ACADEMIA DIPLOMÁTICA DEL PERÚ JAVIER PÉREZ DE CUÉLLAR

MAESTRÍA EN DIPLOMACIA Y RELACIONES INTERNACIONALES

TESIS PARA OBTENER EL GRADO DE MAESTRO EN DIPLOMACIA Y RELACIONES INTERNACIONALES

TEMA DE TESIS:

Aportes para la política exterior peruana en materia de amenazas híbridas en el ciberespacio

PRESENTADO POR:

Daniel Andrés Huapaya Noriega

ASESOR:

Asesor Académico: Dr. Pablo Moscoso de la Cuba

Asesora Metodológica: Dra. Ofelia Santos

Lima, 21 de noviembre de 2022

ACADEMIA DIPLOMÁTICA DEL PERÚ JAVIER PÉREZ DE CUÉLLAR

FORMULARIO DE AUTORIZACIÓN PARA LA PUBLICACIÓN DE TESIS EN EL REPOSITORIO DIGITAL DE LA ACADEMIA DIPLOMÁTICA DEL PERÚ JAVIER PÉREZ DE CUÉLLAR

1. DATOS DEL AUTOR DE LA TESIS

Apellidos y nombres: **Daniel Andrés Huapaya Noriega**

DNI Nº: 70000564

2. IDENTIFICACIÓN DE LA TESIS

Título de la tesis: **Aportes para la política exterior peruana en materia de amenazas híbridas en el ciberespacio**
Asesor Académico: Magíster Pablo Moscoso de la Cuba
Asesor Metodológico: Doctora Ofelia Carmen Santos Jiménez
Año: 2022

3. GRADO O TÍTULO

Bachiller (a) ( ) Licenciado (a) ( ) Maestro (a) (x)

4. LICENCIA Y AUTORIZACIÓN

A través del presente documento declaro que la tesis indicada en el numeral 2 es una creación de mi autoría y de mi exclusiva titularidad y que no infringe derechos de autor o de terceros, sobre la base de lo cual otorgo a la Academia Diplomática del Perú Javier Pérez de Cuéllar, licencia para reproducirla en cualquier tipo de soporte y en más de un ejemplar, sin modificar su contenido, con el único objeto de su preservación.
Asimismo,

( ) Autorizo el depósito inmediato de mi tesis en el Repositorio Digital de la Academia Diplomática, donde será de libre acceso y consulta.
(X) Autorizo que se deposite mi tesis a partir del 19/12/2022 en el Repositorio Digital de la Academia Diplomática, donde será de libre acceso y consulta.
( ) No autorizo que mi tesis se deposite en el repositorio digital de la Academia Diplomática (especificar el motivo)

_____

_____

Lima, 14 de noviembre de 2022

Firma del tesista

AGRADECIMIENTOS

Antes que nada, deseo agradecer a Dios por darme todas las oportunidades que he tenido hasta ahora.

En segundo lugar, a mis padres y mi familia, por apoyarme en la decisión de entrar a la ADP, y durante todo el proceso. Por sus palabras de aliento, su soporte incondicional y su cariño.

Luego, a todas las personas que de una manera u otra contribuyeron en la elaboración de esta tesis. Me encantaría poder nombrarlos a todos, pero la lista sería interminable, pero desde el fondo de mi corazón, mi eterna gratitud. Y un agradecimiento muy especial al Dr. Pablo Moscoso, por todas las reuniones y coordinaciones que me brindó, y por su apoyo en cada etapa.

Finalmente, a todos mis amigos, quienes me apoyaron especialmente con su aliento, su empuje y su fuerza.

Gracias eternas a cada uno de ustedes.

RESUMEN EJECUTIVO

Esta investigación busca brindar aportes para el diseño de los lineamientos de la política exterior peruana en materia de amenazas híbridas en el ciberespacio. Para ello, se planteó que esta investigación tenga un enfoque cualitativo, con un alcance descriptivo y un diseño de teoría fundamentada. Asimismo, para el recojo de información se utilizaron entrevistas, aplicando una guía de entrevista, y análisis documental, a través de una lista de cotejo. A partir de ello, se verificó la aproximación doctrinaria a las definiciones de amenazas híbridas (así como sus categorías de conflicto híbrido y guerra híbrida), así como el ciberespacio, las ciberoperaciones y los ciberataques. Luego de ello se definió que, para ser respondidas aplicando las normas de derecho internacional, se requería que el ciberataque sea equiparable a un ataque armado y atribuible a un Estado. Además, se determinó que, dependiendo del contexto en que ocurra un ciberataque (en tiempo de paz o en un conflicto armado), corresponde aplicar normas del *ius ad bellum* o *ius in bello*. Finalmente, se realizó un análisis comparativo del tratamiento que dan distintos Estados y organizaciones internacionales de las amenazas híbridas en el ciberespacio. Ello confirmó la necesidad de que el Perú incorpore estos fundamentos a su política exterior en esta materia, para lo cual se propone un modelo conceptual que incorpora los elementos antes descritos.

Palabras clave: amenaza híbrida, conflicto híbrido, guerra híbrida, ciberataque, ataque armado convencional, atribución a un Estado, *ius ad bellum*, *ius in bello*.

ABSTRACT

This research seeks to contribute to the design of Peruvian foreign policy guidelines on hybrid threats in cyberspace. For this purpose, it was proposed that this research should have a qualitative approach, with a descriptive scope and a grounded theory design. Likewise, for the collection of information, interviews were used, applying an interview guide, and documentary analysis, through a checklist. From this, the doctrinal approach to the definitions of hybrid threats (as well as their categories of hybrid conflict and hybrid warfare), as well as cyberspace, cyber operations and cyber-attacks were verified. It was then defined that, to be responded to by applying the norms of international law, it was required that the cyberattack be comparable to an armed attack and attributable to a State. In addition, it was determined that, depending on the context in which a cyberattack occurs (in peacetime or in an armed conflict), the rules of *ius ad bellum* or *ius in bello* apply. Finally, a comparative analysis was made of the treatment given by different States and international organizations to hybrid threats in cyberspace. This confirmed the need for Peru to incorporate these fundamentals to its foreign policy in this matter, for which a conceptual model incorporating the elements described above is proposed.

Keywords: hybrid threat, hybrid conflict, hybrid warfare, cyber-attack, conventional armed attack, attribution to a State, *ius ad bellum*, *ius in bello*.

SIGLAS Y ACRÓNIMOS

Carta de la ONU: Carta de la Organización de las Naciones Unidas

CAI: Conflicto Armado Internacional

CANI: Conflicto Armado No Internacional

CCFFAA: Comando Conjunto de las Fuerzas Armadas del Perú

CCDCOE: Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN

CICR: Comité Internacional de la Cruz Roja

COCID: Comando Operacional de Ciberdefensa

CIJ: Corte Internacional de Justicia

D. S.: Decreto Supremo

Dec. Leg.: Decreto Legislativo

DDH: Dirección de Derechos Humanos

DGM: Dirección General de Asuntos Multilaterales y Globales

DIH: Derecho internacional humanitario

DSD: Dirección de Seguridad y Defensa

FAP: Fuerza Aérea del Perú

GGE: Grupo de Expertos Gubernamentales sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional

Hybrid COE: Centro Europeo de Excelencia para Contrarrestar las Amenazas Híbridas

Manual de Tallinn 2.0: Manual de Tallinn 2.0 sobre el Derecho Aplicable a la Ciberguerra

OEWG: Grupo de Trabajo de Composición Abierta sobre los avances en el ámbito de la información y las telecomunicaciones en el contexto de la seguridad internacional

ONU: Organización de las Naciones Unidas

OTAN: Organización del Tratado del Atlántico Norte

INDICE

INDICE DE TABLAS Y FIGURAS

INTRODUCCIÓN

La presente investigación busca brindar aportes para el diseño de los lineamientos de la política exterior peruana en materia de amenazas híbridas en el ciberespacio, a través de la aplicación de las normas de derecho internacional que correspondan.

La necesidad de encontrar este marco normativo es que, en un mundo cada vez más globalizado, e integrado digitalmente, los Estados enfrentan nuevas amenazas a su seguridad e integridad. Dichas amenazas van desde el robo de datos, ya sea a civiles e incluso al mismo gobierno, hasta el daño a infraestructura crítica, generando afectación en la prestación de servicios públicos, con el consecuente impacto en la sociedad.

Por ejemplo, a inicios de octubre de este año, el Comando Conjunto de las Fuerzas Armadas (CCFFAA) fue víctima de una intervención de más de 283,000 correos electrónicos, en los cuales se expuso planes de guerra, entre otra información sensible. Ahora bien, para efectos de esta tesis, se tomará como caso más relevante la serie de ciberataques iniciados el 27 de abril del 2007 contra Estonia, a raíz de la iniciativa del gobierno de este país de mover la escultura del Soldado de Bronce (que conmemoraba el apoyo soviético a la liberación de Estonia durante la Segunda Guerra Mundial). A través de *botnets*[1], se afectó a servidores de diversas instituciones estonias, así como bancos y medios de prensa. Ello tuvo un impacto directo en la población, que vio el colapso del sistema financiero, así como la imposibilidad de acceder a servicios básicos que dependían directamente de las redes de tendido eléctrico.

Es así como autores como Anthony Craig y Brandon Valeriano (2018)

[1] Un botnet es el uso de “virus troyanos especiales para crear una brecha en la seguridad de los ordenadores de varios usuarios, tomar el control de cada ordenador y organizar todos los equipos infectados en una red de "bots" que el cibecriminal puede gestionar de forma remota” (Kaspersky, s.f.).

señalan que el ciberespacio es el quinto dominio de la guerra (siendo los otros tierra, mar, aire y espacio ultraterrestre) (p. 85). Es por ello que ahora resulta común hablar no solo de amenazas tradicionales (militares), sino que surge el concepto de amenazas híbridas, a las que autores como Ardila y Jiménez (2018) y Astudillo (2020)[2] entienden como amenazas que combinan medios tradicionales y no tradicionales. En esta línea, autores como Ashley Deeks (2013) y Michael Schmitt (2016) consideran que la creciente utilización del ciberespacio para fines militares, en tanto sea atribuida a un Estado, debe ser considerada como una amenaza híbrida.

Autores como Melzer (2011) y Malekos Smith (2018) han planteado la posibilidad de que las amenazas híbridas en el ciberespacio sean respondidas aplicando las normas sobre el uso de la fuerza, e incluso, en ciertos casos, las normas del derecho internacional humanitario. Sin embargo, su aplicación ha sido materia de controversia, ya que los Estados han adaptado esta normativa de diversas maneras para hacer frente a esta nueva forma de amenazas.

Ahora bien, esta situación podría sonar ajena a un país como el Perú. Sin embargo, tan solo el año pasado, nuestro país sufrió más de 11.5 mil millones de ciberataques, siendo el tercer país más afectado de la región (Agencia Peruana de Noticias Andina, 2022). Además, si bien es cierto que, por ejemplo, las filtraciones sufridas por el CCFFAA no han sido similares a los ciberataques perpetrados contra Estonia, la cantidad de ciberataques refleja que nuestro país es profundamente vulnerable ante este tipo de amenazas. Finalmente, el desarrollo normativo de este tema es escaso, y los trabajos de investigación no han abordado este nuevo tipo de amenazas. Por ello, resulta necesario que nuestro país adopte una posición coherente con las normas de derecho

[2] Cabe resaltar que la Fiscalía ha acusado a César Astudillo por el delito de organización criminal. Esta investigación únicamente hará referencia a sus estudios sobre amenazas híbridas, y no busca exculparlo de dicha acusación fiscal.

internacional para pronunciarse en caso un ataque de la magnitud del de Estonia ocurriera, ya sea en el Perú.

El Ministerio de Relaciones Exteriores, al ser parte del Sistema Nacional de Defensa, tiene un rol fundamental en la formulación de las políticas de defensa del país, especialmente en la aplicación e interpretación de las normas de derecho internacional que correspondan. Por ello, esta investigación pretende desarrollar recomendaciones respecto de la posición que el Perú podría adoptar en esta materia, señalando el marco normativo del derecho internacional que debe aplicarse para responder a las amenazas híbridas en el ciberespacio.

La presente investigación está dividida en tres partes. Luego de la presente introducción, el primer capítulo brinda un marco teórico en el que se explica qué es una amenaza híbrida en el ciberespacio y cuáles son las principales normas aplicables, tanto a nivel internacional como a nivel nacional. En el segundo capítulo se desarrolla la metodología empleada para la elaboración de esta investigación. En el tercer capítulo se analizará si la normativa peruana está en concordancia con las normas del derecho internacional, y cuál es la posibilidad de acción desde Cancillería, y se realiza un estudio comparativo de cómo se han recogido las normas del DIP en otros Estados y Organizaciones Internacionales, para luego recomendar cuál podría ser la posición del Perú en materia de amenazas híbridas en el ciberespacio. Finalmente, se presentarán las conclusiones y recomendaciones.

CAPÍTULO I

MARCO TEÓRICO

ESTADO DE LA CUESTIÓN:

Aproximación a las amenazas híbridas en el ciberespacio:

Conceptualización de las amenazas híbridas:

Antes de ingresar a estudiar las amenazas híbridas en el ciberespacio, creemos importante partir de la definición de amenazas, como concepto base de esta investigación. La Política Nacional Multisectorial de Seguridad y Defensa Nacional al 2030, aprobada por Decreto Supremo 005-21-DE, las define de la siguiente manera:

> Conjunto de situaciones, actividades o acciones desfavorables originadas por las actitudes, comportamientos, conductas y prácticas de actores estatales y/o no estatales, nacionales y transnacionales, con intereses antagónicos u opuestos al Estado y a las personas; o también por la acción del promotor de un suceso real; con la capacidad y la intención de hacer daño a nuestros intereses nacionales para alcanzar sus fines individuales o colectivos. (*D.S. 005-21-DE*, 2021, p. 28)

De la definición precitada, se desprende que una amenaza se compone de cuatro elementos. Primero, que está perpetrada por un actor humano, sea estatal o no estatal. Segundo, este actor humano debe tener la intención de ejecutar una acción perjudicial contra el Estado, en tanto ésta le reporta beneficios. Tercero, esta intención debe poder juzgarse a partir del seguimiento de las acciones del actor humano. Por ejemplo, realizar un análisis de sus

capacidades económicas y militares. Finalmente, en cuarto lugar, el actor humano debe tener la capacidad de causar daño. Es así como, en tanto concurran la capacidad y la intención, podrá hablarse de la existencia de una amenaza.

Las amenazas híbridas, como se verá en el presente Capítulo, incorporan medios convencionales (como los militares) y no convencionales (como los económicos y la desinformación) como parte de las capacidades de los actores humanos. Sin embargo, esta clase de amenaza tiene un desarrollo reciente, por lo que su contextualización resulta compleja. Por ello, antes de brindar una definición, es más conveniente estudiar el desarrollo histórico de éstas.

John J. McCuen (2008) sugiere que las amenazas híbridas son un concepto que, en apariencia, podría parecer novedoso. Sin embargo, en opinión de este autor, la historia ha demostrado que todos los conflictos tienen el potencial de ser híbridos, pues la mayoría de estos no ha sido únicamente convencional, tal y como sucedió durante el conflicto de Vietnam, o en la invasión a Afganistán. Lo único que ha cambiado, entonces, son los medios no convencionales empleados.

Por su parte, Christine Chinkin y Mary Kaldor (2017) opinan que las guerras nuevas realmente no lo son, sino que se usa este término para enfatizar que "la violencia política contemporánea es diferente de la concepción de 'guerra antigua'" (p. 6) [traducción propia]. En palabras del general ruso Valery Gerasimov (2013, citado por Chinkin & Kaldor, 2017), "las guerras ya no son declaradas, y, una vez que comienzan, siguen un patrón poco familiar, (…) [ya que] el uso de fuerzas especiales, la explotación de la oposición interna, así como las campañas de información son los métodos y medios de guerra contemporáneos" (p. 5-6). Sin embargo, estas autoras sí señalan que estas nuevas formas de violencia requieren de un tratamiento distinto, ya que tienen objetivos, actores y medios y métodos de combate diferentes a los

convencionales.

En la misma línea, el jurista español Carlos Galán (2018) señala que la génesis de las amenazas híbridas radica en la "naturaleza cambiante del orden mundial, cuyos componentes sociales, políticos y económicos no han dejado de alterarse desde el fin de la Guerra Fría" (pp. 5-6), lo cual ha planteado nuevas amenazas a la seguridad de los Estados. Asimismo, sugiere que el desarrollo tecnológico, así como los entornos digitales y la rapidez de difusión de la información, han creado nuevos escenarios en los que la acción estatal debe desplegarse con el fin de garantizar su seguridad (p. 6). El reto para los Estados, entonces, consiste en responder a estas nuevas amenazas en escenarios como el internet y las redes sociales. Sin embargo, en línea con lo señalado por Galán, la dificultad radica en la escasa regulación que existe para abordar nuevas amenazas, y así como respecto de los parámetros de acción en los nuevos escenarios.

Por otro lado, Frank Hoffman, citado por Georgios Giannopoulos, Hanna Smith y Marianthi Theocharidou (2020), sugiere que las amenazas híbridas tienen su origen en las nuevas formas de conflictividad, tales como los conflictos desestructurados[3] y los conflictos asimétricos[4]. Así las cosas, este autor sugiere que estas nuevas formas de conflictividad se distinguen por emplear estrategias diferenciadas para librar los conflictos, como los ataques de baja intensidad, pero también nuevos medios para librar la guerra, como el ciberespacio. Pero, además, Giannopoulos et al. sugieren que el empleo de la palabra 'amenaza híbrida' comenzó en el 2014, a raíz de la anexión de Crimea, para referirse a la presión que ejerció Rusia a través de diferentes herramientas, similares a las

[3] Según Salmón (2016) los conflictos desestructurados se refieren a "enfrentamientos generalizados entre diversos grupos, sin que ninguno de ellos represente al Estado" (p. 160-161).
[4] Según Salmón (2016) los conflictos asimétricos "se producen cuando un Estado, por más poderoso que sea, es atacado por actos terroristas globalizados" (p. 166).

utilizadas en el contexto de las nuevas formas de conflictividad, con el objetivo de legitimar su actuación.

De la revisión de los orígenes del concepto de “amenaza híbrida” se pueden observar algunos elementos comunes: la utilización de métodos y medios no convencionales, en entornos no tradicionales, que generan amenazas contra la seguridad del Estado. Es por ello por lo que Patrik Pawlak (2015), en una investigación realizada para el Parlamento Europeo, define a las amenazas híbridas como un “fenómeno resultante de la convergencia e interconexión de diferentes elementos que, juntos, derivan en una amenaza más compleja y multidimensional” [traducción propia]. Asimismo, el general estadounidense George W. Casey (2008, citado en Sánchez García, 2012) señala que las amenazas híbridas son “combinaciones diversas y dinámicas de capacidades convencionales, irregulares, terroristas y criminales” (p. 16).

La Unión Europea (2016) ha desarrollado estos conceptos al señalar lo siguiente:

> Si bien es cierto que las definiciones de las amenazas híbridas varían y deben seguir siendo flexibles para tener en cuenta su carácter evolutivo, el objeto de este concepto es subrayar la *mezcla de actividades coercitivas y subversivas*, de *métodos convencionales y no convencionales* (es decir, diplomáticos, militares, económicos y tecnológicos), que pueden ser *utilizados de forma coordinada por agentes estatales o no estatales* para *lograr objetivos específicos*, manteniéndose por debajo del umbral de una guerra declarada oficialmente. (p. 2) [énfasis propio]

La definición de la Unión Europea ya pone de manifiesto que las amenazas híbridas no implican solamente la utilización de diferentes medios

para realizar actividades tanto coercitivas (militares tradicionales) como subversivas, sino que pone énfasis también en los agentes que pueden realizar amenazas híbridas. Esto es, las amenazas híbridas pueden venir tanto de agentes estatales como de actores no estatales.

El Servicio Europeo de Acción Exterior (2018) ha desarrollado este concepto al señalar que "las amenazas híbridas *combinan actividades convencionales y no convencionales, militares y no militares*, que pueden ser *usadas de manera coordinada por actores estatales y no estatales* para *alcanzar objetivos políticos específicos*" (p. 1) [traducción propia] [énfasis propio]. Es así como confirma la definición brindada por la Unión Europea, en el sentido de que las amenazas híbridas pueden ser planteadas tanto por agentes del Estado, como por actores no estatales. Sin embargo, añade un nivel más de análisis respecto de las amenazas híbridas, y es que "estas amenazas se dirigen contra vulnerabilidades críticas y buscan crear confusión para impedir la toma de decisión rápida y efectiva" (p. 1) [traducción propia]. Dicho de otro modo, para poder afirmar que existe una amenaza híbrida, se requiere de una intención específica de aprovechar las vulnerabilidades de un Estado, para evitar la toma de decisiones. Es así como se puede afirmar que sólo los Estados pueden ser víctimas de amenazas híbridas[5].

El Centro de Excelencia para Contrarrestar las Amenazas Híbridas (Hybrid COE, por sus siglas en inglés) (s.f.) coincide con estos conceptos al caracterizar a las amenazas híbridas de la siguiente manera:

[5] Surge la duda respecto de si aquellas entidades que no cumplen con todos los criterios para ser consideradas como Estados pueden ser víctimas de amenazas híbridas. Este sería el caso, por ejemplo, de Hong Kong o Groenlandia. Esta tesis sostiene que sí es posible que sean víctimas de amenazas híbridas. Sin embargo, en tanto estas entidades son dependientes de Estados quienes ejercen ciertas competencias sobre el territorio de las entidades, se consideraría que la amenaza está dirigida contra estos Estados. Así, una amenaza contra Groenlandia se entendería dirigida contra Dinamarca, así como una amenaza contra Hong Kong se entendería dirigida contra China.

> Acciones coordinadas y sincronizadas que deliberadamente apuntan a Estados democráticos y sus vulnerabilidades sistémicas a través de un amplio rango de medios; Actividades que explotan el umbral de detección y atribución, así como las diferentes interfaces (guerra-paz, seguridad interna-externa, local-estatal, y nacional-internacional); Actividades dirigidas a influenciar diferentes formas de toma de decisión a nivel local (regional), estatal o institucional, y diseñadas para avanzar y cumplir los objetivos estratégicos del agente, a la vez que socavan o dañan al objetivo. [página web] [traducción propia]

Esta definición es quizás la que mejor engloba el concepto de amenazas híbridas, tal y como señalan Dick Zandee, Sico van der Meer y Adája Stoetman (2021), pues ha sido la más recogida en la diversa literatura especializada. Sin embargo, es importante señalar que la posibilidad de ser víctima de amenazas híbridas no debe limitarse únicamente a Estados democráticos, sino que cualquier Estado puede ser víctima de una amenaza híbrida, sin importar el tipo de régimen de gobierno (ver Munteanu, s.f.).

Claudio Payá y José María Luque (2018) recogen esta definición para concluir que las amenazas híbridas son todas aquellas manifestaciones de violencia, perpetrada tanto por actores estatales como no estatales, que buscan explotar vulnerabilidades de los Estados, usando para ello todos los recursos tradicionales (militares) o no tradicionales, con el objetivo de lograr su incapacitación o debilitamiento, o dificultar la toma de decisiones por parte de sus instituciones de gobierno.

De forma similar, Galán (2018) define a las amenazas híbridas de la siguiente manera:

> Acciones coordinadas y sincronizadas – con origen habitualmente,

> pero no solo, en los servicios de inteligencia de los agentes de las amenazas – que atacan deliberadamente vulnerabilidades sistémicas de los Estados y sus instituciones a través de una amplia gama de medios y en distintos sectores objetivos (políticos, económicos, militares, sociales, informativos, infraestructuras y legales). (p. 3)

La OTAN (2018), sin embargo, brinda una aproximación distinta respecto del objetivo de las amenazas híbridas, al señalar lo siguiente:

> Las amenazas híbridas combinan medios militares y no militares, tanto abiertos como encubiertos, incluyendo la desinformación, ciberataques, presión económica, despliegue de grupos armados irregulares, y uso de fuerzas armadas regulares. Los métodos híbridos se usan para desdibujar las líneas entre la guerra y la paz, y pretenden sembrar la duda en las mentes de la población objetivo. Se dirigen a *desestabilizar y socavar las sociedades*. [página web] [traducción propia] [énfasis propio]

Si bien la OTAN coincide con la Unión Europea en que las amenazas híbridas implican métodos y medios convencionales y no convencionales, sí añade una perspectiva distinta, al señalar que las amenazas híbridas deben estar dirigidas contra la población civil, desestabilizándola. No obstante, esto no está del todo reñido con las definiciones antes provistas, ya que coinciden en que el objetivo de las amenazas híbridas es socavar la estabilidad del Estado lo cual también puede ser alcanzado a través de la desestabilización de la población.

Por otro lado, Frank G. Hoffman (2007) analiza qué implica el uso del término híbrido, de la siguiente manera:

> El término “híbrido” captura tanto la organización como los medios. Organizacionalmente, pueden ser perpetradas por estructuras políticas jerárquicas, combinadas con células descentralizadas o unidades tácticas en red. Sus medios también serán híbridos en forma y aplicación. (…) Esto podría incluir Estados que mezclen capacidades de alta tecnología, como armas antisatélite, con terrorismo y guerra cibernética dirigida contra objetivos financieros. Los conflictos también incluirán organizaciones híbridas como *Hezbollah* y *Hamas*, que emplean un conjunto diverso de capacidades. Adicionalmente, los Estados pueden cambiar sus unidades convencionales a formaciones irregulares y adoptar nuevas tácticas. (Hoffman, p. 28) [Traducción propia]

En este sentido, se puede afirmar que el carácter híbrido de una amenaza se refiere a que puede ser perpetrada tanto por actores estatales como no estatales, y porque se utilizan métodos tanto convencionales como no convencionales.

Ahora bien, Galán (2018) resalta que en la doctrina sobre seguridad y defensa no es extraño encontrar el uso de términos como guerra híbrida, amenaza híbrida, ataque híbrido, como si se tratara de sinónimos, y, por tanto, intercambiables. Ello ocurre, en opinión de Pawlak (2015), debido al entorno global cambiante, que ha llevado a la aparición de nuevos retos en materia de seguridad, así como nuevos actores. No obstante, estos conceptos no son intercambiables, debido a que responden a diferentes niveles de intensidad e intencionalidad de los actores (Pawlak). Por ello, se pueden identificar tres conceptos claves: amenaza híbrida, conflicto híbrido, y guerra híbrida.

