplicación en el ciberespacio y existen declaraciones de diversos Estados y ciertos instrumentos de soft law que ayudan en la claridad de tal aplicación, como el Manual de Tallin 2.0. No obstante, esta institución no fue concebida considerando esta realidad, por lo que es ideal que la comunidad internacional regule con mayor precisión el ejercicio de la legítima defensa, y el uso de la fuerza en general, en el ciberespacio mediante un tratado. De este modo, se podrán solucionar varios desafíos en torno a la seguridad y la paz global, considerando que la realización de operaciones de los Estados en el ciberespacio será cada vez más habitual. ◆

23) Al 14 de junio de 2024, la invasión rusa contra Ucrania persiste.

BIBLIOGRAFÍA

Ahmad, A. (2023, 6 noviembre). Enough: Self-Defense and Proportionality in the Israel-Hamas Conflict. Recuperado 21 de enero de 2024, de https://www.justsecurity.org/89960/enough-self-defense-and-proportionality-in-the-israel-hamas-conflict/

Ambos, K. (2015). Responsabilidad penal internacional en el ciberespacio. InDret Revista para el análisis del Derecho, (2), 24-25. Recuperado de https://indret.com/wp-content/themes/indret/pdf/1129.pdf

Añover, A. (2021, 18 junio). Cómo Estonia se convirtió en el país experto en ciberseguridad. La Razón. Recuperado 27 de enero de 2024, de https://www.larazon.es

Auswaertiges-amt. (2021). On the Application of International Law in Cyberspace. Recuperado de https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf

Barber, I. (2023). Application of International Law in Cyberspace: Human Rights Assessment Guide. Global Partners Digital. Recuperado de https://www.gp-digital.org/wp-content/uploads/2023/06/Application-of-Intl-Law-in-Cyberspace-Human-Rights-Assessment-Tool_GPD_.pdf

Beer, Y. (2018). Defensive Deterrence: Legalizing the Stepchild of International Law. En Military Professionalism and Humanitarian Law: The Struggle to Reduce the Hazards of War (pp. 186-188). Oxford University Press. https://doi.org/10.1093/oso/9780190881146.003.0005

Blank, L. (2020). Irreconcilable Differences: The Thresholds for Armed Attack and International Armed Conflict. Notre Dame Law Review, 96, 256-257. Recuperado de https://scholarship.law.nd.edu/cgi/viewcontent.cgi?article=4929&context=ndlr

Bradi, J. (2023). Malvinas y el derecho internacional humanitario. Defensa Nacional, 8, 146-147. Recuperado de https://www.undef.edu.ar/libros/wp-content/uploads/2023/07/8-1-5.pdf

Brownlie, I. (1963). *International Law and the Use of Force by States*. Oxford University Press. https://doi.org/10.1093/acprof:oso/9780198251583.001.0001

Burkhalter, D. (2022, 9 mayo). ¿Cuándo un ciberataque es un crimen de guerra? SWI swissinfo.ch. Recuperado de https://www.swissinfo.ch

Canadian Centre for Cybersecurity. (2022). CYBER THREAT BULLETIN: Cyber Threat Activity Related to the Russian Invasion of Ukraine. Canadian Centre for Cybersecurity. Recuperado de https://www.cyber.gc.ca/sites/default/files/cyber-threat-activity-associated-russian-invasion-ukraine-e.pdf

Centro de Estudios Estratégicos CEEAG. (2018). La Ciberguerra: sus impactos y desafíos (1.a ed.). Recuperado de https://www.ceeag.cl/wp-content/uploads/2020/06/LA-CIBERGUERRA-SUS-IMPACTOS-Y-DESAFIOS.pdf

CICR. (2021, 21 febrero). Guerra informática y derecho internacional humanitario. ICRC. Recuperado 27 de enero de 2024, de https://www.icrc.org

Cocchini, A. (2018). Intentando definir la legítima defensa «preventiva». *Anuario Español de Derecho Internacional*, 34, 500. Recuperado de https://revistas.unav.edu/index.php/anuario-esp-dcho-internacional/article/view/27430

Comisión de Derecho Internacional de las Naciones Unidas. (2001). Informe de la Comisión de Derecho Internacional sobre la labor realizada en su 50.° período de sesiones. *United Nations - Office of Legal Affairs*. Recuperado de https://legal.un.org/ilc/documentation/spanish/reports/a_53_10.pdf

Congressional Research Service. (2023, diciembre). Use of Force in Cyberspace. CRS Reports. Recuperado de https://sgp.fas.org/crs/natsec/IF11995.pdf

Consigli, J., & Lavopa, F. (2006). Dos Aspectos de la Legítima Defensa Frente a la Amenaza Terrorista. En *Anuario Argentino de Derecho Internacional* (Vol. 15, pp. 34-35). Recuperado de https://www.corteidh.or.cr/tablas/R21636.pdf

Corn, G. (2020). The Essential Link between Proportionality and Necessity in the Exercise of Self-Defense. En C. Kreß & R. Lawless (Eds.), *Necessity and Proportionality in International Peace and Security Law Necessity and Proportionality in International Peace and Security Law* (pp. 99-100). Oxford University Press. https://doi.org/10.1093/oso/9780197537374.001.0001

Corte Internacional de Justicia. (1996). Opinión Consultiva sobre la legalidad de la amenaza o el empleo de armas nucleares. Recuperado de https://www.dipublico.org/116807/legalidad-de-la-amenaza-o-el-empleo-de-armas-nucleares-opinion-consultiva-de-8-de-julio-de-1996/

Crawford, E. (2010). *The Treatment of Combatants and Insurgents under the Law of Armed Conflict Treatment of Combatants and Insurgents under the Law of Armed Conflict. Oxford Academic*. https://doi.org/10.1093/acprof:oso/9780199578962.003.0001

Duguin, S., & Pavlova, P. (2023). The role of cyber in the Russian war against Ukraine: Its impact and the consequences for the future of armed conflict. Recuperado de https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/702594/EXPO_BRI(2023)702594_EN.pdf

Fenton, H. (2019). Proportionality and its Applicability in the Realm of Cyber Attacks. Duke Journal of Comparative & International Law, 29, 351-352. Recuperado de https://scholarship.law.duke.edu/djcil/vol29/iss2/6/

Gill, T. (2015). Legal Basis of the Right of Self-Defence under the UN Charter and under Customary International Law. En T. Gill & D. Fleck (Eds.), The handbook of the international law of military operations (2.a ed., p. 7). Oxford University Press. Recuperado de https://pure.uva.nl/ws/files/2589385/179157_512917.pdf

Gisel, L., & Rodenhäuser, T. (2019, 28 noviembre). Cyber operations and international humanitarian law: five key points. Recuperado 25 de enero de 2024, de https://blogs.icrc.org/law-and-policy/2019/11/28/cyber-operations-ihl-five-key-points/

Government of Canada. (2022, 22 abril). International Law applicable in cybers-

pace. Recuperado de https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=eng#a13

Government of the Kingdom of the Netherlands. (2019, 26 septiembre). Appendix: International law in cyberspace. Recuperado 1 de febrero de 2024, de https://www.government.nl/binaries/government/documenten/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace/international-law-in-the-cyberdomain-netherlands.pdf

Green, J. (2015). The Article 51 Reporting Requirement for Self-Defense Actions. Virginia Journal of International Law, 7-8. Recuperado de https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2572406

Fuentes, X. (2015). La prohibición de la amenaza y del uso de la fuerza por el derecho internacional. Araucaria, 16(32), 261. Recuperado de https://revistascientificas.us.es/index.php/araucaria/article/view/779

Hathaway, O., Crootof, R., Levitz, P., Proctor, H., Nowlan, A., Perdue, W., & Spiegel, J. (2012). The Law of Cyber-Attack. California Law Review, 100(4), 836-837. Recuperado de https://openyls.law.yale.edu/bitstream/handle/20.500.13051/3283/Law_of_Cyber.pdf

Hendell, G. (2023, 30 septiembre). The Use of Force by States Under International Law. Recuperado 20 de enero de 2024, de https://theforge.defence.gov.au/article/use-force-states-under-international-law

Hernández Campos, A. (2000). Uso de la fuerza en el derecho internacional : aplicación en conflictos internos. Agenda Internacional, 7(15), 161-181. https://doi.org/10.18800/agenda.200002.008

International Law and the Use of Force: What Happens in Practice? (2013). Indian Journal of International Law, 53, 351-352. Recuperado de https://legal.un.org/avl/pdf/ls/Wood_article.pdf

Jamschon, L. (2021). Actividades cibernéticas y seguridad internacional: Hacia un régimen de normas de comportamiento estatal responsable y medidas de fomento de la confianza. Revista Electrónica. Instituto de Investigaciones Ambrosio L. Gioja, (26), 57. Recuperado de http://revistas.derecho.uba.ar/index.php/revista-gioja/article/view/64

Kareklas, I. (2022, 14 julio). Ius Ad Bellum and Ius In Bello: Humanitarian Law of Armed Conflict. Recuperado de https://www.ccw.ox.ac.uk/blog/ius-ad-bellum-and-ius-in-bello-by-ia-covos-kareklas

Kelsen, H. (1950). The Law of the United Nations: A Critical Analysis of Its Fundamental Problems. The Lawbook Exchange.