Respecto del primer concepto, a partir de las definiciones brindadas en párrafos anteriores, se puede llegar a una definición de amenazas híbridas a

partir de tres características:

- Se trata de la amenaza o recurso de la violencia, a través de la combinación de métodos y medios tradicionales (fuerza militar) y no tradicionales (tecnológicos, diplomáticos, económicos, entre otros), dificultando así el umbral de detección, y, por ende, la posibilidad de atribución a actores específicos.
  Por ejemplo, durante el conflicto ruso-ucraniano, no sólo se dio una invasión militar en el sentido tradicional, perpetrada el 24 de febrero del 2022, sino que también el proveedor ucraniano de internet Ukrtelecom sufrió un ciberataque, atribuido al ejército ruso, que afectó las capacidades de transmisión de datos, y, por ello, las telecomunicaciones en el país (Vallance, 2022) [página web].

- Son acciones que pueden ser realizadas tanto por actores estatales como por actores no estatales, pero van dirigidas contra un Estado o su población.
  En este sentido, y volviendo al ejemplo del conflicto ruso-ucraniano, Galán (2018) señala que, durante la anexión de Crimea en el 2014, el gobierno ruso no sólo apeló al envío de tropas de su ejército, sino también de “hombrecitos verdes”, grupos paramilitares que realizaron diversos tipos de ataques al ejército ucraniano (p. 12).

- Son acciones dirigidas a socavar las vulnerabilidades sistémicas de un Estado, disminuyendo su capacidad de reacción y también su capacidad de toma de decisiones, con el fin de lograr objetivos

estratégicos.

Galán (2018) señala que, en el contexto del conflicto ruso-ucraniano, Rusia aprovechó las vulnerabilidades ucranianas, debido a su dependencia del gas ruso, para evitar su integración como miembro de la Unión Europea (p. 12).

El Servicio Europeo de Acción Exterior (2018) señala que las amenazas híbridas incluyen varias situaciones como los actos terroristas, ciberataques (serán desarrollados con mucha mayor profundidad, al ser el objeto de estudio de esta tesis), acciones de grupos delictivos armados, disputas marítimas, actos económicos hostiles, boicots diplomáticos, operaciones militares encubiertas, entre otros. A partir de este listado, se puede observar, entonces, que las amenazas híbridas engloban un conjunto de actos que pueden o no implicar el uso de violencia. Por lo tanto, se puede afirmar que, al hablar de amenazas híbridas, se trata de un género, que a su vez se subdivide en dos especies, dependiendo del nivel de intensidad del uso de la fuerza.

En primer lugar, el conflicto híbrido, según Pawlak (2015), debe ser definido de la siguiente manera:

> Situación en la cual las partes se abstienen del uso manifiesto de la fuerza, y reposan en una combinación de intimidación militar (que no llega a ser un ataque), explotación de vulnerabilidades económicas y políticas, y medios tecnológicos o diplomáticos para lograr objetivos. (p. 1) [traducción propia]

Sin embargo, en opinión del Consejo de Europa (2018), la característica distintiva de esta especie de amenazas híbridas es que no existe confrontación armada. En la misma línea, la Comisión Europea (2016) ha señalado que el

factor diferenciador es que los conflictos híbridos se mantienen "por *debajo del umbral* de una *guerra declarada oficialmente*. (p. 2) [énfasis agregado]. Es importante precisar que, si bien la definición habla de guerra declarada oficialmente, debe entenderse más bien que aplica a todo conflicto armado que cumpla con los criterios de intensidad y organización, tal y como se señaló en el Caso Tadic (1999).

En la misma línea, Galán considera que se trata de situaciones en las que "Estados o actores no estatales emplean medios no violentos como instrumentos de guerra y los integran con el empleo de la fuerza armada o la amenaza de la fuerza" (p. 5). Para entender esta definición es importante precisar ciertos conceptos. En primer lugar, la violencia se refiere a "actos que caracterizan las hostilidades" (Verri, 2014, p. 113). Por lo tanto, cuando Galán se refiere al "empleo de la fuerza armada o la amenaza de la fuerza", se refiere a los medios tradicionales, es decir, medios de guerra. En línea con lo señalado por Verri (2014), los medios de guerra, o medios violentos, son "armas y sistemas de armas a través de los cuales se ejercer materialmente la violencia contra el adversario" (p. 62). En contraposición, es posible señalar que los medios no violentos son aquellos que no tenían como objetivo causar daños a un adversario. Sin embargo, de la definición de Galán se desprende que, en un conflicto híbrido, se utilizan estos medios como instrumentos de violencia, es decir, se usan en combinación con otros medios con el objetivo de amenazar o usar la fuerza.

Además, es importante resaltar que "los actos aislados y esporádicos de violencia no son suficientes para constituir un conflicto armado" (Verri, 2014, p. 113). Por ello, es posible afirmar que un conflicto híbrido implica la amenaza o uso de la fuerza, pero no alcanza el estado de conflicto armado. Esta aproximación resulta más adecuada, ya que, como se verá más adelante, permite elaborar una respuesta que articule las normas que corresponden del

derecho internacional.

Por otro lado, Pawlak (2015) define a la guerra híbrida como una "situación en la que un Estado resuelve usar abiertamente la fuerza armada contra otro Estado o actor no estatal, en adición a una combinación de otros medios (por ejemplo, económico, político y diplomático)" (p. 1). Galán añade que la guerra híbrida "combina capacidades cinéticas convencionales (acciones armadas no encubiertas) con tácticas irregulares" (p. 4) y, por lo tanto, resulta más preciso utilizar este término cuando existe un conflicto armado que cumpla con los criterios de intensidad y organización (ver Salmón, 2016; Tribunal Penal Internacional para la ex-Yugoslavia, 1999), ya sea de carácter internacional o no internacional, y, por lo tanto, corresponde la aplicación del DIH.

Sánchez García (2012), sin embargo, da una definición bastante más precisa, en los siguientes términos:

> Un conflicto armado en el que se utilizan toda clase de medios y procedimientos ya sea la fuerza convencional o cualquier otro medio irregular como la insurgencia, el terrorismo e incluso otros más sofisticados mediante el empleo de las últimas tecnologías y en las que la influencia sobre la población resulta vital. (pp. 20-21)

Queda claro que tanto los conflictos híbridos, como las guerras híbridas son especies del género de amenazas híbridas, debido a que comparten las tres características fundamentales antes señalas: emplean mecanismos convencionales y no convencionales, pueden estar perpetradas por actores tanto estatales como no estatales, y tienen por objetivo socavar las vulnerabilidades del sistema. Sin embargo, la diferencia entre ambos radica en el nivel de intensidad que supone la utilización de los mecanismos convencionales y no convencionales.

En los conflictos híbridos se usa tanto la amenaza como del uso de la fuerza a través de la combinación de métodos convencionales y no convencionales, pero en un contexto de paz. En la guerra híbrida ello ocurre en el contexto de un conflicto armado. Por lo tanto, requieren una respuesta jurídica diferenciada. La interrogante surge cuando se usa la fuerza a través de los medios no convencionales. Esta tesis abordará esta cuestión desde la perspectiva del uso de la fuerza en el ciberespacio.

Cuadro No. 1: Definición de amenazas híbridas, conflictos híbridos, y guerras híbridas

Amenaza híbrida	Son acciones que implican la amenaza o recurso a la violencia, combinando métodos y medios tradicionales (fuerza militar) y no tradicionales (tecnológicos, diplomáticos, económicos, etc.), perpetradas por actores estatales o no estatales, dirigidas contra un Estado o su población, y con el objetivo de explorar sus vulnerabilidades sistémicas.
Conflicto híbrido	Son amenazas híbridas perpetradas usando la fuerza, más no en un contexto de conflicto armado.
Guerra híbrida	Son amenazas híbridas perpetradas como parte de un conflicto armado.

Fuente: Elaboración propia

Conceptualización de las amenazas híbridas en el ciberespacio:

Galán (2018) pone énfasis en que uno de los entornos más importantes sobre los cuales se despliegan los efectos de las amenazas híbridas es el ciberespacio, debido a que se trata de una herramienta más versátil para la consecución de los objetivos del Estado o actor no estatal atacante.

Para entender a mayor detalle este concepto, corresponde partir desde la concepción de qué es el ciberespacio, que la Real Academia de la Lengua Española (2014) define como el "ámbito virtual creado por medios informáticos" [página web]. Nils Melzer (2011) añade que se trata de "una red global interconectada de información digital e infraestructura de comunicación, que incluye la Internet, las redes de telecomunicación, los sistemas de computación y la información que reside ahí" (p. 4) [traducción propia].

El Departamento de Defensa de los Estados Unidos (2021a) desarrolla esta definición de la siguiente manera:

> Es un dominio global dentro del entorno de la información, que consiste en redes interdependientes de infraestructuras para la tecnología de la información y data residente, incluyendo la internet, las redes de telecomunicación, sistemas de computadora, y procesadores y controladores integrados. [Traducción propia]

En su discurso ante el Cibercomando de los Estados Unidos, el Consejero General del Departamento de Defensa, Paul C. Ney Jr., señaló que el ciberespacio, por su propia naturaleza, está en un estado de transformación constante. En este sentido, "permite la transmisión de datos a través de fronteras internacionales en nanosegundos – controlado más por individuos o máquinas que por los gobiernos – difundiendo ideas a audiencias dispersas y, en algunos casos, generando efectos físicos en lugares alejados" [discurso] [traducción propia], por ello "las nuevas tecnologías son parte de todos los aspectos de una operación militar, creando oportunidades y retos" [discurso] [traducción propia].

De la misma opinión es Charles Weiss (2015), quien considera que, "en el frente de la seguridad, [la tecnología] ha introducido un nuevo dominio de ciberguerras junto con los dominios terrestres, aéreos, marítimos y espaciales, y

ha creado nuevas capacidades y vulnerabilidades para una guerra asimétrica" (p. 415) [traducción propia]. Es así como se puede afirmar que el ciberespacio presenta un reto especial para la seguridad de los Estados, ya que se constituye como un nuevo escenario en donde se gestan amenazas, y sobre el cual se requiere la actuación de los Estados.

En esta línea, Giannopoulos et al. (2020) señalan que el ciberespacio "provee un nuevo mecanismo que incrementa la velocidad, difusión y poder de un ataque, asegurando anonimidad y pocas posibilidades de detección" (p. 28) [traducción propia]. Sin embargo, el principal reto que plantea el ciberespacio, en opinión de estos autores, es que "el bajo precio de entrada, anonimidad y asimetrías en la vulnerabilidad, significan que actores más pequeños tienen la capacidad de ejercer más poder en el ciberespacio" (p. 28) [traducción propia]. Dicho de otro modo, el ciberespacio es utilizado de modo generalizado por los Estados, por lo cual se incrementa la vulnerabilidad de estos, así como de la población civil, que se desenvuelve en este ámbito.

En esta línea, Galán (2018) señala que existen diversos tipos de acciones que pueden perpetrarse desde el ciberespacio, tales como el ciberespionaje, la ciberdelincuencia, o el uso de redes sociales para difundir información falsa o revelar información comprometedora (p. 11), que explotan dicha vulnerabilidad, generando efectos perjudiciales. El Departamento de Defensa de Estados Unidos (2021c) denomina tales acciones como operaciones en el ciberespacio, y las define como "el uso de capacidades en el ciberespacio [dispositivos o programas de computadoras] con el objetivo principal de alcanzar objetivos en, o por medio del, ciberespacio" [traducción propia].

Ahora bien, no todas las operaciones en el ciberespacio pueden ser consideradas como amenazas híbridas. Solo alcanzarán tal categoría aquellas que se empleen como parte de una combinación de métodos convencionales (amenaza o uso de la fuerza militar) y no convencionales (en este caso, la

tecnología), que sean atribuibles a un Estado o actor no estatal, bajo ciertas condiciones que se abordarán más adelante, y tengan por objetivo afectar las capacidades del Estado. Sin embargo, tal y como se puede colegir de la definición, no todas las operaciones en el ciberespacio implican la amenaza o el uso de la fuerza, ni de modo directo ni indirecto. Por ello, no todas pueden ser tratadas como conflictos híbridos, o como guerras híbridas.

No obstante, sí existe un tipo de ciberoperaciones que requiere de mayor desarrollo, pues implican directamente el uso de la fuerza: los ciberataques. El Departamento de Defensa de los Estados Unidos (2021b) los llamaba ataques en el ciberespacio, y los define de la siguiente manera:

> Acciones tomadas en el ciberespacio que crean efectos de negación[6] considerables (por ejemplo, la degradación, disrupción o destrucción[7]) en el ciberespacio, o manipulación que lleva a negación que aparece en un dominio físico[8], y que es considerado como una forma de fuego[9]. [Traducción propia]

La Junta de Jefes de Estado Mayor de los Estados Unidos (1998, citada en Schmitt, 1999), de modo similar, define a los ciberataques como "operaciones para interrumpir, denegar, degradar o destruir información albergada en computadoras y redes de computadora, o a las computadoras y redes en sí

[6] Por efecto de negación, debe entenderse cualquier medida que tenga como objetivo privar o limitar al enemigo del acceso, uso o disfrute de personal e infraestructura (Departamento de Defensa, 2021d, p. 61) [traducción propia].
[7] Por degradación, disrupción o destrucción debe entenderse como "demoliciones, interrupciones o inutilización de productos manufacturados, de instalaciones y de materiales efectuadas – con propósitos ofensivos o defensivos- en el transcurso de operaciones militares" (Verri, 2014, p. 34).
[8] El dominio físico hace referencia a la tangibilidad, es decir a bienes tangibles, corpóreos (Departamento de Defensa, 2021d, p. 168) [traducción propia].
[9] La forma de fuego es "el uso de armas u otras acciones que tienen por objetivo crear efectos letales o no letales en un objetivo" (Departamento de Defensa, 2021d, p. 82) [traducción propia].

mismas" (p. 888)[10].

La Regla 30 del Manual de Tallinn 2.0 sobre el Derecho Aplicable a la Ciberguerra[11] (2017) amplía esta definición al señalar al ciberataque como una "ciber operación, ya sea ofensiva o defensiva, que se espera razonablemente que cause daños o muerte a personas, o daños o destrucción a objetos". Es importante resaltar que, según el comentario de esta regla, la discusión respecto de los objetos no solo debe limitarse a "personas u objetos físicos" (Manual de Tallinn 2.0 sobre el Derecho Aplicable a la Ciberguerra [Manual de Tallinn 2.0], 2017, p. 107) [traducción propia], sino que también deben considerarse "las ciber operaciones realizadas contra datos (que son entidades no físicas)" (p. 108) [traducción propia]. Así las cosas, si un ciberataque se dirige contra datos, y afecta a personas o infraestructuras, claramente se considerará esta operación como un ataque armado (Manual de Tallinn 2.0, 2017, p. 108).

Michael N. Schmitt (1999) encuentra cuatro características comunes a todos los ciberataques, que el Manual de Tallinn 2.0 ha recogido en su definición. Primero, que estos se dirigen contra una nueva categoría de objetivos, es decir las computadoras y redes, es decir, contra la infraestructura digital (p. 888). Aquí es posible añadir, en línea con los señalado por el Manual de Tallinn 2.0, que, si bien el objetivo del ataque son las redes y computadoras, su finalidad es afectar tanto a esa infraestructura como a la población. En segundo lugar, los ciberataques implican que el concepto de uso de la fuerza ha mutado, ya que, hoy por hoy, un ataque podría darse únicamente a través de la

[10] Esta definición se ha mantenido inalterada desde 1998, y fue recogida por el Departamento de Defensa en el DOD Dictionary of Military and Associated Terms, del 2021.

[11] El Manual de Tallinn sobre el Derecho Aplicable a la Ciberguerra fue elaborado por un grupo de veinte expertos en derecho internacional, liderado por Michael Schmitt, a solicitud del Centro de Excelencia en Defensa Cibernética Cooperativa de la OTAN, entre el 2009 y el 2012. Se trata de un documento no vinculante, que busca estudiar la aplicación de las normas de *ius ad bellum* y *ius in bello* a los ciberataques. Se preparó una edición revisada en el 2017, llamada Manual de Tallinn 2.0. (Manual de Tallinn 2.0, 2017). Adicionalmente, en el ámbito de la OTAN, se invocan y aplican sus disposiciones como parte de sus resoluciones.

transferencia de comandos en una computadora (p. 888). En tercer lugar, si bien los ciberataques pueden resultar en la destrucción física de las redes e infraestructura digital, pero también puede tener otro objetivo, como causar una interrupción del servicio o alterar la transferencia de datos (p. 888). Por ejemplo, un ciberataque dirigido contra las redes de tendido eléctrico, como el que sucedió en Ucrania hacia finales de marzo (ver Tidy, 2022), no necesariamente tiene como finalidad destruir la infraestructura, sino reducir la capacidad de generación y transmisión de electricidad. Y finalmente, "los ciberataques amplían las nociones tradicionales de integridad territorial" o inviolabilidad territorial[12] (Schmitt, 1999, p. 888), ya que "en muchos casos, no implicarán el cruce de fronteras políticas por medio de ningún instrumento tangible del atacante, como fuerzas militares, equipos o proyectiles" (Schmitt, p. 888).

De la revisión de las características anteriores podemos apreciar que la definición de ciberataque puede encajar dentro de la de una amenaza híbrida si se produce junto con el empleo de medios militares tradicionales, ya que se trata de una acción que implica la amenaza o recurso a la violencia, usando medios no tradicionales (en este caso, las redes de sistemas y computadoras), que tiene por objetivo vulnerar la infraestructura tecnológica y digital de un Estado, afectando así tanto al gobierno como a la población. En este sentido, los ciberataques podrían ser componentes de una amenaza híbrida en el ciberespacio.

Habiendo situado a los ciberataques en el contexto de las amenazas híbridas, es importante señalar que Weiss (2015) se hace las siguientes preguntas: "¿Cuándo un ciberataque alcanza el nivel de un acto de guerra? Y cuando ello ocurre, ¿qué forma y nivel de retribución están justificados – y qué

[12] Se considera importante añadir la referencia a inviolabilidad territorial debido a que la integridad territorial se refiere a los casos de defensa ante la pérdida del territorio, mientras que la inviolabilidad territorial se refiere a protección ante el ingreso en el territorio de un Estado sin su autorización. (Murphy, 2006)

criterios deben ser usados como base de dicha justificación?" (p. 415) [traducción propia]. En la misma línea, Schmitt (1999) plantea dos cuestiones importantes. La primera es saber cuándo debe responderse a un ciberataque a través de las normas, ya sea del *ius ad bellum* o *ius in bello*, cuyas definiciones serán precisadas más adelante. Una vez definido esto, corresponde analizar cuál es el marco jurídico aplicable (*ius ad bellum* o *ius in bello*). En las próximas líneas, se analizarán estas interrogantes.

Cuadro No. 2: Definición de ciberataque en el contexto de una amenaza híbrida

Acción que implica la amenaza o recurso a la violencia, usando como medio no tradicional el ciberespacio y método no tradicional las ciberoperaciones, y que tiene por objetivo vulnerar la infraestructura tecnológica y digital de un Estado, afectando así tanto al gobierno como a la población. Para que sea respondido aplicando normas del *ius ad bellum* o *ius in bello*, debe: • Ser equiparable a un ataque armado. • Ser atribuible a un Estado.

Fuente: Elaboración propia

Ciberataques, en el contexto de una amenaza híbrida, que deben ser respondidos aplicando las normas *ius ad bellum* o *ius in bello*:

Es importante partir de la premisa de que no todo ciberataque, en el contexto de una amenaza híbrida, puede ni debe ser respondido aplicando normas sobre el uso de la fuerza. El Grupo Internacional de Expertos encargados de elaborar el Manual de Tallinn (2009, citado por Schmitt, 2016) es de la misma opinión, ya que señala que "las normas del *ius ad bellum* [y también las de *ius in bello*] aplican sólo a ciertas ciberoperaciones" (p. 1112) [traducción

propia]. Michael Sulmeyer (2017) también va en la misma línea, ya que, en su opinión, “el problema no es la falta de definición, sino la falta de consenso acerca de qué malas conductas en el ciberespacio necesitan ser detenidas” [página web] [traducción propia].

Es así como se considera que hay dos criterios que deben cumplirse, y se explicarán con mayor detalle. En primer lugar, es necesario que el ciberataque, en el contexto de una amenaza híbrida, sea equiparable a un ataque armado, y, por lo tanto, revista un criterio de gravedad. En segundo lugar, debe ser imputable a un Estado, a través de las reglas de responsabilidad estatal.

El ciberataque, en el contexto de una amenaza híbrida, debe ser equiparable a un ataque armado:

Schmitt (1999) señala que requerirán una respuesta aplicando las normas sobre uso de la fuerza en el Derecho Internacional todos aquellos ciberataques, en el contexto de una amenaza híbrida, siempre que vulneren la prohibición de la amenaza o uso de la fuerza, estipulada en el art. 2, numeral 4 de la Carta de Naciones Unidas[13]. Corresponde entonces analizar qué significa uso de la fuerza, para entender cuándo un ciberataque implica el uso de la fuerza.

Christine Gray (2018) señala que esta discusión es bastante compleja, ya que, en el contexto de la Guerra Fría, se debatió acerca de si este concepto abarcaba la coerción económica, la legítima defensa, el uso de la fuerza para efectos de la libre determinación de los pueblos, y la intervención en guerras civiles. Además, hacia el final de la Guerra Fría, la proliferación de nuevas formas de conflicto, impulsadas especialmente por actores no estatales, así

[13] El referido artículo señala lo siguiente: “Los Miembros de la Organización, en sus relaciones internacionales, se abstendrán de recurrir a la amenaza o al uso de la fuerza contra la integridad territorial o la independencia política de cualquier Estado, o en cualquier otra forma incompatible con los Propósitos de las Naciones Unidas.”

como la aparición de nuevos tipos de armas, generó un nuevo debate acerca del uso de la fuerza (Gray, 2018).

La Corte Internacional de Justicia (1986) (CIJ), en el caso de Nicaragua contra Estados Unidos[14], se basó en la Resolución 3314 (XXIX) de la Asamblea General de las Naciones Unidas, Definición de la Agresión (1974), para equiparar el uso de la fuerza a una agresión. Esta resolución, en su art. 2 señala que se considerará que un acto de agresión es un uso de la fuerza no permitido (Asamblea General de las Naciones Unidas, 1988). Asimismo, el art. 3 de dicha resolución caracteriza como actos de agresión a las invasiones y ocupaciones militares, el bombardeo, el bloqueo de puertos, el ataque de fuerzas armadas, el envío de mercenarios y bandas armadas al territorio de otro Estado, entre otros. En la misma línea, Pietro Verri (2014) añade que una agresión es el "empleo de la fuerza armada por un Estado contra la soberanía, la integridad territorial o la independencia política de otro Estado" (p. 3), y pone como ejemplos la invasión u ocupación militar, el bombardeo, el bloqueo de puertos y el envío de mercenarios.

En la misma línea, la Resolución 42/22 de la Asamblea General de las Naciones Unidas (1987), Declaración sobre el mejoramiento de la eficacia del principio de la abstención de la amenaza o de la utilización de la fuerza en las relaciones internacionales, reitera la prohibición del uso de la fuerza y añade que "los Estados tienen el deber de abstenerse de toda intervención armada y de

[14] El caso relativo a actividades militares y paramilitares en y contra Nicaragua se refiere a las acciones de Estados Unidos para derrocar el régimen socialista establecido en Nicaragua, y a la discusión de si éstas implicaban una vulneración de la prohibición del uso de la fuerza. En 1979, el Frente Sandinista de Liberación Nacional derrocó al gobierno de Anastasio Somoza. Si bien en un principio Estados Unidos apoyó a la nueva Junta Revolucionaria de Gobierno, en 1981, lo retiró para comenzar a apoyar a la guerrilla de Los Contras (opositores al gobierno), establecida en El Salvador. Hacia 1983, agentes de la CIA no sólo entrenaban a los Contras, sino que también les proveían armas y apoyo logístico, para realizar múltiples atentados contra el gobierno nicaragüense. (*Caso relativo a las actividades militares y paramilitares en y contra Nicaragua (Nicaragua contra los Estados Unidos de América) (Fondo del asunto)*, 1986; Kammerhofer, 2018)

cualesquiera otras formas de injerencia o de tentativa de amenaza contra la personalidad del Estado o de sus elementos políticos, económicos y culturales" (1988, sec. 7).

En este sentido, es posible afirmar que el uso de la fuerza se refiere tanto a las intervenciones armadas como a los actos de agresión perpetrados por Estados, esto es, cuando exista un ataque armado. Verri (2014) lo define como "un acto de violencia cometido contra el adversario, cuyo objetivo es tanto ofensivo como defensivo e independientemente del territorio sobre el cual se lleva a cabo" (p. 11), y señala que implica operaciones que afecten tanto a la población civil como a objetivos en tierra.

La pregunta entonces es si es posible equiparar los ciberataques a ataques armados. El Ministerio de Defensa del Reino Unido (2016) considera que una amenaza híbrida constituirá un ataque armado "si su método, gravedad e intensidad de fuerza es tal que sus efectos son equivalentes a aquellos alcanzados por un ataque cinético[15] que alcanza el nivel de un ataque armado" [traducción propia] (p. 13).

El Manual de Tallinn 2.0 (2017) es de la misma opinión, ya que, en su Regla 11, señala que "una ciber operación constituye un uso de la fuerza cuando su escala y efectos son comparables a operaciones no cibernéticas que alcanzan el nivel de uso de la fuerza" (p. 45). Para entender qué significa el uso de la fuerza, se basan en las conclusiones de la CIJ, en el caso de Nicaragua contra Estados Unidos, para señalar que la escala y efectos son un criterio que permite analizar los factores cuantitativos y cualitativos de un ataque[16].

[15] Un ataque cinético se refiere al "uso de fuerza militar activa, como los bombardeos y el uso de armas" (Post Staff Report, 2011) [página web] [traducción propia].

[16] La Corte Internacional de Justicia, en el caso de Nicaragua v. Estados Unidos (1986), se refiere al envío de tropas irregulares por parte de Estados Unidos al territorio nicaragüense, y analiza si esto se constituye como un ataque armado, en función a su escala y efectos. Al respecto, concluye lo siguiente: "La Corte no ve razón para negar que, en el derecho consuetudinario, la prohibición de los ataques armados pueda aplicarse al envío por parte de un Estado de bandas armadas al territorio de otro Estado, si tal operación, debido a su escala y efectos, hubiera sido clasificado como un ataque

Así, lo primero que debe analizarse es la severidad del ataque, esto es, la capacidad que tiene el ataque de generar daños, tanto a nivel personal como de la infraestructura de los Estados (Manual de Tallinn 2.0, 2017; Schmitt, 1999). No se requiere únicamente que generen inconvenientes, sino que efectivamente haya daños, destrucción, heridos o muertos, para hablar de que un ciberataque ha sido lo suficientemente severo. Sin embargo, Jens David Ohlin (2015) señala que este estándar no es suficiente para poder determinar cuándo un ciberataque ha alcanzado el nivel de un ataque armado.

Por ello, tanto el Manual de Tallinn 2.0 como Ohlin coinciden en que la mejor manera de determinar si un ciberataque ha alcanzado el nivel de un ataque armado, es la causalidad próxima. Así las cosas, "si el efecto cinético de un ataque cibernético es razonablemente previsible, entonces el efecto está suficientemente relacionado causalmente con el ataque cibernético para desencadenar un derecho tradicional de legítima defensa" (Ohlin, 2015, p. 45). Dicho de otro modo, se requiere que un ciberataque tenga efectos razonablemente previsibles, para lo cual, debe analizarse otros factores, señalados en los comentarios a la Regla 11 del Manual de Tallinn 2.0, en su conjunto:

- Inmediatez: El Manual de Tallinn 2.0 (2017) señala que los Estados tenderán a calificar como un ataque "una ciberoperación que produce efectos inmediatos como resultado del uso de la fuerza, frente a ciberacciones que toman semanas o meses para alcanzar sus efectos pretendidos" (p. 49). En otras palabras, para que un ciberataque sea considerado como ataque armado, sus

armado y no como un mero incidente fronterizo si hubiera sido llevado a cabo por fuerzas armadas regulares" (párr. 195).

consecuencias deben ser inmediatas, o producirse en un periodo de tiempo muy breve.

Por ejemplo, el ciberataque perpetrado contra Estonia[17], en el 2007, fue calificado como ataque debido a que inmediatamente afectó la capacidad de los ciudadanos de utilizar el sistema financiero (McGuinness, 2017; Traynor, 2007). Por lo tanto, corresponde que, si ocurre un ataque similar, éste tenga la misma calificación.

- Nexo causal: Según el Manual de Tallinn 2.0 (2017) es importante estudiar la cadena de causalidad, esto es, "que la causa y los efectos estén directamente relacionados" (p. 49). Es decir, para que un ciberataque sea considerado como ataque armado, debe haber causalidad directa entre el hecho y las consecuencias. En otras palabras, el hecho debe poder generar las consecuencias esperadas.

  Al respecto, el mismo Manual de Tallinn 2.0 (2017) señala que no sería posible considerar la coerción económica como un ataque, debido a que estas medidas toman meses, o incluso más, en desplegar sus efectos (p. 49).

- Grado de intromisión: Para que sea considerado como un ataque armado, según el Manual de Tallinn 2.0 (2017), el ciberataque

[17] A raíz del traslado de la estatua del Soldado de Bronce de Tallinn (monumento que se erigió para agradecer a los soldados soviéticos que ayudaron a liberar a Estonia de los nazis), se perpetraron numerosos ataques informáticos que afectaron al Parlamento, varios ministerios, partidos políticos, bancos y medios de comunicación. Aunque no fue posible atribuirlos a Rusia por falta de evidencias, el gobierno estonio señaló que el ataque era de tal magnitud que, por lo menos debió contar con la anuencia o colaboración del gobierno ruso. (Fernández, 2009)

debe “tener un alto grado de intromisión no consentida en la soberanía de otro Estado” (p. 49). Así las cosas, será más factible considerar como ataque la intromisión en un servidor militar frente a la intromisión de un servidor de una universidad (Manual de Tallinn 2.0, 2017, p. 49).

Es importante resaltar que este criterio, por sí solo, no debería ser determinante para la consideración de un ciberataque como un ataque armado, ya que podría darse el caso de que un ciberataque afecte los servidores de múltiples instituciones educativas, poniendo en riesgo la capacidad de dichas instituciones de continuar brindando clases. En este sentido, este criterio debe analizarse en conjunto con los otros aquí citados.

- Medición de efectos: El Manual de Tallinn 2.0 (2017) señala que “mientras más cuantificable e identificable sean las consecuencias, será más fácil para un Estado evaluar la situación para determinar si una ciberoperación ha alcanzado el nivel de uso de la fuerza” (p. 50). Así las cosas, para que un ciberataque sea considerado como ataque armado, deben poder cuantificarse las consecuencias de este. Por ejemplo, si puede evaluarse el número de datos corrompidos, los servidores dañados, o la cantidad de archivos confidenciales extraídos (siempre que concurran todos los requisitos aquí señalados), es más probable que un hecho sea calificado como uso de la fuerza (Manual de Tallinn 2.0, 2017, p. 50).

- Carácter militar: El Manual de Tallinn 2.0 (2017) señala que “un nexo entre la ciberoperación y las operaciones militares aumenta

> la probabilidad de caracterización como uso de la fuerza" (p. 50). Verri (2014) define a las operaciones como el "conjunto de acciones militares que, basadas en el movimiento y/o el fuego, tienen un objetivo preciso, de alcance táctico o estratégico" (p. 78). En este sentido, si el ciberataque es utilizado como parte de una operación militar, es posible que sea considerado como un ataque armado.
>
> Ahora bien, este requisito no necesariamente debe verificarse tan pronto haya ocurrido un ciberataque, ya que cabe la posibilidad de que haya sido perpetrado por actores privados, cuyas acciones luego convalida el Estado agresor. Por lo tanto, es probable que este requisito no se cumpla en un primer momento, por lo que debe verificarse la concurrencia de los requisitos anteriormente descritos.

Ahora bien, existe otro criterio para analizar la severidad de un ciberataque que no está contemplado en el Manual de Tallinn 2.0, pero que se desprende de la definición de ataque armado. Verri (2014) señala que un ataque armado es "una parte del combate que permite a una unidad (…) conquistar o destruir un objetivo militar mediante la coordinación del fuego y el desplazamiento" [énfasis agregado] (p. 11). En esta línea, es posible señalar que podría hablarse de severidad en tanto un ciberataque se dirija contra objetivos militares.

Verri (2014) define a los objetivos militares como "bienes que, por su naturaleza, ubicación, finalidad o utilización, contribuyen eficazmente a la acción militar y cuya destrucción total o parcial, captura o neutralización ofrezcan una ventaja militar indefinida" (p. 77). Por ello, un ciberataque que se dirija a afectar, por ejemplo, los servidores militares de un Estado, tiene más probabilidades de

ser considerado como uso de la fuerza (siempre que concurran los demás requisitos).

En conclusión, para que un ciberataque, en el contexto de una amenaza híbrida, merezca una respuesta aplicando las normas sobre el uso de la fuerza a nivel internacional, debe poder ser equiparada con un ataque armado convencional. Esto es, cuando cumpla con un criterio de severidad, debido a los efectos cinéticos que produce. Para ello, debe analizarse la causalidad próxima, para lo cual corresponde estudiar la inmediatez del ataque, su nexo causal, que invada la soberanía e inviolabilidad territorial de otro Estado, que tenga consecuencias cuantificables, que sea realizado como parte de una operación militar (con la salvedad antes comentada) y tenga un objetivo militar.

Sin embargo, existe un segundo requisito que debe analizarse: que el ciberataque sea atribuible a un Estado.

Cuadro No. 3: Criterios para equiparar un ciberataque a un ataque armado

Deben analizarse dos condiciones en conjunto:

- Que el ciberataque haya sido lo suficientemente severo, es decir, que haya daños, destrucción, heridos o muertos.
- Que el ciberataque cumpla con el criterio de causalidad próxima, para lo cual debe verificarse:
    - La inmediatez del ataque.
    - El nexo causal.
    - El grado de intromisión en la inviolabilidad territorial de otro Estado.
    - Que tenga consecuencias cuantificables.
    - Que sea realizado como parte de una operación militar (con la salvedad de que este requisito no necesariamente puede

verificarse al ocurrir un ciberataque). ○ Que se dirija contra un objetivo militar.

Fuente: Elaboración propia

El ciberataque, en el contexto de una amenaza híbrida, debe ser imputable a un Estado:

La segunda condición para que un ciberataque, en el contexto de una amenaza híbrida, sea considerado como un uso de la fuerza, es que sea atribuible a un Estado. Esto significa, en opinión de Sean D. Murphy (2006), que los actos sean "actos de un Estado" (p. 231) [traducción propia], sin embargo "los 'Estados' no cometen actos, sino que los actos son cometidos por los gobiernos, organizaciones y personas con diferentes niveles de conexión con un Estado" (p. 231). En este sentido, tal y como señala Elizabeth Salmón (2014a), corresponde analizar las normas establecidas en el Capítulo II de los Artículos sobre la Responsabilidad de los Estados por Hechos Internacionalmente Ilícitos (en adelante, los Artículos sobre Responsabilidad Estatal), que fueron aprobados por la Resolución No. 56/83 de la Asamblea General de la ONU (2001). Los Artículos sobre Responsabilidad Estatal prevén siete supuestos de atribución de la responsabilidad a un Estado, pero el Manual de Tallinn 2.0 recoge cuatro de ellos a efectos de atribuir un ciberataque. Adicionalmente, esta investigación considera que también resultan de aplicación dos de los otros tres supuestos que el Manual de Tallinn 2.0 no analiza.[18]

El primer supuesto fue recogido por la CIJ, en su Opinión Consultiva acerca de la Diferencia relativa a la inmunidad judicial de un Relator Especial de la Comisión de Derechos Humanos (1999), al señalar que "es una norma de

[18] Cabe precisar que el supuesto contemplado en el art. 9 de los Artículos sobre Responsabilidad Estatal, referido a la actuación de individuos en caso de ausencia del gobierno, no se ha analizado debido a que no se ha presentado ningún caso de un ciberataque realizado en ausencia del gobierno.

derecho internacional comúnmente reconocida que el acto del órgano del Estado debe considerarse como acto de ese Estado" (párr. 62). Asimismo, el art. 4 de los Artículos sobre Responsabilidad Estatal señala lo siguiente:

> 1. Se considerará hecho del Estado según el derecho internacional el comportamiento de todo órgano del Estado, ya sea que ejerza funciones legislativas, ejecutivas, judiciales o de otra índole, cualquiera que sea su posición en la organización del Estado y tanto si pertenece al gobierno central como a una división territorial del Estado.
> 2. Se entenderá que órgano incluye toda persona o entidad que tenga esa condición según el derecho interno del Estado. (Artículos sobre la Responsabilidad de los Estados por Hechos Internacionalmente Ilícitos, 2001, art. 4)

Esto significa que un hecho será atribuible a un Estado en tanto emane de cualquier órgano estatal, sea cual sea su posición, sea que se trate de una entidad individual o colectiva (Salmón, 2014a, p. 292). Respecto de las actuaciones individuales, Antonio Cassese (2005) sugiere que se debe determinar si "el individuo (…) tiene el estatus de Agente Estatal de conformidad con el sistema legal nacional de un estado particular, sea o no un agente del gobierno central (incluyendo las autoridades legislativas o judiciales) o de una unidad territorial" (p. 246).

Esto resulta particularmente importante para efectos de determinar si un ciberataque resulta imputable a un Estado, ya que, de conformidad con lo señalado por el comentario a la Regla 6 del Manual de Tallinn 2.0 (2017), "todas las acciones u omisiones de los órganos del Estado son automática y necesariamente atribuibles a dicho Estado" (p. 30) [traducción propia], y que "toda persona o entidad que tiene ese estatus de conformidad con la legislación

interna de dicho Estado, será considerada como un órgano estatal, sin importar su función o ubicación dentro de la jerarquía estatal" (pp. 30-31) [traducción propia].

Así, por ejemplo, si un ciberataque ha sido perpetrado por una agencia de inteligencia estatal, o por alguna institución militar, o en general cualquier agencia estatal, se puede afirmar que es atribuible a dicho Estado (Manual de Tallinn 2.0, 2017, p. 31). Lo mismo ocurre si un funcionario actúa en calidad de agente estatal (Manual de Tallinn 2.0, 2017, p. 31).

Existe un segundo supuesto de atribución, contemplado en el art. 5 de los Artículos sobre Responsabilidad Estatal:

> Se considerará hecho del Estado según el derecho internacional el comportamiento de una persona o entidad que no sea órgano del Estado según el artículo 4 pero esté facultada por el derecho de ese Estado para ejercer atribuciones del poder público, siempre que, en el caso de que se trate, la persona o entidad actúe en esa capacidad. (Artículos sobre la Responsabilidad de los Estados por Hechos Internacionalmente Ilícitos, 2001, art. 5)

Según Murphy (2006), este artículo significa que las conductas serán atribuibles a un Estado en tanto emanen de "personas que no son agentes estatales, pero que han sido empoderados por dicho Estado para ejercer elementos de autoridad estatal" (p. 231). Si bien la regla general es que los actos de los particulares no pueden atribuirse al Estado (Salmón, 2014a, p. 295), existe una excepción que "para atribuir a dicho Estado conductas de órganos que no son órganos Estatales en el sentido del art. 4, pero que, sin embargo, están autorizados para ejercer autoridad gubernamental" (Crawford, 2002, p. 100).

Así las cosas, “para efectos del derecho de la responsabilidad estatal, las personas o entidades que, si bien no son órganos estatales, pero que están empoderados según la ley nacional para ejercer ‘autoridad gubernamental’ se consideran como órganos estatales” (Manual de Tallinn 2.0, 2017, p. 31). Además, el Manual de Tallinn 2.0 (2017) enfatiza que “la responsabilidad estatal sólo se activa cuando la entidad en cuestión ejerce elementos de autoridad gubernamental” (p. 31).

Cabe señalar que la defensa nacional[19] ha sido tradicionalmente una función gubernamental, por lo tanto, los ciberataques, tanto ofensivos como defensivos, si son realizados por privados que cuentan con autorización gubernamental para ello, son atribuibles al Estado que brindó dicha autorización. En esta línea, se pone como ejemplo a una empresa, que cuenta con la autorización estatal, para realizar operaciones cibernéticas ofensivas, o incluso defensivas (Manual de Tallinn 2.0, 2017, p. 31). Sin embargo, existe un problema en este punto, y es la probanza de la autorización estatal para este tipo de operaciones, ya que es altamente probable que la documentación que acredita tal autorización esté clasificada, por tratarse de asuntos militares.

Existe un tercer supuesto de atribución de responsabilidad relevante a efectos de un ciberataque, recogido en el art. 8 de los Artículos sobre Responsabilidad Estatal:

> Se considerará hecho del Estado según el derecho internacional el comportamiento de una persona o de un grupo de personas si esa persona o ese grupo de personas actúa de hecho por instrucciones o

[19] La defensa nacional es el “conjunto de previsiones, decisiones y acciones que el gobierno genera y ejecuta permanentemente para lograr la seguridad nacional y alcanzar sus objetivos, incluyendo su integridad, unidad, bienestar y la facultad de actuar con autonomía en el ámbito interno, y libre de toda subordinación en el ámbito externo” (CAEN, 2014, citado en Astudillo Salcedo, 2020, p. 21).

> bajo la dirección o el control de ese Estado al observar ese comportamiento. (Artículos sobre la Responsabilidad de los Estados por Hechos Internacionalmente Ilícitos, 2001, art. 8)

La regla general de responsabilidad es que los actos de las personas no generan responsabilidad para los Estados. Sin embargo, y en ciertas circunstancias, "esto sí sucede, dado que existe una relación fáctica entre el privado que realiza la conducta y el Estado" (Salmón, 2014a, p. 295). En este sentido, se requiere que las personas actúen bajo instrucciones o dirección del Estado. Para James Crawford (2002), ello ocurre en dos posibles situaciones, "la primera involucra personas privadas que actúan bajo instrucciones del Estado para cometer la conducta ilícita. La segunda se refiere a una situación más general en la que personas privadas actúan bajo dirección o control del Estado" (p. 110) [traducción propia]. Así, por ejemplo, se podría atribuir responsabilidad a un Estado por actos realizados por una entidad privada contratada por dicho Estado para realizarlos.

Esto cobra especial importancia en el tema del uso de la fuerza, ya que la CIJ (1986), en el caso de Nicaragua contra Estados Unidos, señaló que los actos de agresión o intervenciones militares son casos de uso de la fuerza directo, pero también existen los casos de uso de la fuerza indirecto y que resultan perfectamente atribuibles a un Estado. Específicamente, se señala lo siguiente:

> Aunque no está probado que ningún personal militar de Estados Unidos formó parte directa de las operaciones, agentes de Estados Unidos participaron en la planificación, dirección, soporte y ejecución de las operaciones. La ejecución fue, más bien, el trabajo de los "UCLAs" [*unilaterally controlled latino assets*, o activos latinos controlados

unilateralmente][20], mientras que los nacionales de Estados Unidos participaron en la planificación, dirección y soporte. La imputabilidad a los Estados Unidos de estos ataques parece, por lo tanto, establecida para esta Corte. (Corte Internacional de Justicia, 1986, párr. 86)

Sin embargo, estos actos por si solos no generan responsabilidad estatal, ya que la Corte impone el estándar del control efectivo, de la siguiente manera:

> La Corte ha considerado que la participación de los Estados Unidos, aunque preponderante y decisiva, en el financiamiento, organización, entrenamiento, provisión y equipamiento de los Contras, la selección de sus objetivos militares o paramilitares, y la planificación de toda su operación, es aún insuficiente en sí misma. (…) Para que esta conducta genere responsabilidad legal a los Estados Unidos, tendría que, en principio, probarse que dicho Estado tenía control efectivo de las operaciones militares o paramilitares. (Corte Internacional de Justicia, 1986, párr. 115)

Ahora bien, es importante señalar que existe otro criterio, muy diferente al control efectivo, de interpretación del art. 8 de los Artículos sobre Responsabilidad Estatal, que fue estipulado en el fallo del caso Tadic, emitido por el Tribunal Penal Internacional para la ex Yugoslavia:

> En virtud de este artículo [art. 8 de los Artículos sobre Responsabilidad Estatal], si se prueba que los individuos que no son

[20] Según lo señalado por la Corte Internacional de Justicia (1986), UCLAs es un término usado por la CIA para referirse al personal militar de Estados Unidos u otros países latinoamericanos no identificados, que estaba pagado, o actuaba bajo instrucción directa del ejército de los Estados Unidos o su personal de inteligencia (párr. 75).

> considerados como órganos de un Estado, de conformidad con su legislación interna, actúan de hecho en nombre de ese Estado, sus actos serán atribuibles a dicho Estado. El fundamento de esta regla es evitar que los Estados eludan la responsabilidad internacional al hacer que particulares realicen tareas que no pueden o no deben ser realizadas por funcionarios del Estado, o al afirmar que los individuos que realmente participan en la autoridad gubernamental no están clasificados como órganos del Estado en virtud de la legislación nacional, y por lo tanto no comprometen la responsabilidad del Estado. En otras palabras, los Estados no pueden, por un lado, actuar de facto a través de individuos y, por el otro, desvincularse de tal conducta cuando estos individuos violan el derecho internacional. El requisito del derecho internacional para la atribución a los Estados de actos realizados por particulares es que el Estado ejerza control sobre los particulares. Sin embargo, el grado de control puede variar según las circunstancias de hecho de cada caso. La Sala de Apelaciones no ve por qué en todas y cada una de las circunstancias el derecho internacional debería exigir un umbral alto para la prueba de control. Más bien, se pueden distinguir varias situaciones. (Tribunal Penal Internacional para la ex Yugoslavia, 1999, párr. 117)

En este sentido, se observa que el Tribunal Penal Internacional para la ex Yugoslavia se inclina más por la figura del control general, “que vaya más allá del mero financiamiento y equipamiento de dichas fuerzas e involucre también participación en el planeamiento y supervisión de operaciones militares” (Tribunal Penal Internacional para la ex-Yugoslavia, 1999, párr. 145), pero que no requiere de la emisión de instrucciones específicas. En la misma línea se pronuncia Crawford (2013), quien señala que no se requiere de instrucciones precisas, sino más bien basta con instrucciones generales que permitan la

elección de medios para su cumplimiento (Crawford, 2013, p. 145).

El Manual de Tallinn 2.0 (2017) acoge la teoría del control efectivo, al señalar "que el Estado necesita haber emitido instrucciones específicas, dirigido o controlado una operación particular para incurrir en responsabilidad estatal" (p. 33). Ello debido a que, tal y como señala la CIJ (2007) en el Caso Relativo a la aplicación de la Convención para la Prevención y la Sanción del Delito de Genocidio, el criterio del control general del caso Tadic no resulta realmente aplicable para determinar la responsabilidad estatal por hechos ilícitos internacionales, sino para determinar la existencia de un conflicto armado internacional (párr. 403-405).

Sin embargo, en esta tesis no se busca determinar responsabilidad estatal *per se*, sino, tal y como se señaló anteriormente, determinar si existió amenaza o uso de la fuerza. Por lo tanto, se considera que, para este efecto, es preferible acogerse al criterio del control general expuesto en el caso Tadic.

Asimismo, existe un último caso de responsabilidad atribuible al Estado, que fue primero reconocido por la CIJ en el caso de Estados Unidos contra Irán, relativo al personal diplomático y consular de Estados Unidos en Teherán (Estados Unidos contra Irán, 1980):

> La aprobación dada a estos hechos[21] por el Ayatola Jomeini y otros órganos del Estado Iraní, y la decisión de perpetuarlos, convierte a la ocupación continua de la Embajada y la detención de los rehenes en actos de dicho Estado. Los militantes, autores de la invasión y carceleros

[21] El caso relativo al personal diplomático y consular de Estados Unidos en Teherán se refiere a la toma de la Embajada de Estados Unidos en la capital iraní. "El 4 de noviembre de 1979, estudiantes musulmanes seguidores de la política del Imán realizaron ataques armados contra la Embajada de Estados Unidos y sus Consulados (…) en Teherán. Como consecuencia de dicho ataque, la embajada y los consulados fueron ocupados y el personal diplomático y consular fue secuestrado. (…) Pese a que el gobierno de Irán conocía del ataque, no tomó medidas al respecto. Incluso, luego de realizado el ataque, numerosas autoridades del Estado expresaron su aprobación a lo sucedido." (Salmón, 2014a, p. 299)

> de los rehenes, ahora se han convertido en agentes del Estado Iraní, por cuyos actos el Estado en sí mismo es internacionalmente responsable. (Corte Internacional de Justicia, 1980, para. 74) [Traducción propia]

Esto se refiere a los casos en que los individuos actúan por cuenta propia, pero luego los Estados convalidan ese comportamiento. El art. 11 del Proyecto de Responsabilidad Estatal señala lo siguiente:

> El comportamiento que no sea atribuible al Estado en virtud de los artículos precedentes se considerará, no obstante, hecho de ese Estado según el derecho internacional en el caso y en la medida en que el Estado reconozca y adopte ese comportamiento como propio. (Comité de Derecho Internacional, 2001, art. 11)

En línea con lo señalado por el Manual de Tallinn 2.0 (2017), esto también es relevante respecto de las operaciones cibernéticas, ya que una conducta "será considerada como un acto de un Estado, bajo el derecho internacional, hasta el punto en que dicho Estado reconozca y adopte la conducta en cuestión como suya" (p. 34). Este sería el caso de un ciberataque realizado por un grupo terrorista, al que un Estado ha brindado su apoyo posterior, y ha manifestado que brindará protección (Manual de Tallinn 2.0, 2017, p. 34).

Por otro lado, si bien el Manual de Tallinn 2.0 no se pronuncia al respecto, es posible afirmar que existen dos supuestos adicionales que resultan de relevancia respecto de la atribución de un ciberataque a un Estado. Así, es posible aplicar el art. 6 de los Artículos sobre Responsabilidad Estatal, que señala lo siguiente:

> Se considerará hecho del Estado según el derecho internacional el comportamiento de un órgano puesto a su disposición por otro Estado, siempre que ese órgano actúe en el ejercicio de atribuciones del poder público del Estado a cuya disposición se encuentra.

La práctica ha demostrado que es posible que un Estado brinde apoyo a otro para realizar ciberataques, a través de poner a disposición personal militar u otros involucrados en la realización de dichos ataques. Esto ha ocurrido en el contexto de la guerra en Yemen, ya que Irán ha puesto a disposición de los rebeldes Houthis a operativos especializados en la realización de ciberataques (Boylan, 2018) [página web].

Adicionalmente, también es posible atribuir responsabilidad a un Estado a partir del art. 10 de los Artículos sobre Responsabilidad Estatal de la siguiente manera:

> Se considerará hecho del Estado según el derecho internacional el comportamiento de un movimiento insurreccional que se convierta en el nuevo gobierno del Estado.

A partir de este artículo, es posible atribuir responsabilidad a un Estado en tanto un movimiento insurreccional haya asumido el gobierno, ya que se entendería que hay una continuidad entre el movimiento y el gobierno (Crawford, 2002, p. 117).

Nuevamente, tal y como se aprecia del caso de la guerra en Yemen, la facción rebelde Houthi formó un gobierno ante la ausencia del presidente Hadi, que ha autorizado la realización de ciberataques, por lo cual estos resultan atribuibles directamente a Yemen (Boylan, 2018) [página web].

Así las cosas, un ciberataque, en el contexto de una amenaza híbrida,

ameritará una respuesta en el marco de las normas pertinentes del ordenamiento jurídico internacional en tanto pueda ser atribuible a un Estado, ya sea porque es perpetrado por un órgano estatal, o por personas que actúan por cuenta o en representación de dicho Estado. También será atribuible el ciberataque perpetrado por particulares, en tanto éstos estén bajo el control efectivo del Estado, o que sus acciones hayan sido convalidadas por el Estado.

En tanto un ciberataque cumpla con las características señaladas en el párrafo anterior, corresponderá pasar a un segundo nivel de análisis, esto es, si corresponde aplicar el *ius ad bellum* o el *ius in bello*.

Cuadro No. 4: Criterios para atribuir un ciberataque a un Estado

Para atribuir un ciberataque a un Estado deben cumplirse cualquiera de los siguientes supuestos:

- Que sea perpetrado por un órgano o agentes estatales.
- Que sea perpetrado por un privado que cuenta con autorización del Estado para ejercer funciones gubernamentales, otorgada conforme a la ley doméstica.
- Que sea perpetrado por un privado que lo realiza por instrucción de un Estado, o cuyos actos se encuentran bajo dirección y control general de dicho Estado.
- Que sea perpetrado por un privado, cuyos actos sean reconocidos posteriormente y adoptados como propios por un Estado.
- Que sea perpetrado por órganos que un Estado puso a disposición de otro.
- Que sea perpetrado por movimientos insurreccionales que luego se convierten en el gobierno oficial de un Estado.

Fuente: Elaboración propia

Es importante señalar que, si bien los criterios han sido definidos a nivel teórico, en la práctica existe una dificultad para demostrarlos. El caso más claro son los ciberataques perpetrados recientemente contra el Perú, en concreto el caso que se mencionó respecto a la sustracción de correos electrónicos de las Fuerzas Armadas, ya que, si bien se conoce que son de autoría del grupo Guacamaya (Paez & Ampuero, 2021), no es posible determinar si se pueden atribuir finalmente a un Estado. Por lo tanto, corresponde realizar un análisis caso por caso.