Kjelgaard, J., & Melgaard, U. (2023, 4 julio). Denmark's Position Paper on the Application of International Law in Cyberspace. Recuperado de https://doi.org/10.1163/15718107-20230001

Kolb, R. (1997). Origen de la pareja terminológica ius ad bellum / ius in bello. Revista Internacional de la Cruz Roja, 597-598. Recuperado de https://international-review.icrc.org/sites/default/files/S0250569X00004283a.pdf

Li, H., & Zhang, J. (2022). Application of Existing Rules of International law in Cyberspace. Advances in Economics, Business and Management Research, 215, 169-173. https://doi.org/10.2991/aebmr.k.220405.029

Lin, H. (2021). Russian Cyber Operations in the Invasion of Ukraine on JSTOR. The Cyber Defense Review Home, 7(4), 33. Recuperado de https://cyberdefensereview.army.mil/Portals/6/Documents/2022_fall/02_Lin.pdf

Matalobos, J. (2023, 4 agosto). La ciberinseguridad que viene (y cómo protegernos). Recuperado 27 de enero de 2024, de https://www.bbva.com/es/innovacion/la-ciberinseguridad-que-viene-y-como-protegernos/

Max-Planck-Institut. (s. f.). Summaries of the Decisions - Military and Paramilitary Activities in and against Nicaragua. Recuperado 23 de enero de 2023, de https://www.mpil.de/de/pub/publikationen/archiv/world-court-digest.cfm?fuseaction_wcd=aktdat&aktdat=dec0102.cfm#:~:text=The%20Court%20thus%20decided%2C%20by,of%20its%20customary%20law%20obligation

McMahan, J. (2016). Proportionality and Necessity in Jus in Bello. En S. Lazar & H. Frowe (Eds.), The Oxford Handbook of Ethics of War. Oxford Handbook. https://doi.org/10.1093/oxfordhb/9780199943418.013.24

Melzer, N. (2011). Cyberwarfare and International Law. UNIDIR. Recuperado de https://unidir.org/wp-content/uploads/2023/05/cyberwarfare-and-international-law-382.pdf

Mueller, G., Jensen, B., Valeriano, B., Maness, R., & Macias, J. (2023, 13 julio). Cyber Operations during the Russo-Ukrainian War. Center for Strategic International Studies. Recuperado de https://www.csis.org

Nabulsi, K. (1999). Jus ad Bellum/Jus in Bello. En Crimes of War : What the Public Should Know. W.W. Norton & Company. Recuperado de https://users.ox.ac.uk/~polf0002/director/publications/jusadbellum.pdf

National Cyber Security Centre. (2022, 18 febrero). UK government assess Russian involvement in DDoS attacks on Ukraine. NCSC.GOV.UK. Recuperado 29 de enero de 2024, de https://www.ncsc.gov.uk

North Atlantic Treaty Organization. (2014, 5 septiembre). Wales Summit Declaration [Comunicado de prensa]. Recuperado de https://www.nato.int/cps/en/natohq/official_texts_112964.htm

Orakhelashvili, A. (2011). Collective Security. Oxford University Press. https://doi.org/10.1093/acprof:oso/9780199579846.003.0007

Prucková, M. (2022). Cyber attacks and Article 5 – a note on a blurry but consistent position of NATO. Recuperado 28 de enero de 2024, de https://ccdcoe.org/library/publications/cyber-attacks-and-article-5-a-note-on-a-blurry-but-consistent-position-of-nato/

Redacción Ciencia. (2022, 29 diciembre). Los ciberataques a Ucrania por la guerra entre los mayores de 2022. SWI swissinfo.ch. Recuperado 18 de enero de 2024, de https://www.swissinfo.ch