MARCO NORMATIVO:

Marco normativo del derecho internacional aplicable a los ciberataques, en el contexto de una amenaza híbrida:

Una vez que se ha determinado que un ciberataque es equiparable a un ataque armado y resulta atribuible a un Estado determinado, queda por determinar cuál es el marco normativo aplicable. Ello dependerá de la situación en que se haya suscitado el ciberataque, esto es si fue un uso de la fuerza en tiempos de paz o en tiempos de guerra o conflicto armado.

Así las cosas, corresponde analizar los casos de *ius ad bellum* y *ius in bello*. Conforme lo señala el Comité Internacional de la Cruz Roja (2010), mientras el *ius ad bellum* “procura limitar el recurso a la fuerza entre Estados” [página web], el *ius in bello*, o derecho en la guerra, busca “limitar el sufrimiento causado por la guerra, mediante la protección y la asistencia a las víctimas en la mayor medida posible” [página web]. Tal y como se puede apreciar de la definición, se trata de dos marcos jurídicos intrínsecamente vinculados, ya que el recurso a la fuerza entre Estados, si bien ocurre en tiempos de paz, puede llevar a una situación de conflicto armado.

Por tanto, se analizará en esta sección cada uno de estos marcos

jurídicos por separado, brindando una aproximación histórica, una breve definición, y posteriormente se estudiará qué normas de estos marcos jurídicos se aplican para responder a un ciberataque en el contexto de una amenaza híbrida.

Sin embargo, antes de abordar esta cuestión, es importante hacer una distinción entre los conceptos de ciberseguridad y ciberdefensa, ya que sólo en este último caso ocurre la aplicación tanto del *ius ad bellum* como del *ius in bello*. Por un lado, la ciberseguridad se refiere a la práctica de proteger sistemas críticos e información sensible de ataques cibernéticos, a través de acciones defensivas para combatir amenazas contra los sistemas interconectados y softwares. Por ejemplo, la instalación de firewalls[22] y antivirus[23]. Por otro lado, la ciberdefensa se refiere a la capacidad de un Estado para prevenir y contrarrestar las amenazas o ciberataques que afecten sus capacidades, activos críticos e intereses, a través de acciones defensivas u ofensivas, para asegurar el propio uso del ciberespacio. Por ejemplo, realizar un ciberataque para responder a otro.

De la definición de ambos conceptos, se aprecian ciertas similitudes. Así, ambos pretenden controlar y neutralizar ciberataques. Sin embargo, la ciberdefensa no sólo tiene carácter preventivo y defensivo, sino que permite la realización de acciones ofensivas a fin de salvaguardar la infraestructura crítica. Esta tesis, entonces, se referirá exclusivamente a temas de ciberdefensa, en tanto se analizan casos de ciberataques que sean equiparables a ataques armados cinéticos e imputables a Estados.

[22] Un firewall es “un sistema diseñado para proteger las redes privadas del acceso no autorizado y no verificado en una conexión a Internet. (…) Ayudan a detener a los posibles atacantes antes de que puedan causar algún daño” (HP, 2021) [página web] (ver también What Is a Firewall? - Cisco, s.f.).
[23] Un antivirus es “un tipo de software que se utiliza para evitar, buscar, detectar y eliminar virus de una computadora” (Verizon, s.f.) [página web].

Ius Ad Bellum:

Melzer (2011) define al *ius ad bellum* como "el cuerpo normativo que gobierna el recurso de los Estados a la fuerza en sus relaciones internacionales" (p. 6), y cuya principal fuente está en la Carta ONU (p. 6). Para entender esta definición, sin embargo, es importante estudiar el origen histórico de esta área del derecho internacional.

Este origen está fuertemente anclado en el desarrollo de teóricos como Santo Tomás de Aquino y Hugo Grocio, quienes desarrollaron las ideas de la guerra justa (Balouziyeh & Burns, 2013; Lesaffer, 2015). Santo Tomás de Aquino señalaba tres condiciones para que una guerra sea librada por causas justas: *auctoritas* (que la guerra sea declarada por un soberano), *causa justa* y *recta intentio* (Lesaffer, p. 37). Si bien estos dos últimos no fueron desarrollados por Aquino, "en su texto *De jure belli ac pacis* (1625), el humanista holandés Hugo Grocio (1583-1645) discernía tres causas justas: defensa, reivindicación de propiedad o derechos, y la imposición de castigos" (Lesaffer, p. 37; ver Salmón, 2016). Respecto de la *recta intentio*, esta "implicaba que la guerra debía librarse con la intención de hacer justicia y, en última instancia, de lograr una paz justa" (Lesaffer, p. 37). A partir de esta regulación, se comenzó a desarrollar un cuerpo normativo separado, para limitar los efectos de las hostilidades, dando inicio al *ius in bello*. Esto se explicará más adelante.

Esta concepción de la guerra por causas justas inspiró la práctica estatal de justificar el recurrir a la fuerza armada. Tal y como señala Lesaffer (2015), "los príncipes y las repúblicas de la Europa moderna temprana se tomaron muchas molestias para justificar su decisión de recurrir a la guerra [a través de] textos sustanciales en los que se explicaban en detalle las razones de la guerra" (p. 43). Sin embargo, esto también originó la guerra defensiva, esto es, aquellas que "se libraban como reacción a una amenaza o ataque armado previo del enemigo" (Lesaffer, 2015, p. 45; ver también Namihas, 2003). Así, en opinión de Lesaffer

(2015), “a fines del siglo XIX y principios del XX, este enfoque en la guerra defensiva encontró su correlación en un rechazo cada vez más generalizado de la agresión por parte de la comunidad internacional” (p. 46).

Las Conferencias de Paz de La Haya de 1899 y 1907 buscaron limitar el recurso al uso de la fuerza, y, aunque esto no fue del todo posible, sí se logró introducir una cláusula que señaló que “con miras a obviar, en lo posible, el recurso a la fuerza en las relaciones entre los Estados, las Potencias Signatarias convienen en emplear sus mejores esfuerzos para asegurar el arreglo pacífico de las diferencias internacionales” (Convención (I) para la solución pacífica de disputas internacionales, 1899, art. 1) [traducción propia].

Fue recién con la firma del Pacto Briand-Kellogg, oficialmente llamado Tratado General para la Renuncia a la Guerra, que los Estados partes, entre ellos el Perú[24], convienen en renunciar al recurso de la guerra, esto es, prohibir el uso de la fuerza (Lesaffer, 2015, pp. 51–52; ver también Namihas, 2003; Salmón, 2016). Así, quedó abolido el concepto de la guerra justa. Incluso, el Pacto de la Liga de Naciones, que creaba la Sociedad de Naciones, establecía sanciones a las que los Estados partes del Pacto Briand-Kellogg podían recurrir en caso de guerra (Lesaffer, p. 53).

La prohibición definitiva del uso de la fuerza quedó consagrada en el artículo 2 párrafo 4 de la Carta de las Naciones Unidas (1945):

> Los Miembros de la Organización, en sus relaciones internacionales, se abstendrán de recurrir a la amenaza o al uso de la fuerza contra la integridad territorial o la independencia política de cualquier Estado, o en cualquier otra forma incompatible con los

[24] De acuerdo con el Archivo Nacional de Tratados, el Perú se adhirió a este tratado el 27 de agosto de 1928. Asimismo, lo ratificó mediante Resolución Legislativa 6628, aprobada el 3 de julio de 1929, que fue depositada el 24 del mismo mes.

Propósitos de las Naciones Unidas. (art. 2.4)

Es así como queda prohibido tanto emplear la fuerza (entendida, en los términos explicados anteriormente, como un ataque armado) como amenazar con el uso de esta, salvo aquellas excepciones expresamente contempladas por la Carta de Naciones Unidas: la autorización del Consejo de Seguridad (por aplicación del Capítulo VII de la Carta), y el derecho a la legítima defensa (art. 51 de la Carta). Cabe resaltar que el artículo 2.4 ha sido calificado por la CIJ, en el caso de Nicaragua contra Estados Unidos (1986), como una piedra angular de la Carta ONU y le ha dado carácter de norma consuetudinaria e imperativa en el derecho internacional (párr. 187-190).

Aquí es importante señalar que la misma Corte, en el caso de Nicaragua contra los Estados Unidos (1986), equiparó el uso de la fuerza prohibido con la definición de agresión estipulada en la Resolución No. 3314 (1974) de la Asamblea General de la ONU (párr. 195). Y recientemente, la Comisión de Derecho Internacional, a través del Documento No. A/CN.4/L.967 (2022), que aprueba el texto del proyecto de conclusiones y de anexo acerca de las normas imperativas de derecho internacional general (ius cogens), considera, en su anexo, que la prohibición de agresión tiene dicha calidad.

A partir de este recuento histórico es posible definir al *ius ad bellum* como el área del derecho internacional que prohíbe el uso de la fuerza, y señala las excepciones en las que se admitirá ésta. Al respecto, Salmón (2016), señala lo siguiente:

> Será el Derecho internacional general el que contiene tales previsiones, y la prohibirá de manera general (…) o la permitirá de manera excepcional, en situaciones de legítima defensa frente a un ataque armado (…) o cuando el propio Consejo de Seguridad decida su

> uso frente a una amenaza a la paz, quebrantamiento de la paz o acto de agresión. (p. 28)

Dicho esto, corresponde analizar qué normas del *ius ad bellum* aplican respecto de un ciberataque, en el contexto de una amenaza híbrida.

Ius ad Bellum y Ciberataques en el contexto de una amenaza híbrida:

Tal y como se señaló en párrafos anteriores, para activar la aplicación de *ius ad bellum* (emplear la fuerza en legítima defensa o con la autorización del Consejo de Seguridad) en el contexto de una amenaza híbrida, se requiere que exista un ciberataque, que sea equiparable a un ataque armado y que sea atribuible a un Estado. Es decir, sería en casos de conflictos híbridos, más no de guerras híbridas, cuando uno de los métodos no convencionales sea el uso de ciberataques. Dicho ciberataque equiparable a un ataque armado puede o no dar inicio a una guerra híbrida. Si iniciase una, consideramos que se aplicarían ambos regímenes en simultáneo.

Tal y como se señaló líneas arriba, un conflicto híbrido es aquel tipo de amenaza híbrida en el que se combinan métodos tradicionales y no tradicionales para la amenaza o uso de la fuerza. Por ello, Galán (2018) pone como ejemplos de métodos no convencionales en el contexto de los conflictos híbridos a los ataques terroristas, acciones delictivas de grupos armados, disputas marítimas, actos económicos hostiles, operaciones militares encubiertas y, además, ciberataques.

Así las cosas, un ciberataque, como método no convencional parte de un conflicto híbrido, que se equipare a un ataque armado y que sea atribuible a un Estado, se considerará como un uso de la fuerza prohibido por el art. 2 párrafo 4 de la Carta ONU. Si ello ocurre, en opinión de Gray (2018), se justifica, como respuesta, la aplicación del art. 51 de la Carta ONU, esto es, el derecho a la

legítima defensa (p. 35; ver también Melzer, 2011). Este artículo señala lo siguiente:

> Ninguna disposición de esta Carta menoscabará el *derecho inmanente de legítima defensa*, individual o colectiva, *en caso de ataque armado* contra un Miembro de las Naciones Unidas, hasta tanto que el Consejo de Seguridad haya tomado las medidas necesarias para mantener la paz y la seguridad internacionales. (Carta de Las Naciones Unidas, 1945, art. 51) [Énfasis agregado]

Gray (2018) señala que, de la lectura de este artículo, se desprende que el uso de la fuerza por parte de un Estado faculta a otro Estado a ejercer todas las acciones que considere necesarias como parte de su derecho a la legítima defensa (p. 120-121). En la misma línea, Verri (2014) señala que "de conformidad con la Carta de las Naciones Unidas, todo miembro de la Organización que sea víctima de una agresión puede ejercer su derecho a la legítima defensa de la manera que considere necesaria" (p. 59), que, como se verá más adelante, debe cumplir ciertas condiciones.

Entonces, surge una primera interrogante: ¿es posible invocar el derecho a la legítima defensa ante un ciberataque, en el contexto de un conflicto híbrido? La CIJ (1996), en su Opinión Consultiva sobre el Uso de Armas Nucleares, señala que las provisiones referidas a prohibición del uso de la fuerza "no se refieren a armas específicas. Aplican a cualquier uso de la fuerza, sin importar el armamento utilizado" (párr. 39). Así las cosas, si un Estado es víctima de un ciberataque, en el contexto de un conflicto híbrido, y este ciberataque es equiparable a un ataque armado y atribuible a otro Estado, el primero queda expedito para ejercer su derecho a la legítima defensa a través de todos los medios que considere adecuados en el marco de las limitaciones que serán

desarrolladas más adelante.

La complicación que Gray (2018) encuentra es que existe una controversia respecto del alcance del derecho a la legítima defensa, esto es, cuando se usa la fuerza para responder a un ataque armado (p. 120). Esta discusión no ha sido resuelta por los tratados, sin embargo, Melzer (2011) apunta la siguiente opinión:

> [La legítima defensa] permite al Estado que se defiende tomar las medidas necesarias para repeler un ataque armado, aunque esto pueda requerir acciones que, de otro modo, estarían prohibidas por el derecho internacional, notablemente el uso de fuerza interestatal. La justificación de este permiso reside en la ilicitud inicial de la conducta del Estado infractor y la necesidad de evitar el daño que probablemente resulte de esa conducta ilícita. (p. 17) [Traducción propia]

Es decir, es posible que un ataque armado, incluido un ciberataque, sea respondido a través de otro ataque armado. Sin embargo, esta respuesta mediante el uso de la fuerza debe cumplir ciertas características que fueron formuladas, a raíz del Incidente *Caroline*[25], por el secretario de Estado de los Estados Unidos, Daniel Webster:

> En estas circunstancias, y en las que están inmediatamente

[25] El incidente *Caroline* se refiere a la crisis diplomática que se originó a raíz de la destrucción del barco 'Caroline'. Luego de la guerra de 1812, hubo una revuelta en Upper Canada, que era una colonia británica. En 1837, un grupo de rebeldes canadienses se refugió en una isla del río Niagara, usando la nave estadounidense Caroline. Luego de un intercambio de disparos, las fuerzas británicas capturaron el Caroline, le prendieron fuego y lo arrojaron por las cataratas del Niágara. Esto originó un intercambio de notas diplomáticas de protesta entre el secretario de Estado de Estados Unidos, Daniel Webster, y Lord Ashburton, ministro especial del Reino Unido encargado de negociar un acuerdo. (Wood, 2018, p. 6) Dicho intercambio "condujo a la formulación de una serie de condiciones y modalidades que debían cumplirse para justificar la violación británica de la soberanía territorial de los Estados Unidos" (Melzer, 2011, p. 17).

> relacionadas con la transacción misma, corresponderá al Gobierno de Su Majestad demostrar, sobre qué estado de los hechos y qué normas de la ley nacional, se defenderá la destrucción del 'Caroline'. Corresponderá a ese Gobierno mostrar la *necesidad* de la legítima defensa, *instantánea*, *abrumadora*, *sin dejar elección de medios*, *ni momento para la deliberación*. (Webster, 1841; citado en Wood, 2018, p. 8) [Traducción propia] [énfasis agregado]

En opinión de Melzer (2011), la fórmula que planteó Webster ha derivado en dos principios fundamentales, de necesaria consideración respecto del ejercicio de la legítima defensa: los principios de necesidad y proporcionalidad (p. 17)[26]. Al respecto, señala lo siguiente:

> Mientras que el principio de necesidad define los márgenes de legítima defensa en términos de lo que es objetivamente necesario para evitar o repeler un ataque armado, el principio de proporcionalidad determina en qué medida el daño a prevenir justifica el daño causado por la acción defensiva. (Melzer, 2011, p. 17) [Traducción propia]

La Regla 14 del Manual de Tallinn 2.0 confirma que esta idea también se aplica para efectos del ciberespacio:

> El uso de la fuerza que involucre ciberoperaciones llevadas a cabo por un Estado, en ejercicio de su derecho a la legítima defensa, debe ser necesaria y proporcional. (Manual de Tallinn 2.0, 2017, art. 14)

[26] En el caso Nicaragua vs. Estados Unidos (1986), la Corte Internacional de Justicia también señala que, para que la legítima defensa sea válida, deben cumplirse los criterios de necesidad y proporcionalidad (párr. 194-195).

[Traducción propia]

El principio de necesidad, entonces, se refiere a que la acción, sea militar o no, responda a un ataque armado previo. Así las cosas, la formulación de Webster requiere que sea instantánea y sin dejar momento para la deliberación, lo que se refiere a que "no puede llevarse a cabo legalmente antes de que sea realmente necesaria para repeler un ataque armado, ni cuando ya no sea necesario para ese fin" (Melzer, 2011, p. 17) [traducción propia]. Por ejemplo, no sería admisible una legítima defensa cuando no exista ni un ataque inminente o que ya se está produciendo. Pero, además, "el tipo y grado de fuerza utilizada en defensa propia no exceda de lo que es realmente necesario para repeler el ataque armado en cuestión" (Melzer, 2011, p. 17; Schmitt, 1999) [traducción propia]. Por ejemplo, no sería admisible responder con una bomba nuclear a un ataque lanzado con misiles convencionales.

El Manual de Tallinn 2.0 (2017) señala, en este respecto, que la "necesidad requiere que el uso de la fuerza (…) sea exitoso en repeler un ataque armado inminente o en vencer uno que está en curso" (p. 62) [traducción propia]. En este sentido, se requiere que las acciones de ciberdefensa pasiva, por ejemplo, los firewalls, sean insuficientes para repeler el ataque armado, por lo que resultaría necesario recurrir a la fuerza para resistirlo (Manual de Tallinn 2.0, 2017, p. 62). Sólo así se podría utilizar un ciberataque, o cualquier otro medio, en ejercicio de la legítima defensa.

Respecto del principio de proporcionalidad, "la acción tomada en defensa propia estará legalmente justificada solo en la medida en que el daño que se espera que cause permanezca en una proporción razonable con el daño que pretende prevenir" (Melzer, 2011, p. 18; ver también Schmitt, 2016) [traducción propia]. Si bien esto es muy similar a la necesidad, la proporcionalidad se refiere más bien a los efectos del ataque. Por ejemplo, una acción en legítima defensa

debe causar daños en proporción razonable a los ocasionados por el ataque inicial.

En opinión del Manual de Tallinn 2.0 (2017), la proporcionalidad se refiere a cuánta fuerza es permitida una vez que se ha juzgado necesario utilizarla en ejercicio del derecho a la legítima defensa (p. 62). “Este criterio limita la escala, enfoque, duración e intensidad de la respuesta defensiva a aquella requerida para terminar la situación que originó el derecho a actuar en legítima defensa” (Manual de Tallinn 2.0, 2017, p. 62) [traducción propia]. Así las cosas, es permitido usar un ciberataque como legítima defensa, en tanto se ajuste a un criterio de proporcionalidad. Adicionalmente, si el Estado afectado no contara con las capacidades tecnológicas para responder a través de un ciberataque, sería también posible utilizar un ataque armado convencional como legítima defensa.

Sin embargo, el Manual de Tallinn 2.0 (2017), en su Regla 15, señala que “el derecho a usar la fuerza en legítima defensa surge cuando un ciberataque ocurre o es inminente. Está sujeto, además, a un requisito de inmediatez” (art. 15). La inminencia se refiere a que se permitirá el uso de la fuerza como respuesta ante ataques que estén ocurriendo, o, como en el caso de los conflictos híbridos, cuando el ciberataque sea el primer paso para luego aplicar otras medidas, así como ante la amenaza real y confirmada de la ocurrencia de un ataque armado (Manual de Tallinn 2.0, 2017, p. 63).[27] Asimismo, la inmediatez permite distinguir un acto en legítima defensa de una retaliación, ya que “se refiere al periodo siguiente a la ejecución de un ataque armado, dentro

[27] Es importante señalar que hay dos posiciones encontradas con respecto a la interpretación de la inminencia, como requisito para facultar el uso de la legítima defensa ante un ataque armado: una interpretación restrictiva (se permitirá la legítima defensa sólo ante la ocurrencia de un ataque armado) y una interpretación expansiva (se permitirá la legítima defensa también ante un ataque inminente). El Manual de Tallinn 2.0 ha recogido esta última interpretación. Ahora bien, el Perú aún no ha expresado una posición definida, sin embargo, de la revisión del sentido de sus declaraciones ante la ONU, especialmente en el caso de la invasión a Irak (ver LMT en Español, 2003), es posible deducir que optaría por la interpretación restrictiva.

del cual un Estado puede responder en legítima defensa" (Manual de Tallinn 2.0, 2017, p. 66). En este sentido, deben analizarse tres factores: la proximidad temporal entre el ataque y la respuesta, el tiempo necesario para identificar al atacante, y el tiempo necesario para preparar la respuesta (Manual de Tallinn 2.0, p. 66).

En resumen, cabe la posibilidad de ejercitar el derecho a la legítima defensa ante un ciberataque, en el contexto de una amenaza híbrida, ya sea por medios cinéticos o también a través de otro ciberataque. Para ello, deben cumplirse con los criterios de necesidad, proporcionalidad, inminencia e inmediatez.

Cuadro No. 5: Respuesta a un ciberataque en el contexto de una amenaza híbrida aplicando las normas de *ius ad bellum*

<table>
<tr><td colspan="2">Para que un ciberataque en el contexto de una amenaza híbrida pueda ser respondido aplicando las normas del ius ad bellum deben cumplir las siguientes condiciones:
Sea equiparable a un ataque armado.
Sea atribuible a un Estado.
Ocurra en tiempos de paz (tomando en consideración que también podría dar inicio a una guerra híbrida).
Entonces, en principio, el Estado afectado podrá aplicar cualquiera de las 2 alternativas (que no son excluyentes) presentadas a continuación:</td></tr>
<tr><td>Prohibición del uso de la fuerza</td><td>El ciberataque será considerado como un uso de la fuerza prohibido, en virtud del art. 2.4 de la Carta ONU. Por lo tanto, se podrían aplicar las disposiciones del Capítulo VII de la Carta ONU, referidas a las funciones del Consejo de Seguridad con respecto al uso de la fuerza y las medidas</td></tr>
</table>

	que éste determina, incluyendo la autorización del uso de la fuerza.
Legítima Defensa	El Estado afectado podrá ejercer su derecho a la legítima defensa, ya sea a través de un ciberataque o cualquier otro medio, en tanto este sea: • Proporcional • Necesario • Inmediato

Fuente: Elaboración propia

Ius In Bello:

Tal como ha reconocido el Comité Internacional de la Cruz Roja (2010) al *ius in bello* se le conoce también como derecho internacional humanitario (DIH). Sin embargo, al igual que sucede con otras ramas del derecho, no existen fuentes principales que lo definan directamente. Por ello, se debe recurrir a las fuentes auxiliares. Así, Verri (2014) define al DIH como el "conjunto de normas del derecho internacional de origen convencional o consuetudinario, específicamente destinadas a *regular problemas acaecidos en período de conflictos armados internacionales o no internacionales*" (p. 33) [énfasis agregado].

Jean Pictet (citado en Salmón, 2014b) plantea una definición similar en los siguientes términos:

> Se trata de un conjunto de normas, de origen convencional o consuetudinario, cuya finalidad específica es solucionar los problemas de índole humanitaria directamente derivados de los conflictos armados y que, por razones humanitarias, restringe la utilización de ciertos métodos o medios de combate. (p. 27)

En este sentido, de la revisión de ambas definiciones, es posible encontrar puntos en común que nos permiten entender de un modo más comprensivo el ámbito de aplicación del DIH. En primer lugar, se trata de un conjunto de normas que provienen de fuentes convencionales, es decir tratados, así como de fuentes consuetudinarias. En segundo lugar, estas normas buscan brindar soluciones a los problemas humanitarios surgidos en los conflictos armados. En tercer lugar, establecen límites al uso de ciertos medios o métodos para librar la guerra.

Sin embargo, a pesar de tener ciertos puntos en común, las definiciones aquí provistas tienen un enfoque limitado. Ello se explica pues el DIH ha tenido un desarrollo histórico que conviene mencionar brevemente.

La regulación de las normas que deben regir respecto de la guerra, o el conflicto armado, tienen antecedentes muy antiguos, enraizados en la necesidad del ser humano de moderar las hostilidades (Namihas, 2003, p. 31). Estos antecedentes están basados, tal y como se explicó en la sección anterior, en el *ius ad bellum*. Cabe recordar, entonces, que, entre 1265 y 1274, en su tratado Suma Teológica, Santo Tomás de Aquino propuso la idea de un *iustus bellum*, es decir, una guerra por causas justas, tales como defender al Estado o incluso restaurar la paz (Salmón, 2014b, p. 63). En 1625, Hugo Grocio desarrolló la idea de la guerra por causas justas (tal y como se explicó anteriormente), y a partir de ello comenzó a establecer ciertas reglas que, a su criterio, se habían vuelto uniformes para todos los reinos que libraban la guerra: la necesidad de declarar la guerra, la inmunidad de los soldados y el rey ante la comisión de asesinatos, la protección del estatuto de neutralidad para aquellos reinos que no participaban en las hostilidades, la protección de la población civil, entre otros (Hathaway & Shapiro, 2017, pp. 75–77).

La codificación de las normas consuetudinarias vinculadas a la guerra se

dio recién durante las Conferencias de Paz de La Haya, llevadas a cabo en 1899 y 1907. Estas conferencias fueron convocadas por el Zar Nicolás II, con la finalidad de tratar de encontrar un mecanismo para que la paz perdure y establecer los métodos y medios permitidos para librar la guerra (Namihas, 2003, pp. 66–72; Salmón, 2014b, p. 64). Posteriormente, los Convenios de Ginebra de 1949, y sus Protocolos Adicionales de 1977 y 2005, consagraron niveles de protección adicionales respecto de las partes en conflicto, estableciendo reglas específicas para enfermos y heridos (Convenios I y II), prisioneros de guerra (Convenio III) y personas civiles (Convenio IV) (Namihas, 2003, pp. 82–84; Salmón, 2014b, pp. 66–67). En la misma línea, en el 2005, el Comité Internacional de la Cruz Roja (CICR) publicó una lista de normas consuetudinarias del DIH, a partir de un estudio sobre la materia (Namihas, 2003, pp. 86–87; Salmón, 2014b, p. 67).

De este muy breve recuento histórico se desprende que el DIH se ha regido siempre por normas convencionales, los tratados de paz de La Haya o los Convenios de Ginebra, o por normas consuetudinarias, ya sea la compilación de Grocio o la lista de normas del CICR. Sin embargo, tal y como señala Salmón (2016), estas normas reposan sobre principios del DIH que “pretenden guiar [la interpretación de las otras normas del DIH] dándole el sentido más acorde con el mayor objetivo del DIH, que no es otro que el de proteger a las víctimas de los conflictos” (pp. 57-58).

Asimismo, vemos que la definición del DIH no provee una explicación de qué debe entenderse por problemas humanitarios. Pero este recuento histórico nos da una idea de que las normas del DIH han estado dirigidas a limitar los efectos de la guerra sobre aquellos que no participan de las hostilidades, tanto la población civil como otros Estados declarados neutrales. Ello se materializa en el principio de humanidad, que “consiste en respetar y tratar a todas las personas con humanidad, tanto a los combatientes –a quienes no se les hará padecer

sufrimientos innecesarios–, como a los no combatientes –quienes en todo momento deberán ser tratados con humanidad" (Salmón, 2016, pp. 59–60). Por ello, sería más pertinente referirse al DIH como un conjunto de normas que tienen como base el principio de humanidad[28].

Por estas consideraciones, nosotros proponemos definir al DIH como un conjunto de normas convencionales y consuetudinarias, así como principios generales, que tienen como base el principio de humanidad, y que recurren, para tal fin, a regular y limitar ciertos métodos y medios para llevar a cabo las hostilidades.

Ius in Bello y Ciberataques en el contexto de una amenaza híbrida:

Es importante recordar el concepto de guerra híbrida a efectos de abordar la normativa correspondiente al *ius in bello*. Al respecto, Frank G. Hoffman (2007) señala lo siguiente:

> Las guerras híbridas incorporan un rango de diferentes modos de guerra, incluyendo capacidades convencionales, tácticas y formaciones irregulares, actos terroristas que incluyen violencia y coerción indiscriminada, y desorden criminal. Estas actividades multimodales pueden ser llevadas a cabo por unidades separadas, o incluso por la misma unidad, pero, generalmente, son dirigidas operacional y tácticamente, y coordinadas, dentro del campo de batalla principal, para alcanzar efectos sinérgicos. (Hoffman, p. 29) [Traducción propia]

En ese sentido y en línea con lo desarrollado anteriormente en este estudio, por guerra híbrida debe entenderse, entonces, aquel conflicto armado

[28] Tal y como indica Salmón, los demás principios del DIH se desprenden del principio de humanidad. (Salmón, 2016)

en el que se combinan tanto métodos convencionales o cinéticos, es decir, el uso de fuerza militar en el sentido tradicional, con métodos no convencionales, como los ciberataques. La característica principal de este tipo de conflictos es que ambos métodos se fusionan en un mismo espacio de combate, ya que los métodos no convencionales pretenden ser tan decisivos como los métodos convencionales; esto es, no buscan únicamente alargar el conflicto, provocar reacciones o incrementar los costos de seguridad, sino más bien afectar las capacidades críticas de los Estados (Hoffman, 2007, p. 29).

En este sentido, Galán señala que "es más preciso utilizar el término guerra híbrida solo cuando existe un conflicto armado declarado y no encubierto y, en consecuencia, se activa la aplicación del Derecho Internacional Humanitario (DIH)" (p. 4). Sin embargo, es importante resaltar, tal y como se señaló anteriormente, que las normas del DIH no aplican únicamente a conflictos declarados, sino a todos aquellos que cumplen con los criterios de intensidad y organización.

Al respecto, cabe señalar que, en consonancia con lo dicho por Melzer (2011), cuando las normas del derecho internacional humanitario fueron redactadas, el desarrollo tecnológico no permitía pensar en la posibilidad de realizar ciberataques (p. 22). Sin embargo, el art. 36 del Protocolo Adicional I a los Convenios de Ginebra (1977) prevé lo siguiente:

> Cuando una Alta Parte contratante estudie, desarrolle, adquiera o adopte una nueva arma, o nuevos medios o métodos de guerra, tendrá la obligación de determinar si su empleo, en ciertas condiciones o en todas las circunstancias, estaría prohibido por el presente Protocolo o por cualquier otra norma de derecho internacional aplicable a esa Alta Parte contratante. (Protocolo Adicional I, art. 36)

Esta norma se refiere a que, en el desarrollo de un arma nueva, deberán observarse los principios y normas del DIH, y esto no excluye a los ciberataques (Melzer, 2011, p. 23). Sin embargo, se requiere que el ciberataque tenga un nexo directo al conflicto armado, esto es, que sea usado como método no convencional de ataque[29] en el contexto de una guerra híbrida (Melzer, p. 23). El Manual de Tallinn 2.0 (2017) se pronuncia en la misma línea al señalar que "las operaciones cibernéticas ejecutadas en el contexto de un conflicto armado están sujetas a las leyes de los conflictos armados" (Regla 20).

Esta tesis no pretende hacer un análisis exhaustivo de los tipos de conflictos armados, sin embargo, sí conviene precisar que la doctrina tradicional prevé dos tipos de conflictos:

- Conflicto Armado Internacional (CAI): Se trata de "una confrontación armada entre entidades estatales" (Verri, 2014, p. 25). Al respecto, el Manual de Tallinn 2.0 (2017) prevé que las hostilidades pueden incluir, o incluso limitarse[30], a ciberataques (p. 83-84).
- Conflicto Armado No Internacional (CANI): Se refiere al "enfrentamiento entre las fuerzas armadas de un Estado y las fuerzas armadas disidentes o rebeldes" (Verri, 2014, p. 26). Al respecto, se requiere que dichos enfrentamientos tengan un cierto nivel de intensidad, y las partes en conflicto tengan un mínimo de organización (Salmón, 2016, pp. 130–131). Además, el Manual de Tallinn 2.0 (2017) señala que es posible que las

[29] Por ataque se entienden los "actos de violencia contra el adversario, sean ofensivos o defensivos" (Comité Internacional de la Cruz Roja, 1977, art. 49.1).
[30] En el supuesto de que se un CAI se limite a operaciones cibernéticas, se denominaría una guerra cibernética, y por lo tanto no podríamos estar hablando de una guerra híbrida.

hostilidades impliquen ciberataques (p. 85).

En este sentido, en tanto un ciberataque sea perpetrado como parte de un CAI o de un CANI, serán de aplicabilidad, en primer lugar, los principios del DIH. El primero de ellos es el principio de distinción, contemplado en la Regla 31 del Manual de Tallinn 2.0, y también en otros cuerpos normativos vinculantes. Este principio está explicado en el art. 48 del Protocolo Adicional I a los Convenios de Ginebra (1977):

> A fin de garantizar el respeto y la protección de la población civil y de los bienes de carácter civil, las Partes en conflicto harán distinción en todo momento entre población civil y combatientes, y entre bienes de carácter civil y objetivos militares y, en consecuencia, dirigirán sus operaciones únicamente contra objetivos militares. (Protocolo Adicional I, art. 48)

Como consecuencia de este principio, "no serán objeto de ataque la población civil como tal ni las personas civiles" (Comité Internacional de la Cruz Roja, 1977, art. 51.2). Al respecto, José Luis Miní y Julia Corí (2003) señalan que este principio tiene un doble efecto: por un lado, distinguir a aquellos que participan de las hostilidades[31] de los que no, y por otro, conocer quién o qué puede ser objeto de un ataque armado[32] (p. 137) (ver también Chinkin & Kaldor,

[31] Para determinar la participación directa en las hostilidades deben cumplirse tres condiciones: umbral del daño (probabilidad de que el acto tenga efectos negativos contra una de las partes en conflicto); causalidad directa (vínculo causal entre el acto y el daño causado); y nexo beligerante (el propósito del acto debe ser causar daño en apoyo de una de las partes en conflicto). (Melzer, 2010)

[32] "En lo que respecta a los bienes, los objetivos militares se limitan a aquellos objetos que por su naturaleza, ubicación, finalidad o utilización contribuyan eficazmente a la acción militar o cuya destrucción total o parcial, captura o neutralización ofrezca en las circunstancias del caso una ventaja militar definida." (Comité Internacional de la Cruz Roja, 1977, p. 52.2)

2017, pp. 238–239). Además, se requiere que un ciberataque perpetrado en el contexto de una guerra híbrida, y que vaya dirigido contra la población o bienes civiles, alcance el estado de un ataque armado, esto es, que revista un alto grado de severidad (lo cual ya fue explicado anteriormente) (Manual de Tallinn 2.0, 2017, p. 112).

Es de este principio del que se derivan diferentes normas de protección, estipuladas entre las Reglas 43 y 40 del Manual de Tallinn 2.0, tanto para la población civil, e incluso a individuos en particular, en tanto estos no participen de las hostilidades, y bienes civiles, esto es infraestructura que no sea usada como objetivo militar.

El segundo principio fundamental es el de proporcionalidad, que, si bien no está expresamente recogido por las normas del DIH, debe entenderse como una exigencia de que los métodos y medios de combate no sean desproporcionados en relación con la ventaja militar buscada (Miní & Cori, 2003, p. 137; Verri, 2014, p. 89).

Chinkin y Kaldor (2017) señalan que debe distinguirse entre la proporcionalidad *ad bellum* y la proporcionalidad *in bello*:

> La proporcionalidad *ad bellum* se refiere al criterio para recurrir a la guerra en sí mismo, que el daño causado por la guerra sea menor que el beneficio de pelear la guerra; la proporcionalidad *in bello* se refiere a la aplicación mínima de fuerza, no más de la necesaria para alcanzar un objetivo militar en particular. (Chinkin & Kaldor, p. 239) [Traducción propia]

Siendo que, en este supuesto ya se está frente a un conflicto armado, no corresponde analizar la proporcionalidad *ad bellum*, sino más bien la intensidad de la fuerza que resulte necesaria para alcanzar un objetivo militar, es decir la

proporcionalidad *in bello*.

Respecto de los ciberataques, el Manual de Tallinn 2.0 (2017) es bastante más específico en la delimitación del principio de proporcionalidad:

> Un ciberataque que puede esperarse que cause pérdida incidental de vidas civiles, daños a civiles, daño a objetos civiles o una combinación de las anteriores, que sea excesivo en relación con la ventaja militar concreta y directa que haya sido anticipada, está prohibido. (Manual de Tallinn 2.0, Regla 51) [Traducción propia]

De este principio se desprende la prohibición contemplada en las Reglas 42[33] y 43[34] del Manual de Tallinn, referidas al empleo de métodos y medios de ciberataques que causen daños superfluos, innecesarios o indiscriminados.

La contracara del principio de proporcionalidad es el principio de necesidad militar, que "permite solamente a los combatientes debilitar o destruir el potencial bélico de su contendor, de forma que no se causen daños desproporcionados al objetivo que se persigue" (Miní & Cori, 2003, p. 135). Este principio se constituye en la justificación de un ataque en el marco de un conflicto armado, ya que "la necesidad militar (…) solo puede invocarse si en el derecho positivo se admite explícitamente que, por excepción hecha en nombre de esta necesidad, se suspenda una prohibición o una limitación [contemplada por las normas del *ius in bello*]" (Verri, 2014, p. 70). Se considera que, si bien este principio no ha sido recogido en el Manual de Tallinn 2.0, su aplicación resulta

[33] "Se prohíbe usar medios y métodos de ciber guerra cuya naturaleza sea causar daños superfluos o sufrimiento innecesario". (Manual de Tallinn 2.0, Regla 42) [Traducción propia]

[34] "Se prohíbe emplear medios y métodos de ciber guerra que sean indiscriminados por naturaleza. Los medios y métodos de ciber guerra son indiscriminados por naturaleza cuando no: (a) son dirigidos a un objetivo militar específico, o; (b) son limitados en sus efectos, según lo requerido por las leyes de los conflictos armados; y consecuentemente tienen la naturaleza de atacar objetivos militares y población o bienes civiles sin distinción." (Manual de Tallinn 2.0, 2017, Regla 43) [Traducción propia]

fundamental en el contexto de una guerra híbrida, que incluya a ciberataques como medios no convencionales. Así las cosas, este principio permitirá determinar de modo adecuado y concreto cuándo es posible atacar una cierta infraestructura cibernética o no, y es posible justificar este ataque dentro de la necesidad militar.

Además del principio de necesidad militar, existen otros no contemplados en el DIH. En primer lugar, de la definición de esta rama del derecho se desprende el principio de humanidad, que, como ya fue explicado anteriormente, "consiste en respetar y tratar a todas las personas con humanidad, tanto a los combatientes –a quienes no se les hará padecer sufrimientos innecesarios–, como a los no combatientes –quienes en todo momento deberán ser tratados con humanidad" (Salmón, 2016, pp. 59–60; ver también Miní & Cori, 2003). De este se deriva el principio de limitación, que señala que "el derecho a elegir los métodos y medios de combate no es ilimitado, sino que deben atenderse razones humanitarias" (Salmón, 2016, pp. 61–62; ver también Miní & Cori, 2003). Además, la prohibición de causar daños superfluos o innecesarios tiene la finalidad de "prohibir las armas pensadas para ocasionar efectos innecesarios en relación con el fin de dejar a los enemigos fuera de combate" (Salmón, 2016, p. 62; ver también Miní & Cori, 2003). Es fundamental que los ciberataques respeten estos principios, y que no causen más daños de los necesarios, o que afecten gravemente a la población civil.

En conclusión, y en línea con lo señalado por Melzer (2011), si bien es cierto que aún los ciberataques no tienen un alto potencial destructivo, su potencial para causar daños incrementa cada vez más, con "la creciente dependencia en los sistemas controlados por computadoras para sostener nuestras vidas diarias" (p. 36). En este sentido, resulta necesario limitar los potenciales efectos negativos que éstos puedan tener en el caso de un conflicto armado, y de allí la importancia de aplicar los principios del DIH al caso de las

guerras híbridas.

Cuadro No. 6: Respuesta a un ciberataque en el contexto de una amenaza híbrida aplicando las normas de *ius in bello*

Para que un ciberataque en el contexto de una amenaza híbrida pueda ser respondido aplicando las normas del *ius in bello* deben cumplir las siguientes condiciones:

- Sea equiparable a un ataque armado.
- Sea atribuible a un Estado.
- Ocurra en el marco de un conflicto armado (sea CAI o CANI).

Entonces, para poder realizar un ciberataque como parte de las acciones militares del conflicto armado, el Estado deberá respetar los siguientes principios del DIH:

- Humanidad
- Distinción
- Proporcionalidad
- Necesidad militar
- Limitación
- Prohibición de causar daños superfluos o innecesarios

Fuente: Elaboración propia

Marco normativo peruano:

En esta sección se describirá, brevemente, cuál es el marco normativo aplicable en el Perú respecto de los ciberataques, y cuáles son las competencias de Cancillería en la materia.

Normas sobre Ciberdefensa:

La defensa nacional es una de las funciones del Estado, según lo señalado en el art. 44 de la Constitución:

> Son deberes primordiales del Estado: *defender la soberanía nacional*; garantizar la plena vigencia de los derechos humanos; proteger a la población de las amenazas contra su seguridad; y promover el bienestar general que se fundamenta en la justicia y en el desarrollo integral y equilibrado de la Nación. (Constitución Política Del Perú, 1993, art. 44) [Énfasis agregado]

La defensa de la soberanía es la primera que se asigna al Estado, y Enrique Bernales Ballesteros (2012) la explica de la siguiente manera:

> Tiene que ver tanto con la protección del Perú frente a las amenazas del exterior, como frente a las amenazas que provengan del interior. Se amenaza la soberanía cuando un Estado extranjero pretende parte de nuestro territorio o su dominación política. Pero también queda amenazada cuando una fuerza organizada y con múltiples ramificaciones, el narcotráfico por ejemplo, pretende ejercer influencia en las decisiones internas para facilitar sus actividades. (p. 323)

En esta línea, el Estado debe tomar todas las medidas necesarias para evitar que su soberanía sea vulnerada. Jorge León Vásquez (2013) señala que la defensa de la soberanía, "en su dimensión externa, (…) implica para el Estado soberano la exclusión de toda forma de subordinación" (p. 945). De igual manera Salmón (2014a) señala que uno de los atributos de la soberanía es el "derecho de excluir que otro Estado ingrese a su territorio" (p. 65), por lo tanto, el Perú

puede tomar todas las acciones necesarias para evitar que ello suceda.

Entonces, cuando un ciberataque afecta tanto a la población civil como a bienes ubicados dentro del territorio nacional, es posible afirmar que se ha vulnerado el principio de inviolabilidad territorial (tal y como se explicó anteriormente), y la soberanía del Perú ha sido afectada. Por lo tanto, es fundamental que el Estado ejerza la defensa de la soberanía, respondiendo a dicho ciberataque, aplicando las normas del derecho internacional que correspondan.

Por otro lado, tal y como señala León Vásquez (2013) al comentar el art. 44, las amenazas a la seguridad no deben entenderse únicamente en el sentido de conflictos armados, sino que, existen otras amenazas no tradicionales que "obligan a los actuales Estados democráticos a elaborar, desarrollar y ejecutar políticas públicas, a fin de brindar a la población las condiciones necesarias para garantizar su seguridad" (p. 947). Es por ello por lo que la Política Nacional Multisectorial de Seguridad y Defensa Nacional al 2030, aprobada mediante Decreto Supremo No. 005-2021-DE, y citando lo señalado por la Política de Inteligencia Nacional, reconoce que los ataques a la seguridad digital son un tipo de amenaza generadora de escenario de riesgo. Así las cosas, esta norma reconoce lo siguiente:

> El entorno digital brinda ventajas para un mayor desarrollo y bienestar de las personas y las organizaciones, pero también, nos hace altamente vulnerables a una amplia variedad de peligros y riesgos físicos como cibernéticos. Los actores estatales y no estatales tradicionales y no convencionales, actúan virtualmente, desde cualquier parte del mundo, explotando las fragilidades de nuestro entorno digital a efectos de robarnos información sensible de interés, y así, interrumpir, poner en peligro o destruir nuestra capacidad de proveer servicios eficientes a la

población. (D.S. 005-2021-DE, 2021, p.86)

Para mitigar estas amenazas se promulgó la Ley No. 30999, Ley de Ciberdefensa, cuya finalidad es “defender y proteger la soberanía, los intereses nacionales, los activos críticos nacionales y recursos claves para mantener las capacidades nacionales frente a amenazas o ataques en y mediante el ciberespacio, cuando estos afecten la seguridad nacional” (Ley 30999, 2019, art. 2).

Esta ley define a las Fuerzas Armadas como órganos ejecutores de todas las acciones vinculadas a la ciberdefensa (*Ley 30999*, art. 5), e impone el respeto a las disposiciones sobre *ius ad bellum* y *ius in bello* de la siguiente manera:

> El uso de la fuerza por la Fuerzas Armadas en y mediante el ciberespacio se sujeta a las disposiciones contenidas en el artículo 51 de la Carta de las Naciones Unidas y el presente dispositivo legal, y está regido por las normas del Derecho Internacional de los Derechos Humanos y del Derecho Internacional Humanitario que sean aplicables. (*Ley 30999*, art. 9)

Esto significa que, en todo el accionar que realicen frente a aquellos ciberataques que afecten la seguridad nacional, las Fuerzas Armadas deberán respetar las normas del derecho internacional que resulten aplicables, a saber, el *ius in bello* y el ius *ad bellum*, así como las normas del Derecho Internacional de los Derechos Humanos pertinentes. Es decir, deberá respetarse, entre otros, todo el marco normativo ya explicado en este capítulo. No obstante, es importante señalar que no hay un reglamento de la Ley 30999, por lo que la manera en la que deberán aplicarse las normas no está desarrollada.

Rol de Cancillería:

Tal y como se explicó, del art. 44 de la Constitución se desprende el deber de defensa de la soberanía del Estado. Si bien podría parecer que cancillería no juega un papel en esta función, la Ley de Organización y Funciones (en adelante, LOF) señala, como parte de sus funciones específicas, que este ministerio puede "participar en el Sistema de Seguridad y Defensa Nacional" (Ley 29357, 2009, art. 6).

Ello se desarrolla a través del art. 6 del Decreto Legislativo No. 1129, que el Sistema de Defensa Nacional (2012). Dicho artículo detalla que el Ministerio de Relaciones Exteriores forma parte del Consejo de Seguridad Nacional. Además, el reglamento de esta norma, aprobado mediante Decreto Supremo No. 037-2013-PCM, entiende que una de las funciones relacionadas a la defensa nacional vinculadas al Ministerio de Relaciones Exteriores es la formulación de la política exterior del Perú en la materia, así como la representación del Estado y la defensa de la soberanía (D.S. 037-2013-PCM, 2013, art. 4). Asimismo, y como parte del Consejo de Seguridad Nacional, Cancillería tiene la potestad de "asesorar al Consejo sobre los aspectos relacionados a su competencia" (D.S. 037-2013-PCM, art. 12).

De igual manera, el Reglamento de Organización y Funciones del ministerio (en adelante, ROF) reitera esta función específica (D.S. 135-2010-RE, 2010, art. 3). En este sentido, es posible que Cancillería se constituya en asesor del Consejo de Seguridad Nacional para la implementación de las normas de derecho internacional que correspondan, en este caso, *ius ad bellum* y *ius in bello*. En el capítulo III se desarrollará de manera más detallada las funciones específicas de los órganos competentes de Cancillería.

Es por ello por lo que el Ministerio de Relaciones Exteriores, dentro del modelo conceptual planteado en el Plan Estratégico Sectorial Multianual

(PESEM) 2015-2025[35] (2015), se refiere al componente de “defensa de la soberanía y protección de los intereses nacionales permanentes en el exterior” (p. 7). Además, el PESEM define a la defensa de la soberanía como “el conjunto de acciones político-diplomáticas que despliega el sector para cautelar, defender y proteger la soberanía nacional y la integridad territorial” (p. 45).

Asimismo, en su Plan Estratégico Institucional 2020-2022 (2019), el Ministerio de Relaciones Exteriores contempló entre sus acciones estratégicas institucionales el “preservar y defender la soberanía nacional” (p. 8), así como “ampliar el protagonismo del Perú en los principales organismos internacionales con miras a reafirmar la vigencia del derecho internacional” (p. 8).

[35] Mediante Resolución Ministerial 0657-2021/RE, emitida el 30 de diciembre de 2021, se amplió el horizonte temporal del PESEM hasta el 2025.

CAPÍTULO II

METODOLOGÍA

ENFOQUE, ALCANCE Y DISEÑO DE INVESTIGACIÓN:

Esta investigación tiene un enfoque cualitativo, que Ñaupas et al. (2014) consideran como “un estilo que adopta el investigador en razón del objeto de estudio, de sus objetivos, de los problemas concretos que selecciona en su área profesional” (p. 353). En la misma línea, Hernández et al. (2014) señalan que “el enfoque cualitativo se selecciona cuando el propósito es examinar la forma en que los individuos perciben y experimentan los fenómenos que los rodean, profundizando en sus puntos de vista, interpretaciones y significados” (p. 7). Por lo tanto, “pueden desarrollar preguntas e hipótesis antes, durante o después de la recolección y el análisis de los datos” (Hernández et al., 2014, p. 7). Es decir, no hay un proceso de investigación definido, sino que se irá construyendo conforme se vaya avanzando en la investigación.

Asimismo, el alcance de esta investigación es descriptivo, que Hernández et al. (2014) definen como aquel tipo de estudio que “busca especificar propiedades y características importantes de cualquier fenómeno que se analice” (p. 92). Es así como esta tesis busca estudiar las características de las amenazas híbridas en el ciberespacio, para, a partir de ello, determinar cuáles son las normas de derecho internacional que deben ser aplicadas para responder a éstas.

Finalmente, esta investigación tiene un diseño de teoría fundamentada. Según Hernández et al. (2014), este tipo de investigación busca “desarrollar teoría basada en datos empíricos” (p. 472). Asimismo, señalan que, en este diseño, “el investigador produce una explicación general o teoría respecto a un fenómeno, proceso, acción o interacciones que se aplican a un contexto

concreto y desde la perspectiva de diversos participantes" (Hernández et al., 2014, p. 472). En esta investigación, entonces, a partir de la revisión de las teorías ya presentadas en el marco teórico y normativo, se determinará cuáles son las normas que el Perú debe aplicar al responder a las amenazas híbridas que se susciten desde el ciberespacio.

SUJETOS DE ESTUDIO:

En esta investigación existen dos sujetos de estudio: la doctrina y los sujetos de entrevistas. En primer lugar, se realizó un estudio de documentación que conforma la doctrina en la materia. Luego, se entrevistó a dos juristas especializados en el tema del *ius ad bellum* y *ius in bello*, así como a miembros del Servicio Diplomático de la República, específicamente de la Dirección de Seguridad y Defensa.

TÉCNICAS Y HERRAMIENTAS DE RECOJO DE INFORMACIÓN Y ANÁLISIS:

A partir de los sujetos de estudios, se utilizaron dos técnicas de recojo de información, y sus correspondientes herramientas. La primera técnica es el análisis documental, que, en opinión de Hernández et al., "le sirven al investigador para conocer los antecedentes de un ambiente, así como las vivencias o situaciones que se producen en él y su funcionamiento cotidiano y anormal" (p. 415). Así, la herramienta a utilizar será la lista de cotejo.

La segunda técnica es la entrevista, que Hernández et al. (2014) definen como "una reunión para conversar e intercambiar información entre una persona (el entrevistador) y otra (el entrevistado) u otras (entrevistados)" (p. 403). A partir de ello, la herramienta a utilizar será una guía de entrevista.

CAPÍTULO III

DISCUSIÓN DE RESULTADOS

ANÁLISIS DE LA NORMATIVA PERUANA SOBRE CIBERATAQUES EN EL CONTEXTO DE AMENAZAS HÍBRIDAS:

Normativa sobre ciberdefensa:

La Política Nacional de Seguridad y Defensa Nacional del Estado Peruano, aprobada mediante Decreto Supremo No. 012-2017-DE[36], reconoce lo siguiente:

> Las tecnologías de la información están cada vez más integradas a la operación de infraestructura física, incluida la infraestructura crítica, por lo que hay un mayor peligro de que se pueda dañar o interrumpir el funcionamiento de las mismas, poniendo en riesgo la economía y la vida cotidiana de millones de personas. A la luz de estos riesgos y sus potenciales consecuencias, proteger el ciberespacio y su infraestructura se convierte en un asunto de Seguridad Nacional. (D.S. 012-2017-DE, 2017, p.21)

En este sentido, se reconoce que la infraestructura cibernética, así como el ciberespacio, son importantes en el desarrollo de las actividades del Estado, y, por tanto, es fundamental combatir las amenazas que pueden surgir contra estos. En este sentido, su protección se vuelve fundamental, por lo que la ciberdefensa se vuelve prioritaria. Ello se confirma al revisar el Objetivo No. 1 de

[36] Cabe resaltar que este D.S. fue derogado por el D.S. 005-2021-DE, que aprueba la "Política Nacional Multisectorial de Seguridad y Defensa al 2030". Sin embargo, se cita la norma derogada debido a que hace referencia directa a la ciberdefensa, mientras que la normativa vigente no la aborda a ese nivel de profundidad.

la Política, garantizar la soberanía, independencia, integridad territorial y la protección de intereses nacionales. Al respecto, una de las acciones fundamentales de este objetivo es “proteger los activos críticos nacionales (ACN) contra todo tipo de amenazas, así como los sistemas de información, de las amenazas que, desde el ciberespacio, atenten contra la Seguridad y Defensa Nacional” (D.S. 012-2017-DE, 2017, p. 26). No obstante, aquí es importante hacer una atingencia, y es que la Política de Seguridad y Defensa Nacional no se refiere a ciberdefensa, sino a ciberseguridad. Asimismo, es importante resaltar que dicha política ha sido derogada. No obstante, la Política Nacional Multisectorial de Seguridad y Defensa Nacional al 2030, que se encuentra vigente, no aborda este tema con la misma profundidad.