Roscini, M. (2010). World Wide Warfare – Jus ad bellum and the Use of Cyber Force. Max Planck Yearbook of United Nations Law, 14, 86-88. Recuperado de https://www.mpil.de/files/pdf3/03_roscini_14.pdf

Roscini, M. (2014). Cyber Operations and the Use of Force in International Law. Oxford University Press. https://doi.org/10.1093/acprof:oso/9780199655014.001.0001

Salmón, E. (2016). Introducción al Derecho Internacional Humanitario (4.a ed.). Instituto de Democracia y Derechos Humanos Pontificia Universidad Católica del Perú. Recuperado de https://repositorio.pucp.edu.pe/index/bitstream/handle/123456789/169952/2016---Introducci%c3%b3n%20al%20Derecho%20Internacional%20Humanitario.pdf?sequence=1&isAllowed=y

Salmón, E. (2017). Nociones de Derecho Internacional Público (1.a ed.). Fondo Editorial PUCP. Recuperado de https://repositorio.pucp.edu.pe/index/bitstream/handle/123456789/170667/06%20Nociones%20b%C3%A1sicas%20de%20derecho%20internacional%20con%20sello.pdf?fbclid=IwAR2lnmrkII4-XkbCW6-2vdmT_-I96KX3jKQ-DKc-J6AUBRk4dmIuQ1yPQoh8

Sari, A. (2023, marzo). International Law and Cyber Operations: Current Trends and Developments. Council of Europe. Recuperado de https://rm.coe.int/64th-cahdi-pr-aurel-sari-presentation/1680aaaf48

Schmitt, M. (2020, 27 agosto). Noterworthy Releases of International cyber law positions - Part I: NATO. Lieber Institute for Law & Land Warfare - West Point. Recuperado 30 de enero de 2024, de https://lieber.westpoint.edu

Schmitt, M. (2021, 10 junio). The Sixth United Nations GGE and International Law in Cyberspace. Recuperado 29 de enero de 2024, de https://www.justsecurity.org/76864/the-sixth-united-nations-gge-and-international-law-in-cyberspace/

Shandler, R., Gross, M., & Canetti, D. (2023). Cyberattacks, Psychological Distress, and Military Escalation: An Internal Meta-Analysis. Journal of Global Security Studies, 8(1), 24-25. https://doi.org/10.1093/jogss/ogac042

Sierra, P., Fonseca, T., & Fernández, A. (2021). Jus ad bellum, jus in bello, jus ex bello y jus post bellum. En Ética militar y fundamentación profesional. Evolución, conceptos y principios (Vol. 1, pp. 29-31). Sello Editorial ESMIC. Recuperado de https://librosesmic.com/index.php/editorial/catalog/download/80/71/1756?inline=1

Tiirmaa-Klaar, H. (2021). The Evolution of the UN Group of Governmental Experts on Cyber Issues. Cyberstability Paper Series: New Conditions and Constellations in Cyber, 5. Recuperado de https://hcss.nl/wp-content/uploads/2021/12/Klaar.pdf

Tsagourias, N. (2012). The Tallinn Manual on the International Law Applicable to Cyber Warfare: A Commentary on Chapter II — The Use of Force. Yearbook of International Humanitarian Law, 15, 35-36. https://doi.org/10.1007/978-90-6704-924-5_2

United Kingdom Mission to the United Nations. (2018). United Nations Group of Governmental Experts on advancing responsible state behaviour in cyberspace in the context of International Security. GOV.UK. Recuperado de https://assets.publishing.service.gov.uk/media/60b775388fa8f54899011dec/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement.pdf

Valencia, A. (2013). Derecho internacional humanitario. Conceptos básicos: Infracciones en el conflicto armado colombiano (2.a ed.). Oficina en Colombia del Alto Comisionado de las Naciones Unidas para los Derechos Humanos. Recuperado de https://www.oas.org/es/sla/ddi/docs/dih_conceptos_basicos_2013.pdf

Zahra, I., Handayani, I., & Wulan Christianti, D. (2021). Cyber-Attack in Estonia: a New Challenge in The Applicability of International Humanitarian Law. Yustisia Jurnal Hukum, 10(1), 58-59. https://doi.org/10.20961/yustisia

Waxman, M. (2018, 28 de agosto). The Caroline Affair in Evolving International Law of Self-Defense. https://www.lawfareblog.com/carolineaffair.

Recibido: 07/02/2024
Aprobado: 10/06/2024