El tema de la ciberdefensa ha sido desarrollado a través de la Ley No. 30999, Ley de Ciberdefensa, cuya finalidad es “defender y proteger la soberanía, los intereses nacionales, los activos críticos nacionales y recursos claves para mantener las capacidades nacionales frente a amenazas o ataques en y mediante el ciberespacio, cuando estos afecten la seguridad nacional” (Ley 30999, 2019, art. 2).

Esta ley entiende que la ciberdefensa es “la capacidad militar que permite actuar frente a amenazas o ataques realizados en y mediante el ciberespacio cuando estos afecten la seguridad nacional” (Ley 30999, 2019, art. 4). Asimismo, asigna a las Fuerzas Armadas como órganos ejecutores de todas las acciones vinculadas a la ciberdefensa (*Ley 30999*, art. 5), e impone el respeto a las disposiciones sobre *ius ad bellum* y *ius in bello* en todo el accionar que realicen frente a aquellos ciberataques que afecten la seguridad nacional (*Ley 30999*, art. 9).

No obstante, esta norma no ha definido qué tipo de ataques activarían una respuesta a través de la ciberdefensa, sino que se ha limitado a señalar que se aplicará la ley frente a amenazas o ataques que afecten la seguridad

nacional. Ello demuestra que no se ha recogido lo desarrollado en el Marco Teórico (Capítulo 1) acerca de la gravedad (equipararlo a un ataque armado cinético) o atribución de los ciberataques.

Por otro lado, esta ley desarrolla únicamente las normas vinculadas al *ius ad bellum*, ya que contempla que "*toda amenaza o ataque en y mediante el ciberespacio* que ponga en riesgo la soberanía, los intereses nacionales, los activos críticos nacionales y recursos claves para mantener las capacidades nacionales, da lugar al *ejercicio del derecho de legítima defensa*" (Ley 30999, 2019, art. 10) [énfasis agregado]. Asimismo, sujeta la legítima defensa a los principios de legalidad[37], necesidad y oportunidad (*Ley 30999*, art. 11).

En otras palabras, en opinión del teniente FAP Kenny Keith Meza Chalco, Jefe de la División de Respuesta del COCID del CCFFAA, quien fue entrevistado para esta investigación, el uso de la fuerza por la Fuerzas Armadas en y mediante el ciberespacio se sujeta a las disposiciones contenidas en el artículo 51 de la Carta de las Naciones Unidas y la Ley 30999, y está regido por las normas del Derecho Internacional de los Derechos Humanos y del Derecho Internacional Humanitario.

De lo observado en el Capítulo I, la norma parece estar en consonancia con lo propuesto por el Manual de Tallinn 2.0. Sin embargo, no ha recogido el principio de proporcionalidad, que resulta de aplicación fundamental para la legítima defensa. Tampoco ha desarrollado qué normas de *ius in bello* resultarían aplicables. Por lo tanto, se puede afirmar que esta norma por sí sola no permitiría un adecuado manejo de ciberataques en el contexto de amenazas híbridas.

De la misma opinión es el teniente FAP Meza, y señala que, si bien es

[37] Por legalidad debe entenderse que "en el caso de conducir una operación de respuesta en y mediante el ciberespacio que contenga un ataque deliberado, debe realizarse de acuerdo a ley" (Ley 30999, 2019, art. 11).

cierto que la Ley de Ciberdefensa hace referencia, en su Capítulo II, al -uso de la fuerza en y mediante el ciberespacio-, aún no se tiene la reglamentación de dicha Ley, lo que ayudaría de manera para una mejor planificación y panorama, frente al ejercicio del Derecho Internacional de los Derechos Humanos y del Derecho Internacional Humanitario frente a operaciones cibernéticas. Esto presenta una oportunidad para Cancillería, tal y como se explicará en la próxima sección.

Dicho esto, es importante precisar que el Perú no cuenta con una norma relativa al uso de la fuerza en caso de un CAI. Sin embargo, sí existe una norma que regula el uso de la fuerza cinética dentro del territorio nacional en casos de un estado de emergencia en el territorio nacional[38], a saber, el Decreto Legislativo 1095. El art. 1 de dicha norma señala lo siguiente:

> [Regular] los principios, formas, condiciones y límites para el empleo y uso de la fuerza por parte de las Fuerzas Armadas en cumplimiento de su función constitucional, mediante el empleo de su potencialidad y capacidad coercitiva para la protección de la sociedad, en defensa del Estado de Derecho y a fin de asegurar la paz y el orden interno en el territorio nacional. (Dec. Leg. 1095, 2010) [art. 1]

Además, esta norma contempla que las Fuerzas Armadas intervendrán para "prestar apoyo a la Policía Nacional, en casos de (…) protección de instalaciones estratégicas para el funcionamiento del país, servicios públicos

[38] De conformidad con el art. 137 de la Constitución, el estado de emergencia aplica "en caso de perturbación de la paz o del orden interno, de catástrofe o de graves circunstancias que afecten la vida de la Nación" (*Constitución Política Del Perú*, 1993). En caso sea declarado, "puede restringirse o suspenderse el ejercicio de los derechos constitucionales relativos a la libertad y la seguridad personales, la inviolabilidad del domicilio, y la libertad de reunión y de tránsito en el territorio" (*Constitución Política Del Perú*, 1993).

esenciales" (Dec. Leg. 1095, 2010) [art. 4.3]. Sin embargo, prevé dos supuestos de intervención, frente a los cuáles aplican marcos normativos diferentes:

- El artículo 5.1 del Dec. Leg. 1095 contempla, en el primer supuesto, permitir a las Fuerzas Armadas conducir operaciones militares para hacer frente a un grupo hostil (Dec. Leg. 1095, 2010). En este caso, resultarán de aplicación las normas sobre el *ius in bello*.
- En los artículos 5.2 y 5.3 se contempla la intervención de las Fuerzas Armadas, con el objetivo de apoyar a la Policía Nacional para el control del orden interno (Dec. Leg. 1095, 2010). En este caso, se deberán aplicar las normas de derechos humanos que correspondan.

En este sentido, es posible entender que esta norma habilita a las Fuerzas Armadas a aplicar los principios de las normas del *ius in bello*, explicados en el capítulo I de la presente investigación, tanto exista la necesidad de responder a un grupo hostil, para proteger aquellas instalaciones que se consideren estratégicas para el funcionamiento del país, es decir, infraestructura crítica, de cualquier tipo de amenazas. Así, resultan de aplicación los principios de humanidad, distinción, limitación, necesidad militar y proporcionalidad, explicados en el art. 7 del Dec. Leg. 1095 y su reglamento, aprobado por D.S. 003-2020-DE, en caso de cualquier modalidad de empleo de la fuerza cinética.

En opinión de Juan José Alencastro Moya, Asesor Jurídico del Comité Internacional de la Cruz Roja para el Perú, Bolivia y Ecuador, quien fue entrevistado para esta investigación, estos principios deberían poder aplicarse *mutatis mutandis* a cualquier ciberoperación. Sin embargo, añade que es importante que países como el Perú, que no cuentan con amplias capacidades tecnológicas, deben observar el ciberespacio y las amenazas que se gestan desde este escenario como un problema y una oportunidad, y por lo tanto deben

comenzar a desarrollar una normativa robusta para proteger este entorno.

Oportunidades para Cancillería:

Antes de ingresar a analizar las oportunidades, es importante recordar la competencia que tiene Cancillería en el ámbito de la defensa nacional. Al respecto, el art. 6 del Decreto Legislativo No. 1129, que estableció el Sistema de Defensa Nacional, señala que el Consejo de Seguridad Nacional, ente máximo de este sistema, incluye al Ministerio de Relaciones Exteriores (D.Leg. 1129, 2012). Además, el reglamento de esta norma, aprobado mediante Decreto Supremo No. 037-2013-PCM, entiende que una de las funciones relacionadas a la defensa nacional vinculadas al Ministerio de Relaciones Exteriores es la formulación de la política exterior del Perú en la materia, así como la representación del Estado y la defensa de la soberanía (D.S. 037-2013-PCM, 2013, art. 4). Asimismo, y como parte del Consejo de Seguridad Nacional, Cancillería tiene la potestad de "asesorar al Consejo sobre los aspectos relacionados a su competencia" (D.S. 037-2013-PCM, art. 12).

Dicho esto, la normativa específica de Cancillería, la Ley de Organización y Funciones (en adelante, LOF) señala, como parte de sus funciones específicas, que a este ministerio le corresponde "participar en el Sistema de Seguridad y Defensa Nacional" (Ley 29357, 2009, art. 6). El Reglamento de Organización y Funciones del ministerio (en adelante, ROF) reitera esta función específica (D.S. 135-2010-RE, 2010, art. 3). En este sentido, es posible que Cancillería se constituya en asesor del Consejo de Seguridad Nacional para la implementación de las normas de derecho internacional que correspondan, en este caso, *ius ad bellum* y *ius in bello*.

Por otro lado, la LOF establece la organización interna de Cancillería, creando, como órganos de línea a las Direcciones Generales que correspondan (Ley 29357, art. 13). Es el ROF el que detalla que uno de los órganos de línea es

la Dirección General de Asuntos Multilaterales y Globales (en adelante, DGM), a quien asigna la función de promover y proteger los intereses del Perú en materia de seguridad internacional, entre otros temas, así como de negociar sobre tales asuntos (D.S. 135-2010-RE, 2010, art. 93), y señala que, para ello, puede "coordinar con los sectores públicos y privados pertinentes a fin de conciliar las posiciones de dichos sectores con la política exterior del Estado" (D.S. 135-2010-RE, art. 94). En esta línea, es perfectamente posible establecer canales de cooperación a fin de articular una política de defensa nacional en materia de ciberdefensa.

También es importante resaltar que, dentro de la estructura de la DGM, se encuentran la Dirección de Seguridad y Defensa (en adelante, DSD) y la Dirección de Derechos Humanos (en adelante, DDH) (D.S. 135-2010-RE, 2010, art. 95). La DSD tiene entre sus funciones "analizar el tratamiento multilateral a los asuntos de seguridad internacional, desarme, no proliferación y los demás temas que le sean encomendados" (D.S. 135-2010-RE, art. 97), y por lo tanto resultaría el órgano idóneo para realizar un análisis comparado de las políticas de ciberdefensa, esto es, de qué manera se incorporan tanto las normas de *ius ad bellum* como de *ius in bello* a las políticas de ciberdefensa a nivel mundial.[39] Asimismo, la DDH tiene entre sus funciones "fomentar, en calidad de miembro de la Comisión Nacional de Estudio y Aplicación del Derecho Internacional Humanitario – CONADIH, la aplicación y difusión del Derecho Internacional Humanitario" (D.S. 135-2010-RE, art. 99), por lo que este órgano podría estudiar, a partir del análisis que se realice en la DSD, cuáles son las normas de *ius in bello* que resultarían aplicables dentro del marco jurídico del Perú.

En esta línea, es importante resaltar que el teniente FAP Meza señala

[39] En cumplimiento con lo dispuesto por el ROF, y a fin de articular una interpretación integral respecto de las normas del DIH, corresponde que la DSD solicite opinión tanto a la Dirección General de Tratados como a la Oficina General de Asuntos Legales en lo que corresponda a cada una en el ámbito de su competencia.

que el CCFFAA, a través del COCID, tiene estrechos lazos de cooperación con los países que actualmente se encuentran en desarrollo de la normativa en ciberdefensa, gracias a reuniones bilaterales y tripartitas, las cuales son planificadas gracias al Ministerio de Relaciones Exteriores.

Asimismo, en entrevista para esta investigación, el Ministro SDR Gonzalo Voto Bernales, Director de Seguridad y Defensa, señaló que la DSD ha impulsado el acercamiento del COCID con reputados centros de excelencia sobre la materia, como lo son: el Centro Europeo de Excelencia contra Amenazas Híbridas (HybridCoE), con sede en Helsinki; y, el Centro de Excelencia de Ciberdefensa Cooperativa (CCDCoE) de la OTAN. El Perú fue el primer país de América Latina en acercarse al HybridCoE y, dadas les reuniones celebradas, se pudieron establecer puntos de contacto para una comunicación directa entre el COCID y estos Centros de Excelencia, lo cual coadyuvará a su trabajo.

Por otro lado, también es importante destacar que el Perú participa activamente en los procesos multilaterales más importantes para la promoción de una conducta responsable de los Estados en el ciberespacio: el Grupo de Trabajo de Composición Abierta sobre los avances en el ámbito de la información y las telecomunicaciones en el contexto de la seguridad internacional (OEWG, por sus siglas en inglés)[40] y el Grupo de Trabajo de Medidas de Fomento de la Confianza y Cooperación en el Ciberespacio[41] del CICTE - OEA.

[40] De acuerdo con la Resolución 73/27 de la Asamblea General de la ONU, del 5 de diciembre de 2018, el OEWG tiene el objetivo de establecer normas y principios que regulen el comportamiento responsable de los Estados en el ciberespacio.
[41] El Grupo de Trabajo de Medidas de Fomento de la Confianza y Cooperación en el Ciberespacio fue creado mediante Resolución CICTE/RES.1/17, del Comité de Interamericano contra el Terrorismo de la OEA, con el objetivo de mejorar la cooperación y reducir las posibilidades de conflicto que puedan surgir por el uso de la tecnología. Es importante resaltar que esta resolución fue presentada por el Perú, junto con las delegaciones de Chile, Colombia, Costa Rica, Canadá, Guatemala y México, el 7 de abril de 2017.

Es así como Cancillería, en opinión del teniente FAP Meza, sirve como nexo para permitir intercambiar información y doctrina, planear operaciones de ciberdefensa, y demás información; en materia de ciberseguridad y ciberdefensa, con los países de la región y del mundo. En la misma línea, el Ministro Voto Bernales resalta una oportunidad para que Cancillería pueda brindar apoyo en la construcción de capacidades y el fortalecimiento de la normativa a partir de la experiencia de otros Estados y los esfuerzos multilaterales que actualmente se están llevando a cabo y que tienen por objetivo estudiar marcos normativos existentes aplicables al contexto cibernético.

ESTUDIO COMPARATIVO DEL TRATAMIENTO DE AMENAZAS HÍBRIDAS EN EL CIBERESPACIO EN OTROS SUJETOS DEL DERECHO INTERNACIONAL:

Tal y como se observó en la sección anterior, la normativa peruana en materia de ciberdefensa presenta muchas oportunidades de mejora, y Cancillería, como parte de su participación en el Sistema de Defensa Nacional, juega un rol importante en la recomendación de la normativa aplicable al responder a las amenazas híbridas en el ciberespacio.

Así, esta sección busca realizar un estudio comparativo cómo otros Estados y Organizaciones Internacional abordan a las amenazas híbridas en el ciberespacio, con el objetivo de brindar recomendaciones respecto de la legislación nacional. Se ha escogido a tres Estados dado que han abordado estos temas de manera directa. No se consideró a ningún Estado de América Latina, ya que, según lo manifestado por Alencastro en entrevista para esta tesis, éstos no han desarrollado el tema de las amenazas híbridas. Asimismo, se desarrollará el tratamiento que la OTAN y la Unión Europea han dado a esta materia, debido a que, si bien la ONU cuenta con el OEWG y el Grupo de Expertos Gubernamentales sobre los Avances en la Esfera de la Información y

las Telecomunicaciones en el Contexto de la Seguridad Internacional (GGE, por sus siglas en inglés)[42], estos se han enfocado en brindar principios más generales respecto de la conducta de los Estados en el ciberespacio, pero no se han enfocado específicamente en el tema de amenazas híbridas.

Estados Unidos:

El desarrollo conceptual de las amenazas híbridas en los Estados Unidos es bastante reciente, y parte de los trabajos del teniente coronel Frank G. Hoffman luego del 11-S (2001). Tal y como se señaló en el marco teórico de esta investigación, Hoffman sostenía que el 11-S determinó la aparición de un nuevo tipo de conflictividad. Así, "los modos de guerra borrosos, la borrosidad de quién lucha y qué tecnologías se aplican, produce una amplia gama de variedad y complejidad que llamamos Conflictividad Híbrida" (Hoffman, 2007, p. 14) [traducción propia]. Esta nueva forma de conflictividad tiene una lógica propia, basada en la "preocupación por entender al adversario, y así, descubriendo sus vulnerabilidades, enfocarse en ellas para obtener una ventaja" (Payá & Luque, 2018, p. 27).

Así, Hoffman entiende a la conflictividad híbrida como aquella "que incorpora capacidades convencionales, tácticas y formaciones irregulares, actos terroristas, que incluyen violencia indiscriminada y coerción, y desorden criminal" (Hoffman, 2007, p. 14). En esta línea, no se eliminan las amenazas tradicionales, sino que las amenazas híbridas se suman y se mezclan con estas, actuando sobre campos antes no previstos. Uno de estos es el ciberespacio, tal y como señala la Guía estratégica provisional de seguridad nacional, aprobada por el

[42] La Resolución 73/266 de la Asamblea General de la ONU solicitó al Secretario General de la ONU crear el GGE con el objetivo de promover normas para el comportamiento responsable de los Estados en el ciberespacio, en el contexto de la seguridad internacional.

presidente Joseph R. Biden en marzo de 2021.[43]

De igual manera, Paul C. Ney Jr. (2020), Consejero General del Departamento de Defensa de los Estados Unidos, reconoce que "el ciberespacio es cada vez más dinámico y disputado, incluso como un dominio de guerra" [página web]. Por lo tanto, este espacio es susceptible de ser afectado a través de distintos tipos de amenazas, desde ciberataques hasta el robo de datos (Ney Jr., 2020). Todas estas amenazas encajan dentro de aquello de Hoffman denominaba conflictividad híbrida, y, tal y como reconoce la Estrategia Militar Nacional del 2018, requieren de una acción militar directa para evitar que erosionen las capacidades críticas del Estado (Junta de Jefes de Estado Mayor de los Estados Unidos, 2018).[44]

Es así como Estados Unidos reconoce la necesidad de "responsabilizar a los actores por actividades cibernéticas maliciosas destructivas, perturbadoras o desestabilizadoras, y responder rápida y proporcionalmente a los ataques cibernéticos imponiendo costos sustanciales a través de medios cibernéticos y no cibernéticos" (Biden, 2021, p. 18). En esta línea, se resalta la importancia de aplicar criterios de atribución para identificar a aquellos que perpetren ciberataques, y la necesidad de responder a estos en estricta aplicación de las normas que correspondan, a saber, el principio de proporcionalidad explicado en

[43] Cabe resaltar que, de conformidad con lo señalado por McInnis (2021), investigadora del Servicio de Investigación del Congreso de Estados Unidos, es la primera vez que la presidencia de Estados Unidos emite una guía provisional. Ello debido a que, de conformidad con la Ley Goldwater-Nichols de reorganización del Departamento de Defensa de 1986 (Ley pública 99-433), corresponde al Congreso emitir la Estrategia de Seguridad Nacional. Por ello, la Guía estratégica provisional de seguridad nacional responde a la visión del presidente Biden respecto de la seguridad nacional y las amenazas que enfrenta el país, y servirá como una guía para el Congreso en la elaboración de la Estrategia de Seguridad Nacional.

[44] De conformidad con la Ley Goldwater-Nichols de reorganización del Departamento de Defensa de 1986 (Ley pública 99-433), corresponde al Jefe del Estado Mayor, luego un proceso de consultas con los Comandantes de Combate y los demás miembros del Estado Mayor, emitir la Estrategia Militar Nacional. Este documento "sirve de marco estratégico para la ejecución por parte de las fuerzas armadas de los objetivos políticos generales establecidos en la Estrategia de Seguridad Nacional y la Estrategia de Defensa Nacional más recientes" (Office of the Secretary of Defense, s.f.) [página web].

el capítulo I de la presente investigación.

Asimismo, Ney Jr. (2020) señala que toda respuesta a un ciberataque debe ser consistente con las normas que corresponden, para lo cual primero se hace un análisis de la normativa nacional y luego un análisis de la normativa internacional que corresponda [página web]. Respecto de las normas del derecho internacional, se analiza si el ciberataque ha vulnerado la prohibición del uso de la fuerza, estipulada en el art. 2.4 de la Carta de la ONU, y por lo tanto habilita al uso del derecho a la legítima defensa, en tanto cumpla con los principios de necesidad y proporcionalidad (Ney Jr., 2020). De igual manera, el Departamento de Defensa de los Estados Unidos reconoce que lo siguiente:

> Incluso si el derecho de la guerra no se aplica técnicamente porque la ciberoperación militar propuesta no se llevaría a cabo en el contexto de un conflicto armado, el Departamento de Defensa aplica los principios de este. Esto significa que los principios de *ius in bello*, como la necesidad militar, la proporcionalidad y la distinción, continúan guiando la planificación y ejecución de ciberoperaciones militares, incluso fuera del contexto de un conflicto armado. (Ney Jr., 2020) [Página web]

En resumen, es posible apreciar cómo Estados Unidos guía su respuesta a un ciberataque aplicando la normativa del derecho internacional explicada en el capítulo I de esta investigación. Así las cosas, se pueden extraer las siguientes conclusiones:

- Se parte del reconocimiento de que el ciberespacio es un entorno en constante cambio, por lo cual la normativa debe adecuarse a estos.
- Se define de modo preciso las conductas que califican como una amenaza híbrida en el ciberespacio, pero no es una lista *númerus*

clausus, sino abierta, por lo que cualquier conducta que afecte la infraestructura crítica o las capacidades del Estado podrá ser considerada como tal.

- Se realiza un análisis respecto de la atribución de los ciberataques, aplicando para ello las normas de responsabilidad estatal que corresponden.
- Para responder a estos, se analiza la normativa nacional e internacional a fin de dar una respuesta articulada a los ciberataques.

Rusia:

Tal y como se comentó en el primer capítulo de esta investigación, uno de los ideólogos del concepto de amenazas híbridas es el general ruso Valery Gerasimov, Jefe del Estado Mayor del ejército ruso, quien formuló la idea de la "guerra sin límites" en los siguientes términos:

> Las guerras ya no se declaran ni se ganan o pierden, sino que, en este estado de guerra constante, es necesario utilizar medios no militares para alcanzar objetivos políticos y estratégicos en modo más eficaz que con el tradicional uso de la fuerza armada. Desde esta lógica, los Estados deben encontrar y explotar en todo momento las vulnerabilidades de los adversarios en todos los ámbitos sociales. (Payá & Luque, 2018, p. 24)

Así, para Gerasimov, las guerras sin límites tienen algunas características a detallar que las convierten en verdaderos conflictos híbridos (Payá & Luque, 2018, p. 25):

- No es necesaria una declaración de guerra para realizar acciones militares, sino que éstas se pueden realizar en un periodo de paz.

- La neutralización de las capacidades militares del oponente no se realiza únicamente por medios militares, sino que también se hace a través de ataques quirúrgicos, tales como los ciberataques, dirigidos contra la infraestructura crítica que sustenta dichas capacidades militares.
- Se usan nuevas armas de precisión, operaciones especiales y nuevas tecnologías.
- Se aprovecha a los civiles, con el objetivo de distorsionar la atribución de las acciones a un Estado.

Si bien es cierto que Gerasimov cita otras características, bastan las antes señaladas para poder afirmar que la nueva forma de conflictos se trata sin duda de una guerra híbrida. Este tipo de guerra se justifica porque, tal como señala la Estrategia de Seguridad Nacional rusa[45] (citada por Duclos, 2021) [página web], Rusia se enfrenta a una serie de países no aliados que buscan desestabilizar su sistema político. Es en este contexto que los ciberataques resultan muy atractivos para Rusia, en tanto permiten una respuesta más rápida a las amenazas y dificultan el grado de atribución para este país (Wolff, 2021) [página web].

Por lo tanto, la normativa en materia de ciberdefensa rusa prevé al ciberespacio como una continuación del espacio físico y, por ello, cualquier ataque dirigido contra esta se tomará como una violación a la soberanía rusa, y una violación al principio de no intervención (Hakala & Melnychuk, 2021, p. 7). Es así como se justifica la legítima defensa contra cualquier amenaza a la soberanía rusa, sin que ello escale a un conflicto de mayor envergadura (Hakala & Melnychuk, p. 9).

Pero, además, Janne Hakala y Jazlyn Melnychuk (2021) señalan que la

[45] Este documento fue aprobado por el presidente Vladimir Putin mediante Decreto Presidencial No. 400, del 2 de julio de 2021.

estrategia militar rusa contempla el uso de ciberataques como una medida de disuasión estratégica, ya que con estos se busca “lograr efectos estratégicos y ganar superioridad sobre los oponentes” (p. 10) [traducción propia]. En esta línea, los ciberataques desempeñan “un papel esencial en la compensación de la fuerza convencional, ya que permiten deshabilitar la infraestructura civil crítica, como la energía, el transporte y las capacidades C2 (Comando y Control), debilitando drásticamente las capacidades de guerra de un adversario” (Hakala & Melnychuk, 2021, p. 10) [traducción propia]. Además, se prevén una serie de mecanismo que “incluyen (…) el fortalecimiento de las salvaguardias contra los ciberataques, el desarrollo sistemático de tecnologías nacionales y, de manera más general, el establecimiento de las ‘fuerzas y medios de confrontación de la información’”(Duclos, 2021) [traducción propia] [página web].

Así, podemos extraer una serie de conclusiones de la lectura de las normas rusas en materia de ciberdefensa:

- Existe una conceptualización bastante precisa de lo que debe entenderse como amenaza híbrida, conflicto híbrido y guerra híbrida, a partir de la doctrina de la guerra sin límites propuesta por Valery Gerasimov.
- Un ciberataque se conceptualiza como una violación a la soberanía rusa, y por tanto faculta al derecho a la legítima defensa, en línea con lo señalado por el art. 51 de la Carta ONU.
- Como parte del concepto de disuasión estratégica, se adoptan diversos mecanismos de ciberdefensa con el objetivo de reducir la vulnerabilidad rusa a las ciberamenazas de otros Estados.

China:

La Estrategia Militar China[46] (2015) reconoce lo siguiente:

> China, como un gran país en vías de desarrollo, todavía enfrenta múltiples y complejas amenazas a su seguridad (…). Las preocupaciones de seguridad de subsistencia y desarrollo, así como las amenazas de seguridad tradicionales y no tradicionales están entrelazadas. Por lo tanto, China tiene una ardua tarea para salvaguardar sus intereses de unificación nacional, integridad territorial y desarrollo. [Página web] [Traducción propia]

Sin embargo, estas preocupaciones no son nuevas para la República Popular China. Es por ello por lo que, en 1999, los coroneles chinos Qiao Liang y Wang Xiangsui publicaron el libro "Guerra sin restricciones". En este texto, sostienen la tesis de que la guerra ha sufrido una metamorfosis, engendrándose una semi-guerra o cuasi-guerra, en la que la violencia militar (método tradicional) ha sido sustituida por otros tipos de violencia, como la política, económica o tecnológica (métodos no tradicionales) (Liang & Xiangsui, 1999, p. 4). En esta línea, también ha cambiado el objetivo mismo de las guerras, pues ya no se trata de usar la fuerza para someter al adversario, sino de usar "usar todos los medios, incluida la fuerza de las armas y los sistemas ofensivos militares y no militares, letales y no letales, para obligar al enemigo a aceptar nuestros propios intereses" (Payá & Luque, 2018, p. 20).

Liang y Xiangsui parten de la premisa de que, debido al desigual desarrollo tecnológico y económico, las guerras son peleadas por actores asimétricos, y por tanto, la lógica de la guerra se modifica (Payá & Luque, 2018,

[46] Este documento fue aprobado a través de un Libro Blanco emitido por el Consejo de Estado de la República Popular China en mayo del 2015.

p. 21). Así, “la estrategia de la guerra sin límites requiere (…) de una combinación estratégica de terrorismo, manipulación de los medios de comunicación, ataques a sitios web, manipulación de las bolsas bursátiles para causar crisis financieras, difusión de virus informáticos y otras armas no convencionales” (Payá & Luque, 2018, p. 21). En esta línea, y en opinión de Manuel de Pablo (2015):

> La Guerra Irrestricta se puede comprender como una guerra combinada que trasciende las principales áreas y métodos de los asuntos militares y no militares, donde se deben incluir todas las dimensiones que ejercen influencia sobre la seguridad nacional y donde se persigue un objetivo político por medio del ejercicio de la violencia en un sentido amplio. (p. 4)

Es así se puede afirmar que la doctrina de la guerra irrestricta no es otra cosa que una denominación diferente de una guerra híbrida, en el sentido explicado en el marco teórico de esta investigación. Y ello se encuentra plasmado en la Estrategia Militar China (2015), que señala lo siguiente:

> En respuesta al nuevo requisito de salvaguardar la seguridad nacional y los intereses de desarrollo, las fuerzas armadas de China trabajarán más intensamente para crear una postura estratégica favorable con mayor énfasis en el empleo de fuerzas y medios militares, y brindarán una sólida garantía de seguridad para el desarrollo pacífico del país. [Página web] [Traducción propia]

Además, esta estrategia contempla la posibilidad de que China sea vulnerable en el ciberespacio, por lo que “acelerará el desarrollo de una fuerza

cibernética y mejorará sus capacidades de conocimiento de la situación del ciberespacio, ciberdefensa, apoyo a los esfuerzos del país en el ciberespacio y participación en la cooperación cibernética internacional" (Estrategia Militar China, 2015) [página web] [traducción propia]. Por lo tanto, esta estrategia contempla la opción de emplear ciberataques como un elemento válido de la guerra irrestricta. Pero, además, contempla la guerra híbrida, empleando medios cibernéticos, como una alternativa viable para la protección de la seguridad china.

En opinión de José Mancera (2014), este documento tiene se siguiente objetivo:

> Defiende los propios intereses, amplía zonas de influencia, se apropia de información o activos informáticos, interrumpe, bloquea o impide el uso del recurso informático y el ciberespacio al enemigo para, en el mejor de los escenarios, obligar al contrincante a aceptar los propios intereses. (Mancera, 2014, p. 92)

Es por ello por lo que el Ejército de Liberación Popular de China aprobó la Estrategia General de la Guerra de Información (INEW, por sus siglas en inglés). Esta estrategia consolida la utilización de medios de ciberataque y ciberdefensa con el objetivo de "desarrollar una arquitectura completamente en red capaz de coordinar operaciones militares en tierra, aire, mar, espacio y en todo el espectro electromagnético" (Sharma, 2010, p. 37).

Sin embargo, tal y como analizó Greg Austin (2018), a pesar de la fuerte inversión del gobierno chino, los cimientos de la ciberdefensa son bastante débiles [página web]. Ello se debe a que este país no cuenta propiamente con normas de ciberdefensa, sino más bien de ciberseguridad. No obstante, Zhang (2012) señala que China aboga por un uso pacífico del ciberespacio, y tiene una

política de no emplear ciberarmas contra civiles (p. 807). Además, este autor afirma que China considera que las normas de la Carta ONU, así como el DIH, en especial los principios de distinción y proporcionalidad, resultan aplicables a todas las operaciones cibernéticas (Zhang, 2012, p. 808).

Así, es posible extraer dos lecciones valiosas de la regulación china respecto de las guerras híbridas:

- La doctrina de la guerra irrestricta provee un contenido respecto de qué debe entenderse como guerra híbrida. Por lo tanto, de la revisión de la Estrategia Militar de China, se desprende que existe una conceptualización que permite entender que las amenazas híbridas también pueden ocurrir en el ciberespacio.
- Si bien es cierto que China no cuenta con un marco normativo específico, de la investigación realizada se ha ubicado autores que consideran que, para China, las normas de *ius in bello* y *ius ad bellum* resultan aplicables para responder a las amenazas híbridas en el ciberespacio.

OTAN:

La OTAN es la organización que más ha desarrollado el concepto de amenazas híbridas. Sin embargo, tal y como se señaló en el capítulo I de esta investigación, y en línea con lo explicado por Payá y Luque (2018), esta organización reconoce que no se trata de un fenómeno nuevo, sino que han sido utilizados desde hace mucho tiempo para desestabilizar al adversario.

Ahora bien, la novedad respecto de las amenazas híbridas radica en la velocidad, la escala y la intensidad, así como en los escenarios en los cuales se materializan. Ejemplos de ello son el ciberataque sufrido por Estonia, y las acciones rusas para tomar el control de la península de Crimea (ver Lasconjarias & Larsen, 2015). Es por ello por lo que Lasconjarias y Larsen (2015) las definen

como el “mayor nivel de mezcla entre las formas de conflicto convencionales y no convencionales, que se caracterizan por la agilidad y la adaptación -por ejemplo, a través de medios tecnológicos- en un intento de lograr efectos decisivos tanto en el campo de batalla físico como en el psicológico” (p. 1-2) [traducción propia].

Esta definición ha sido adoptada por la OTAN en sus múltiples documentos, y, según Lasconjarias y Larsen (2015), de ella se desprenden 3 características fundamentales:

- No hay una distinción entre lo militar y lo civil, por lo que cabe la posibilidad de aplicar métodos y medios tradicionalmente no militares, como la tecnología.
- Debido a esta distorsión entre lo militar y lo civil, cabe la posibilidad de que los actores que perpetran estas amenazas sean tanto estatales como no estatales.
- El espacio sobre el cual se materializan no es necesariamente físico.

Es aquí donde cobra importancia el tema del ciberespacio, ya que la OTAN reconoce abiertamente que es uno de los posibles escenarios sobre el cual se pueden desplegar las amenazas híbridas. Ello a raíz del ciberataque sufrido por Estonia. Es por ello que, en octubre de 2008, se inauguró el CCDCOE, que tiene como objetivo “apoyar a nuestros países miembros y a la OTAN con una experiencia interdisciplinaria única en el campo de la investigación, la formación y los ejercicios de ciberdefensa que abarcan las áreas de enfoque de la tecnología, la estrategia, las operaciones y el derecho” (NATO Cooperative Cyber Defence Centre of Excellence, s.f.) [página web].

Es el CCDCOE en donde se desarrollan las principales respuestas contra las amenazas híbridas que se gestan desde el ciberespacio. Así, se elaboró el Manual de Tallinn 2.0, que ha sido desarrollado extensamente en el capítulo I de

la presente investigación. Este manual contempla la aplicación tanto del *ius in bello* como del *ius ad bellum* a la respuesta ante ciberataques. Pero, además, ha realizado diferentes ejercicios militares con sus miembros, para asegurar la correcta aplicación de estas normas, como por ejemplo el ejercicio *Locked Shields* (NATO Cooperative Cyber Defence Centre of Excellence, s.f.) [página web].

Asimismo, en octubre de 2017 se inauguró el "Centro de Excelencia Europeo para Contrarrestar Amenazas Híbridas" (Hybrid COE), que funciona como un foro de intercambio de experiencias en el que participan tanto miembros de la Alianza Atlántica como de la Unión Europea, que asiste a los países para mejorar sus capacidades cívico-militares para contrarrestar amenazas híbridas (European Centre of Excellence for Countering Hybrid Threats, s.f.) [página web]. Este centro reconoce que el ciberespacio es, hoy por hoy, el principal dominio sobre el cual ocurren las amenazas híbridas, ya que "proporciona un nuevo mecanismo de entrega que puede aumentar la velocidad, la difusión y la potencia de un ataque, y garantizar el anonimato y la indetectabilidad" (Giannopoulos et al., 2020, p. 28) [traducción propia].

Ante ello, el Hybrid COE aprobó la creación de la Comunidad de Interés en Estrategia y Defensa, que tiene como objetivo brindar una visión holística al responder a las amenazas híbridas. Esto significa que no sólo se aplican respuestas militares, sino que más bien se busca que éstas den cumplimiento a las normas del derecho internacional que correspondan (European Centre of Excellence for Countering Hybrid Threats, s.f.-a).

En conclusión, se pueden extraer los siguientes puntos:

- Se define de modo muy preciso el concepto de amenazas híbridas, incorporando el ciberespacio como un dominio sobre el cual se materializan.
- Se reconoce a los ciberataques como un medio no convencional de

ejercicio de las amenazas híbridas.

- Se contempla la aplicación de las normas de *ius ad bellum* y *ius in bello* ante la ocurrencia de ciberataques.

Unión Europea:

La Unión Europea tiene una aproximación más comprehensiva de las amenazas híbridas, tal y como se observó en las definiciones brindadas en el Capítulo I de la presente investigación (ver Comisión Europea, 2016; Pawlak, 2015). Ello responde al hecho de que "la diversidad de las ciberamenazas ha aumentado a lo largo del tiempo, pasando a abarcar desde el ciberconflicto o la guerra cibernética directos hasta el sabotaje y espionaje en el ciberespacio" (Latici, 2021, p. 1). Asimismo, el Consejo de la Unión Europea (2022) considera lo siguiente:

> Las *dinámicas de inestabilidad a escala local y regional*, fruto de contiendas y disfunciones de la gobernanza en nuestra vecindad en sentido amplio y fuera de ella, y alimentadas a veces por las desigualdades y las tensiones religiosas y étnicas, están cada vez más *entremezcladas con amenazas no convencionales* y transnacionales y con rivalidades entre potencias geopolíticas. (p. 7) [énfasis añadido]

Es así como la Unión Europea reconoce la existencia de nuevas amenazas que pueden provenir desde el ciberespacio, llegando a considerarlo incluso como "el quinto ámbito bélico junto con el mar, la tierra, el aire y el espacio" (Latici, 2021, p. 1). En este sentido, Tania Latici (2021) considera que "los ciberataques coordinados, junto con la presión económica, la desinformación y la guerra armada, están poniendo a prueba la resiliencia de los Estados e instituciones democráticos, y suponen un ataque directo a la paz y la seguridad"

(p. 1).

Es por ello por lo que el Consejo de la Unión Europea (2018) considera que “para responder a los retos cambiantes en el ámbito de la seguridad, la UE y sus Estados miembros deben reforzar la ciberresiliencia y desarrollar capacidades sólidas en ciberseguridad y defensa” (p. 2). En esta línea, el Consejo de la Unión Europea ha elaborado un marco normativo bastante robusto, compuesto principalmente por dos documentos: el Marco Político de Ciberdefensa y la Brújula Estratégica para la Seguridad y la Defensa.

El primer documento, el Marco Político de Ciberdefensa de la Unión Europea fue aprobado y actualizado por el Consejo de la Unión Europea en el 2018, mediante Documento del Consejo No. 14413/18. Parte de la concepción de que las ciberamenazas ahora incluyen nuevos tipos de actuaciones, por lo que el término ciberataque “cubre todo tipo de cibercrimen, desde desfigurar un sitio web hasta afectar campañas electorales” (Latici, 2020, p. 3) [traducción propia]. Además, hace una distinción muy clara entre ciberseguridad y ciberdefensa, en los siguientes términos:

> La ciberseguridad se refiere principalmente a actividades civiles relacionadas con la seguridad de la información y de las redes, mientras que la ciberdefensa tiende a referirse al ámbito militar, incluida la protección de activos clave. (Latici, 2021, p. 1)

Asimismo, el Marco Político de Ciberdefensa señala tres principios fundamentales que se describen a continuación:

> La UE promueve (…) un marco estratégico para la prevención de conflictos, la cooperación y la estabilidad en el ciberespacio, que incluye (i) la aplicación del Derecho internacional, y en particular la Carta de las

> Naciones Unidas en su totalidad, en el ámbito del ciberespacio; (ii) el respeto de normas, reglas y principios universales y no vinculantes de comportamiento responsable de los Estados; (iii) el desarrollo y la aplicación de medidas regionales de fomento de la confianza. (Consejo de la Unión Europea, 2018, p. 8)

En este sentido reconoce que la ciberdefensa debe partir de las normas del derecho internacional, en especial la Carta de la ONU, y el respeto por los principios del derecho internacional. Por lo tanto, es posible afirmar que, a pesar de no mencionarlo expresamente, el Marco Político de Ciberdefensa reconoce la aplicación del *ius ad bellum*, al referirse a las normas de la Carta del a ONU, y el ius in bello, en tanto resulten aplicables.

Esto se confirma al revisar el segundo documento: la Brújula Estratégica para la Seguridad y la Defensa, que fue aprobada el 21 de marzo de 2022 por el Consejo de la Unión Europea, a través del Documento del Consejo No. 7371/22. Este documento reconoce expresamente la existencia de amenazas híbridas, y resalta la importancia de continuar desarrollando la política de ciberdefensa como parte del combate ante las amenazas híbridas. En esta línea, señala el compromiso de la UE por "promover e impulsar la seguridad humana, el respeto y el cumplimiento del Derecho internacional humanitario" (Consejo de la Unión Europea, 2022, p. 16). Asimismo, reconoce la necesidad de continuar desarrollando un marco de protección en materia de ciberdefensa, a través del fortalecimiento de las normas existentes y las asociaciones estratégicas con la OTAN y la ONU (Consejo de la Unión Europea, 2022, pp. 22–23).

En este sentido, se puede observar una estrategia articulada y estructurada por parte de la UE para hacer frente a las amenazas híbridas en el ciberespacio, de la cual se puede extraer las siguientes conclusiones:

- Existe una definición precisa de amenazas híbridas y ciberataques, que

parte del reconocimiento de las amenazas que enfrenta la UE a su seguridad.

- Hace una distinción muy clara entre ciberseguridad y ciberdefensa, y como parte de esta última, reconoce la necesidad de proteger la infraestructura crítica.
- Reconoce expresamente la necesidad de aplicar normas del derecho internacional, haciendo referencia a la Carta de la ONU, por lo que resulta de aplicación las normas de *ius ad bellum*, y también del *ius in bello*, para responder a un ciberataque en el contexto de una amenaza híbrida.

PROPUESTAS DE POLÍTICA EXTERIOR PARA EL MINISTERIO DE RELACIONES EXTERIORES:

Vistas las experiencias internacionales, queda claro que países como Estados Unidos, China y Rusia están tomando una posición respecto de las amenazas híbridas en el ciberespacio. En estos países no sólo han desarrollado documentos respecto de esta materia, sino que también se han desarrollado corrientes de pensamiento que teorizan al respecto. De manera similar, resultaría importante que el Perú también se posicione dentro de esta conversación a nivel multilateral, tomando una política exterior clara y conforme al derecho internacional. Además, esto colocaría al Perú en una situación de avanzada frente al resto de países latinoamericanos, que tal y como comentó Alencastro en entrevista para esta tesis, no han desarrollado una normativa robusta ni tampoco han expresado una posición.

Además, se ha visto que organizaciones internacionales como la OTAN y la UE ya han desarrollado distintos tipos de normas y documentos sobre las amenazas híbridas en el ciberespacio. Y, como se ha indicado previamente, la ONU también ha impulsado, aunque tangencialmente, este debate a través del

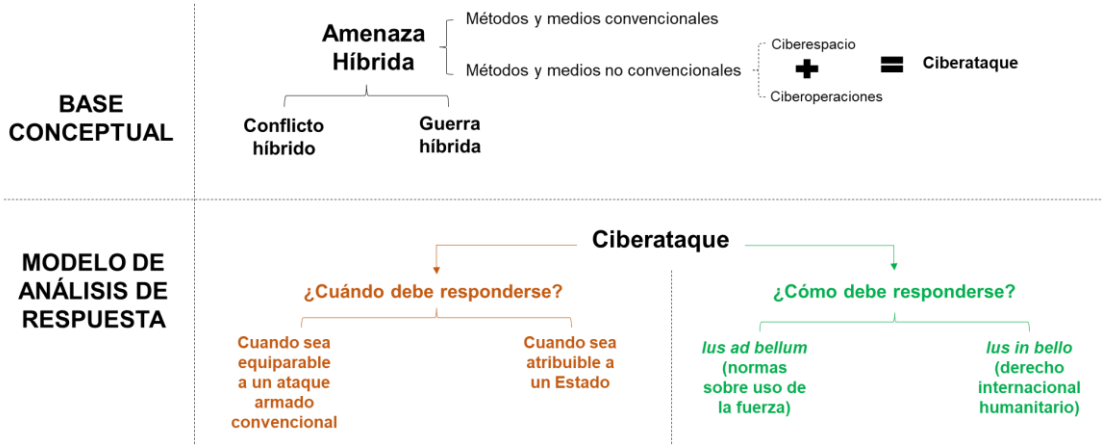
OEWG y el GGE. Para el Perú resultaría muy importante poder ser parte de este debate, para lo cual se requiere una posición fundamentada en el derecho internacional que permita a nuestro país pronunciarse en estos foros. Además, al ser el primer país latinoamericano en expresar una posición, es posible que esto coloque al Perú en una situación de ventaja, y le permita liderar el bloque de países latinoamericanos en los diferentes foros multilaterales.

Pero, además, tomando en consideración que cancillería cumple un rol fundamental de asesoramiento dentro del Consejo de Seguridad Nacional, es importante que este ministerio pueda ser parte del diálogo respecto de la necesidad de establecer normas de ciberdefensa. Así las cosas, Cancillería también podría aportar en el ámbito de sus competencias en la elaboración del Reglamento de la Ley 30999, que se encuentra actualmente en preparación.

Sin embargo, creemos que no sería posible ejercer este rol de asesoramiento sin que antes cancillería haya tomado una posición al respecto. En este sentido, resulta importante, en línea con lo señalado por Alencastro en la entrevista realizada para la presente investigación, que la posición adoptada por Cancillería parta de la definición de los conceptos clave, para luego pronunciarse respecto la aplicación de los marcos normativos necesarios para responder a las amenazas híbridas desde el ciberespacio.

Así las cosas, se propone que Cancillería adopte una política exterior acorde con el siguiente modelo conceptual, que luego podrá ser propuesto también como parte del Reglamento de la Ley 30999:

Figura 1: Modelo conceptual resumido para responder a las amenazas híbridas desde el ciberespacio, en aplicación de las normas de *ius ad bellum* y *ius in bello*



Fuente: Elaboración propia

Base Conceptual:

En primer lugar, debería observarse de las experiencias internacionales, que existen conceptos como ciberataque, ciberoperación y ciberdefensa que están definidos de una forma lo más completa posible, lo cual posibilita una comprensión mayor de cuáles son las normas que corresponde aplicar. Sin embargo, estos conceptos, tal y como se aprecia de las experiencias internacionales, se fundan en la existencia de amenazas a la seguridad y la soberanía de los Estados.

Por ello, resulta importante que la posición de Cancillería se funde en la existencia de estas amenazas, que son híbridas en su génesis, y contemple las siguientes definiciones:

- Amenaza híbrida: Son acciones que implican la amenaza o recurso a la violencia, combinando métodos y medios tradicionales (fuerza militar) y no tradicionales (tecnológicos, diplomáticos, económicos, etc.), perpetradas por actores estatales o no estatales, dirigidas contra un Estado o su población, y con el objetivo de explorar sus vulnerabilidades sistémicas.
- Conflicto híbrido: Son amenazas híbridas que comprenden acciones equivalentes al uso de la fuerza, más no en un contexto de conflicto

armado.

- Guerra híbrida: Son amenazas híbridas que tienen lugar en el contexto de un conflicto armado.

Adicionalmente, es importante que Cancillería formule otros conceptos claros como parte de su posición. En este sentido, y en línea con lo señalado en el capítulo I de esta investigación, el primer concepto a definir es el de ciberespacio, el que se recomienda definir en los mismos términos que el Departamento de Defensa de los Estados Unidos (Departamento de Defensa, 2021a), como un "dominio global dentro del entorno de la información, que consiste en redes interdependientes de infraestructuras para la tecnología de la información y data residente, incluyendo la internet, las redes de telecomunicación, sistemas de computadora, y procesadores y controladores integrados" [traducción propia].

Asimismo, se recomienda definir a las ciberoperaciones, en línea con lo señalado por el Departamento de Defensa de los Estados Unidos (Departamento de Defensa, 2021c), como "el uso de capacidades en el ciberespacio con el objetivo principal de alcanzar objetivos en, o por medio del, ciberespacio" [traducción propia].

Finalmente, se recomienda definir a los ciberataques como acciones que implican la amenaza o recurso a la violencia, usando como medio no tradicional el ciberespacio y método no tradicional las ciberoperaciones, y que tiene por objetivo vulnerar la infraestructura tecnológica y digital de un Estado, afectando así tanto al gobierno como a la población. A partir de estas definiciones, será posible que los Estados puedan plasmar las distintas respuestas a estos, y decidir cuáles son los marcos jurídicos aplicables.

Modelo de Análisis de Respuesta:

Antes de iniciar el análisis respecto del modelo de respuesta, es importante recordar que el art. 98.3 del D.S. 029-2021-PCM señala lo siguiente:

> La Presidencia del Consejo de Ministros, en su calidad de miembro del Consejo de Seguridad y Defensa Nacional, establece los protocolos de escalamiento, coordinación, intercambio y activación para lo indicado en la Ley Nº 30999, Ley de Ciberdefensa. Esta función se ejerce a través de la Secretaría de Gobierno Digital en su calidad de ente rector del Sistema Nacional de Transformación Digital y de seguridad y confianza digital en el país, quien emite los lineamientos y las directivas correspondientes. (D.S. 029-2021-PCM, 2021)

En resumen, corresponde a la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, determinar la activación de todos los mecanismos de la Ley 30999. Por lo tanto, será esta entidad quien realice el primer nivel de análisis. Sin embargo, también es importante que Cancillería tome una posición debido a que, tal y como se señaló anteriormente, cumple con un rol de asesoramiento en el Consejo de Defensa Nacional, el cual también integra la Presidencia del Consejo de Ministros, y, por lo tanto, podría aportar en el análisis que realice esta entidad.

Así las cosas, en el primer nivel de análisis, tal y como se explicó en el marco teórico de la presente investigación, corresponde determinar si el ciberataque amerita la aplicación de las normas del derecho internacional que corresponda. En primer lugar, el ciberataque debe equipararse a un ataque armado, para lo cual deben analizarse dos condiciones en conjunto:

- Que el ciberataque haya sido lo suficientemente severo, es decir, que haya daños, destrucción, heridos o muertos.

- Que el ciberataque cumpla con el criterio de causalidad próxima, para lo cual debe verificarse:
    - La inmediatez del ataque, lo que implica que sus consecuencias ocurran de inmediato o dentro de un plazo muy breve de tiempo.
    - El nexo causal, o que el ciberataque produzca las consecuencias esperadas del mismo.
    - Que exista un alto grado de intromisión en la inviolabilidad territorial de otro Estado.
    - Que tenga consecuencias cuantificables.
    - Que sea realizado como parte de una operación militar.
    - Que se dirija contra un objetivo militar u otros que resulten fundamentales para la prestación de servicios públicos esenciales.

En segundo lugar, tal y como se explicó en el capítulo I de esta investigación, se debe determinar que ciberataque debe ser atribuible a un Estado, en aplicación de las siguientes normas del derecho internacional:

- Que sea perpetrado por un órgano o agentes estatales.
- Que sea perpetrado por un privado que cuenta con autorización del Estado para ejercer funciones gubernamentales, otorgada conforme al Derecho interno.
- Que sea perpetrado por un privado que lo realiza por instrucción de un Estado, o cuyos actos se encuentran bajo dirección y control general de dicho Estado.
- Que sea perpetrado por un privado, cuyos actos sean reconocidos posteriormente y adoptados como propios por un Estado.
- Que sea perpetrado por órganos que un Estado puso a disposición de otro.

- Que sea perpetrado por movimientos insurreccionales que luego se convierten en el gobierno oficial de un Estado.

Una vez que se ha superado el primer nivel de análisis, corresponde entonces determinar el marco normativo aplicable para responder a los ciberataques en el contexto de una amenaza híbrida. En opinión de Alencastro, en entrevista para esta investigación, no resulta necesario que el Estado Peruano asuma nuevos compromisos, sino que aplique las normas ya vigentes de *ius ad bellum* y *ius in bello*. Ello resulta sumamente importante para articular una posición desde Cancillería.

Así las cosas, el *ius ad bellum* aplicará cuando el ciberataque sea parte de un conflicto híbrido, esto es, cuando ocurra en tiempos de paz. Así las cosas, la política exterior del Perú puede contemplar las siguientes posibilidades respecto del uso de la fuerza en materia de defensa contra amenazas híbridas en el ciberespacio:

- Que sea considere al ciberataque en el contexto de un conflicto híbrido como un uso de la fuerza prohibido, en virtud del art. 2.4 de la Carta de la ONU, por lo que el Estado Peruano queda expedito para solicitar la intervención del Consejo de Seguridad de la ONU, siendo Cancillería la entidad encargada de representar al Perú en este foro, de conformidad con el art. 5 de la Ley 29357, Ley de Organización y Funciones del Ministerio de Relaciones Exteriores, y el art. 3 del ROF, el cual fue aprobado por el D. S. 135-2010-RE.
- Que, ante un ciberataque en el contexto de un conflicto híbrido, el Estado Peruano ejerza su derecho a la legítima defensa, activando los mecanismos de la Ley 30999, ya sea a través de un ciberataque o cualquier otro medio, en tanto se cumpla con los siguientes requisitos:
    - Proporcionalidad, lo que significa que una acción en legítima defensa debe causar daños en proporción razonable a los

ocasionados por el ciberataque inicial.

- Necesidad, esto es, que la acción en legítima defensa, sea militar o no, responda a un ciberataque previo.
- Inmediatez, para lo cual el Manual de Tallinn 2.0 requiere que se analicen la proximidad temporal entre el ataque y la respuesta, el tiempo necesario para identificar al atacante, y el tiempo necesario para preparar la respuesta.

Respecto del *ius in bello*, el teniente FAP Kenny Meza señala que rige al uso de la fuerza cuando se presente una amenaza o exista un ataque inminente desde el ciberespacio, que ponga en riesgo la soberanía, los intereses nacionales, los activos críticos nacionales y recursos claves para mantener las capacidades nacionales. Sin embargo, de la revisión del tratamiento que dan otros Estados a las amenazas híbridas desde el ciberespacio, consideramos que una política exterior en esta materia debería contemplar que, si bien las normas específicas aplican únicamente en tiempos de guerra, esto es, cuando existen guerras híbridas, también es importante que, como mínimo, los principios de esta rama del derecho se apliquen incluso en tiempos de paz, siguiendo el ejemplo de los Estados Unidos.

Así las cosas, y en línea con lo señalado por Alencastro en la entrevista para la presente investigación, los principios explicados en el Dec. Leg. 1095 sobre el uso de la fuerza cinética deben aplicar *mutatis mutandis* a las ciberoperaciones. Por lo tanto, la política exterior en materia de amenazas híbridas en el ciberespacio debería contemplar la aplicación de los siguientes principios:

- Humanidad, que, en línea con lo señalado por Salmón, consiste en que se trate tanto a los combatientes como a los no combatientes con humanidad, evitando los sufrimientos innecesarios.

- Distinción, que implica que los ciberataques no pueden ser dirigidos contra población civil, o activos civiles que no sean utilizados con fines militares.
- Limitación, que implica que la elección de medios para realizar un ciberataque no puede ser ilimitada, sino que deben escogerse aquellos métodos y medios que resulten menos lesivos en atención al principio de humanidad.
- Necesidad militar, que implica que sólo podrán realizarse ciberataques que resulten estrictamente necesarios para debilitar el potencial bélico del contendor, evitando generar daños superfluos o innecesarios.
- Proporcionalidad, que implica que el ciberataque realizado no sea desproporcionado respecto de la ventaja militar que se busca obtener. En este sentido, estarán prohibidos los ciberataques que causen daños superfluos, innecesarios o indiscriminados.

CONCLUSIONES

1. El objetivo general de esta tesis fue brindar aportes para el diseño de los lineamientos de la política exterior peruana en materia de amenazas híbridas en el ciberespacio. Ello debido a que el desarrollo tecnológico ha generado nuevas formas de conflictividad, así como nuevas amenazas a la seguridad de los Estados. Tal y como se aprecia de las recomendaciones brindadas en el Capítulo III, este objetivo se cumplió por las razones que se explicarán a continuación. Sin embargo, para cumplirlo, fue necesario que esta investigación se plantee tres objetivos específicos, que se explican a continuación.

2. Para poder cumplir con el objetivo general, esta tesis se plantó como primer objetivo específico definir qué debe entenderse por amenaza híbrida en el ciberespacio. Este objetivo se cumplió, ya que de la doctrina revisada se determinó que las amenazas híbridas se definen como acciones que implican la amenaza o recurso a la violencia, combinando métodos y medios tradicionales (fuerza militar) y no tradicionales (tecnológicos, diplomáticos, económicos, etc.), perpetradas por actores estatales o no estatales, dirigidas contra un Estado o su población, y con el objetivo de explorar sus vulnerabilidades sistémicas.

   Es importante precisar que, dentro de las amenazas híbridas existen dos clases que esta investigación ha comentado en detalle. La primera, el conflicto híbrido, se define como una amenaza híbrida perpetrada usando la fuerza, más no en un contexto de conflicto armado. Por otro lado, la segunda, la guerra híbrida, se define como una amenaza híbrida perpetrada como parte de un conflicto armado.

Asimismo, se determinó que, debido al desarrollo tecnológico, uno de los espacios desde los cuáles se gestan amenazas hacia la seguridad del Estado es el ciberespacio, definido como un entorno tanto físico como digital consistente en infraestructura física, tal como sistemas de computadoras, procesadores y otros hardware, así como las redes de interconexión, es decir la internet y otros sistemas, y la data residente en la misma. En este sentido, las acciones que se gestan desde el ciberespacio, aprovechando sus potencialidades, se denominan como ciberoperaciones.

Finalmente, se determinó que existen muchos tipos de ciberoperaciones que ponen en riesgo la seguridad de los Estados, tales como el ciberespionaje o el cibercrimen. Sin embargo, la más relevante son los ciberataques, pues se trata de amenazas híbridas definidas como acciones que implican la amenaza o recurso a la violencia, usando como medio no tradicional el ciberespacio y método no tradicional las ciberoperaciones, y que tiene por objetivo vulnerar la infraestructura tecnológica y digital de un Estado, afectando así tanto al gobierno como a la población.

3. El segundo objetivo específico fue determinar qué tipo de amenazas híbridas en el ciberespacio debían ser respondidas aplicando normas del derecho internacional. Este objetivo se cumplió ya que, de la revisión de la doctrina se determinó que deberán responderse aquellos ciberataques que cumplan con dos condiciones.

   La primera es que sea equiparable a un ataque armado. Esto significa

que debe cumplirse con dos condiciones:

a. Que el ciberataque haya sido lo suficientemente severo (que haya daños, destrucción, heridos o muertos).
b. Que el ciberataque tenga causalidad próxima, para lo cual debe verificarse:
    i. Que tenga consecuencias que ocurran de inmediato o dentro de un plazo muy breve de tiempo.
    ii. Que produzca las consecuencias esperadas del mismo.
    iii. Que exista un alto grado de intromisión en la inviolabilidad territorial de otro Estado.
    iv. Que tenga consecuencias cuantificables.
    v. Que sea realizado como parte de una operación militar.
    vi. Que se dirija contra un objetivo militar u otros que resulten fundamentales para la prestación de servicios públicos esenciales.

La segunda es que sea atribuible a un Estado, en aplicación de las siguientes normas del derecho internacional:

a. Que sea perpetrado por un órgano o agentes estatales.
b. Que sea perpetrado por un privado que cuenta con autorización del Estado para ejercer funciones gubernamentales, otorgada conforme al Derecho interno.
c. Que sea perpetrado por un privado que lo realiza por instrucción de un Estado, o cuyos actos se encuentran bajo dirección y control general de dicho Estado.
d. Que sea perpetrado por un privado, cuyos actos sean reconocidos posteriormente y adoptados como propios por un Estado.
e. Que sea perpetrado por órganos que un Estado puso a

disposición de otro.

f. Que sea perpetrado por movimientos insurreccionales que luego se convierten en el gobierno oficial de un Estado.

4. El tercer objetivo específico fue determinar cuál es el marco normativo que corresponde aplicar para responder a las amenazas híbridas en el ciberespacio. Este objetivo se cumplió ya que, de la revisión de la doctrina especializada en la materia, se determinó que existen dos posibilidades.

   Una primera posibilidad es aplicar las normas referidas al *ius ad bellum*, es decir el uso de la fuerza prohibido, en aplicación del art. 2.4 de la Carta de la ONU. Para ello, debe observarse que se trate de un ciberataque en el contexto de una amenaza híbrida ocurrido en tiempos de paz, esto es, un conflicto híbrido. Así, el Estado afectado podrá aplicar cualquiera de las dos alternativas:

   a. El ciberataque será considerado como un uso de la fuerza prohibido, en virtud del art. 2.4 de la Carta de la ONU y el Estado agraviado podrá recurrir al Consejo de Seguridad, que debería proceder conforme a lo señalado en el Capítulo VII de la Carta de la ONU.

   b. El Estado agraviado podrá ejercer su derecho a la legítima defensa, en el marco del art. 51 de la Carta de la ONU, ya sea a través de un ciberataque o cualquier otro medio, en tanto este sea proporcional, necesario e inmediato.

La segunda posibilidad es determinar que el ciberataque en el contexto de una amenaza híbrida haya ocurrido como parte de una operación militar en tiempos de CAI o CANI, lo cual constituiría una guerra híbrida. En este sentido, correspondería aplicar los principios del *ius in bello* o DIH, además de las disposiciones del DIDH que correspondan. Así las cosas, los Estados inmersos en una guerra híbrida deberán respetar, como mínimo, los siguientes principios del DIH:

a. Humanidad
b. Distinción
c. Proporcionalidad
d. Necesidad militar
e. Limitación
f. Prohibición de causar daños superfluos o innecesarios

5. Adicional a los objetivos explicados anteriormente, es importante señalar que, para poder contribuir en la elaboración de la política exterior en lo que se refiere a amenazas híbridas en el ciberespacio, fue necesario describir el tratamiento que se brinda actualmente en el Perú, y compararlo con el de otros sujetos del derecho internacional. Así las cosas, la Política Nacional de Seguridad y Defensa Nacional del Estado Peruano, aprobada mediante Decreto Supremo No. 012-2017-DE, se limita a reconocer las amenazas que el Estado Peruano puede sufrir en el ciberespacio, más no desarrolla normas específicas de ciberdefensa. Es recién con la aprobación de la Ley 30999, Ley de Ciberdefensa, que se desarrollan los alcances de la respuesta que debe darse a las amenazas que provengan desde el ciberespacio.

Asimismo, de la revisión de la experiencia comparada de Estados como

Estados Unidos, Rusia y China, así como organizaciones internacionales como la OTAN y la Unión Europea, quedó demostrada la necesidad de establecer definiciones claras que el Perú debería considerar como base fundamental de su política exterior en la materia. Esto refuerza el cumplimiento del primer objetivo específico. Además, tanto la OTAN como los Estados Unidos y la Unión Europea coinciden en que las normas de *ius ad bellum* y *ius in bello* resultan aplicables en la respuesta a los ciberataques, entendidos como amenazas híbridas desde el ciberespacio, lo cual refuerza el cumplimiento del tercer objetivo específico.

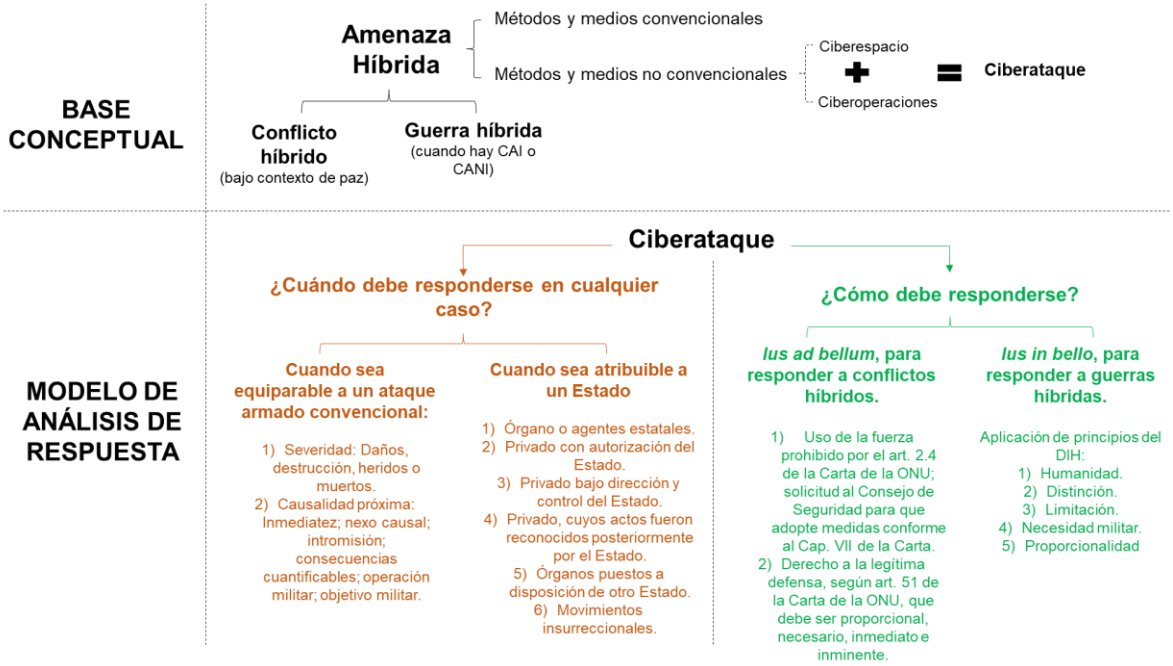
En esta línea, resulta importante que Cancillería tome una posición sobre esta materia, que esté en consonancia con las normas del derecho internacional y permita al Perú mantener una posición de liderazgo en las organizaciones internacionales en las que se discuta el asunto de amenazas híbridas en el ciberespacio. De esta manera, el Perú podría fortalecer su posición en el OEWG, así como participar más activamente en caso este tema se discuta en la Asamblea General de la ONU o, de ser el caso, en el Consejo de Seguridad de la ONU u otros órganos.

Asimismo, adoptar una posición sobre esta materia permitirá que el Perú ejerza de modo más efectivo su rol de asesoramiento al Consejo de Defensa Nacional, y pueda participar de modo activo en el proceso de elaboración del Reglamento de la Ley 30999. Finalmente, podría servir de apoyo para los funcionarios y personal de Cancillería de los órganos competentes y que, por diversos motivos, tengan algún contacto con esta materia.

RECOMENDACIONES

Se recomienda al Ministerio de Relaciones Exteriores incorporar a la política exterior consideraciones respecto de las amenazas híbridas en el ciberespacio que se encuentren en consonancia con el siguiente modelo conceptual:

Figura 2: Modelo conceptual detallado para responder a las amenazas híbridas desde el ciberespacio, en aplicación de las normas de *ius ad bellum* y *ius in bello*



Fuente: Elaboración propia

1. En primer lugar, deberá partir de la definición de conceptos como amenaza híbrida y sus clases (conflicto híbrido y guerra híbrida), así como ciberespacio, ciberoperaciones y ciberataque.
2. Una vez adoptada esta base conceptual, se definirá qué tipo de ciberataques deberán ser respondidos en aplicación del derecho

internacional. Para ello, se analizará si el ciberataque es equiparable a un ataque armado convencional, y si es atribuible a otro Estado.

3. Finalmente, se determinará si corresponde emplear normas del *ius ad bellum* o *ius in bello*, según corresponda.

BIBLIOGRAFÍA

Agencia Peruana de Noticias Andina. (2022, February 17). *Perú sufrió más de 11.5 mil millones de intentos de ciberataques en 2021*. https://andina.pe/agencia/noticia-peru-sufrio-mas-115-mil-millones-intentos-ciberataques-2021-881221.aspx

Ardila Castro, C. A., & Jiménez Reina, J. (Eds.). (2018). *Convergencia de Conceptos: Propuestas de Solución a las Amenazas Actuales para la Seguridad y Defensa de Colombia*. Escuela Superior de Guerra "General Rafael Reyes Prieto"; Centro de Estudios Estratégicos en Seguridad y Defensa Nacionales.

Asamblea General de las Naciones Unidas. (1988). *Resolución 42/22 (1988), Declaración sobre el mejoramiento de la eficacia del principio de la abstención de la amenaza o de la utilización de la fuerza en las relaciones internacionales*. Organización de las Naciones Unidas. https://www.dipublico.org/4073/declaracion-sobre-el-mejoramiento-de-la-eficacia-del-principio-de-la-abstencion-de-la-amenaza-o-de-la-utilizacion-de-la-fuerza-en-las-relaciones-internacionales-resolucion-4222-de-la-asamblea-genera/

Astudillo Salcedo, C. A. (2020). *Un ensayo sobre la seguridad y la defensa en el Perú. Nuevas amenazas, nuevos roles* (2nd ed.).

Austin, G. (2018, July 1). *How Good Are China's Cyber Defenses?* . The Diplomat; University of Chicago Press. https://doi.org/10.1086/697089

Balouziyeh, J., & Burns, J. (2013). Just War Theory: Religious Perspectives and Modern International Law Compared. *Emerging Issues*, *7050*.

Bernales Ballesteros, E. (2012). *La Constitución de 1993: veinte años después* (6th ed.). IDEMSA.

Biden, J. R. (2021). *Interim National Security Strategic Guidance*. The White

House.

Boylan, D. (2018, November 30). *Iran helps Houthis fight Yemen war in cyberspace*. The Washington Times. https://apnews.com/article/383b8c2d35b98a107fe067a563fe0e09

Carta de las Naciones Unidas. (1945).

Cassese, A. (2005). *International Law* (2da ed.). Oxford University Press.

Centro Europeo de Excelencia para Contrarrestar las Amenazas Híbridas. (n.d.). *Hybrid threats as a concept*. Retrieved June 1, 2022, from https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/

Chinkin, C., & Kaldor, M. (2017). *International law and new wars*. Cambridge University Press.

Cisco. (n.d.). *What Is a Firewall?* Retrieved July 10, 2022, from https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html

Texto del proyecto de artículos sobre la responsabilidad del Estado por hechos internacionalmente ilícitos, (2001) (testimony of Comisión de Derecho Internacional).

Comisión de Derecho Internacional. (2022). *Documento No. A/CN.4/L.967, Normas imperativas de derecho internacional general (ius cogens)*.

Comisión Europea. (2016). *Comunicación conjunta sobre la lucha contra las amenazas híbridas, una respuesta de la Unión Europea*. Unión Europea.

Comité de Asuntos Legales y Derechos Humanos. (2018). *Legal challenges related to hybrid war and human rights obligations*.

Comité Internacional de la Cruz Roja. (1977). *Protocolo I adicional a los Convenios de Ginebra de 1949 relativo a la protección de las víctimas de los conflictos armados internacionales*. https://www.icrc.org/es/document/protocolo-i-adicional-convenios-ginebra-1949-proteccion-victimas-conflictos-armados-internacionales-1977

Comité Internacional de la Cruz Roja. (2010, October 29). *Jus ad bellum y jus in bello*. https://www.icrc.org/es/doc/war-and-law/ihl-other-legal-regmies/jus-in-bello-jus-ad-bellum/overview-jus-ad-bellum-jus-in-bello.htm

Conferencia de paz de La Haya de 1899. (1899). *Convención (I) para la solución pacífica de disputas internacionales (La Haya I)*. https://web.archive.org/web/20080503221742/http://www.yale.edu/lawweb/avalon/lawofwar/hague01.htm

Constitución política del Perú, (1993) (testimony of Congreso Constituyente Democrático).

Congreso de la República del Perú. (2009). Ley No. 29357, Ley de Organización y Funciones del Ministerio de Relaciones Exteriores. In *Diario Oficial El Peruano*.

Congreso de la República del Perú. (2019). Ley No. 30999, Ley de Ciberdefensa. In *Diario Oficial El Peruano* (pp. 9–10).

Consejo de la Unión Europea. (2018). Marco político de ciberdefensa de la UE (actualización de 2018). In *Documento del Consejo No. 14413/18*. Consejo de la Unión Europea.

Consejo de la Unión Europea. (2022). Una Brújula Estratégica para la Seguridad y la Defensa – Por una Unión Europea que proteja a sus ciudadanos, defienda sus valores e intereses y contribuya a la paz y la seguridad internacionales. In *Documento del Consejo No. 7371/22*. Consejo de la Unión Europea.

Corte Internacional de Justicia. (1980). Caso relativo al personal diplomático y consular de los Estados Unidos en Teherán. In *Reports of Judgements, Advisory Opinions and Orders*. https://www.icj-cij.org/public/files/case-related/64/064-19800524-JUD-01-00-EN.pdf

Caso relativo a las actividades militares y paramilitares en y contra Nicaragua (Nicaragua contra los Estados Unidos de América) (Fondo del asunto),

(1986). https://www.dipublico.org/cij/doc/79.pdf

Corte Internacional de Justicia. (1996). Legalidad de la amenaza o uso de armas nucleares. In *Reports of Judgements, Advisory Opinions and Orders* (pp. 226–267).

Corte Internacional de Justicia. (1999). *Diferencia relativa a la inmunidad judicial de un Relator Especial de la Comisión de Derechos Humanos*.

Corte Internacional de Justicia. (2007). Caso relativo a la aplicación de la Convención para la Prevención y la Sanción del Delito de Genocidio (Bosnia y Herzegovina vs. Serbia y Montenegro). In *Reports of Judgements, Advisory Opinions and Orders* (pp. 43–240).

Craig, A., & Valeriano, B. (2018). Realism and Cyber Conflict: Security in the digital age. In D. Orsi, J. R. Avgustin, & M. Nurnus (Eds.), *Realism in practice: an appraisal* (pp. 85–101). E-International Relations Publishing.

Crawford, J. (2002). *The International Law Commission's Articles on State Responsability: Introduction, text and commentaries*. Cambridge University Press.

Crawford, J. (2013). *State Responsability: The general part*. Cambridge University Press.

de Pablo, M. (2015). *La guerra irrestricta: ¿un nuevo modo de hacer la guerra?*

Deeks, A. (2013). The Geography of Cyber Conflict: Through a Glass Darkly. *International Law Studies*, *89*, 1–20.

Departamento de Defensa. (2021a). Cyberspace. In *DOD Dictionary of Military and Associated Terms*.

Departamento de Defensa. (2021b). Cyberspace attack. In *DOD Dictionary of Military and Associated Terms, (2021)*.

Departamento de Defensa. (2021c). *Cyberspace Operations*. Departamento de Defensa.

Departamento de Defensa. (2021d). *DOD Dictionary of Military and Associated*

Terms. Departamento de Defensa.

Development Concepts and Doctrine Centre. (n.d.). *Cyber Primer* (2nd ed.). Ministry of Defense.

Duclos, M. (2021, August 2). *Russia's National Security Strategy 2021: the Era of "Information Confrontation."* Institut Montaigne. https://www.institutmontaigne.org/en/analysis/russias-national-security-strategy-2021-era-information-confrontation

European Centre of Excellence for Countering Hybrid Threats. (n.d.-a). *COI Strategy and Defence*. Retrieved October 6, 2022, from https://www.hybridcoe.fi/coi-strategy-and-defence/

European Centre of Excellence for Countering Hybrid Threats. (n.d.-b). *What is Hybrid CoE?* Retrieved October 6, 2022, from https://www.hybridcoe.fi/who-what-and-how/

Fernández, R. (2009, May 30). *Estonia, primera víctima de los "hackers"* . El País. https://elpais.com/diario/2009/05/30/internacional/1243634402_850215.html

Galán, C. (2018). *Amenazas híbridas: nuevas herramientas para viejas aspiraciones* (Documento de Trabajo 20/2018).

Giannopoulos, G., Smith, H., & Theocharidou, M. (2020). *The landscape of hybrid threats: A conceptual model*.

Gray, C. (2018). *International law and the use of force* (4th ed.). Oxford University Press.

Hakala, J., & Melnychuk, J. (2021). *Russia's Strategy in Cyberspace*.

Hathaway, O. A., & Shapiro, S. J. (2017). *The Internationalists: How a radical plan to outlaw war remade the world* (1st ed.). Simon & Schuster.

Hernández, R., Fernández, C., & Baptista, M. del P. (2014). *Metodología de la Investigación*. McGraw Hill Education.

Hoffman, F. G. (2007). Conflicts in the 21st century: The Rise of hybrid wars. In

Potomac Institute for Policy Studies. https://doi.org/10.20542/0131-2227-2019-63-12-56-66

HP. (2021, August 31). *¿Qué es un firewall de red y cómo funciona?* . https://www.hp.com/cl-es/shop/tech-takes/que-es-un-firewall-de-red-y-como-funciona

International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence. (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (M. N. Schmitt, Ed.; 2nd ed.). Cambridge University Press.

Junta de Jefes de Estado Mayor de los Estados Unidos. (2018). *Description of the National Military Strategy 2018*.

Kammerhofer, J. (2018). The US intervention in Nicaragua - 1981-88. In T. Ruys, O. Corten, & A. Hofer (Eds.), *The use of force in international law: A case based approach* (1st ed., pp. 342–360). Oxford University Press.

Kaspersky. (n.d.). *¿Qué es un botnet? - Definición*. Retrieved August 8, 2022, from https://www.kaspersky.es/resource-center/threats/botnet-attacks

Lasconjarias, G., & Larsen, J. A. (2015). Introduction: A new way of warfare. In G. Lasconjarias & J. A. Larsen (Eds.), *NATO's response to hybrid threats*.

Latici, T. (2020). Understanding the EU's approach to cyber diplomacy and cyber defence. In *Documento No. PE 651.937*. Servicio de Estudios del Parlamento Europeo.

Latici, T. (2021). Las capacidades de ciberdefensa de la UE. In *Documento No. PE 698.032*. Servicio de Estudios del Parlamento Europeo.

León Vásquez, J. L. (2013). Art. 44: Deberes fundamentales del Estado. In W. Gutiérrez (Ed.), *La Constitución Comentada* (2nd ed., Vol. 1, pp. 943–952). Gaceta Jurídica.

Lesaffer, R. (2015). Too Much History: From War as Sanction to the Sanctioning of War. In M. Weller (Ed.), *The Oxford Handbook of the Use of Force in*

International Law (pp. 35–55).

Liang, Q., & Xiangsui, W. (1999). *Unrestricted Warfare*. PLA Literature and Arts Publishing House.

LMT en Español. (2003, March 23). *Perú no apoya acción armada en Irak*. LMT. https://www.lmtonline.com/lmtenespanol/article/Per-no-apoya-acci-n-armada-en-Irak-10329327.php

Malekos Smith, J. (2018). Swinging a Fist in Cyberspace. *Houston Law Review: Off the Record*, *9*(1).

Mancera, J. M. (2014). La ciberguerra china desde la lógica de la guerra irrestricta. *Ciencia y Poder Aéreo*, *9*, 89–96.

McCuen, J. J. (2008). Hybrid Wars. *Military Review*, *April*, 107–113.

McGuinness, D. (2017, May 6). *Cómo uno de los primeros ciberataques de origen ruso de la historia transformó a un país*. BBC News. https://www.bbc.com/mundo/noticias-39800133

McInnis, K. (2021). *The Interim National Security Strategic Guidance*.

Melzer, N. (2010). *Guía para interpretar la noción de participación directa en las hostilidades según el derecho internacional humanitario*.

Melzer, N. (2011). *Cyberwarfare and International Law*. http://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf

Miní, J. L., & Cori, J. Y. (2003). Funciones, principios y fuentes del derecho internacional humanitario. In F. Novak (Ed.), *Derecho internacional humanitario* (1st ed.). Fondo Editorial de la Pontificia Universidad Católica del Perú.

Ministerio de Defensa. (2017). Decreto Supremo No. 012-2017-DE, Decreto Supremo que aprueba la Política de Seguridad y Defensa Nacional. In *Diario Oficial El Peruano* (pp. 9–29).

Ministerio de Defensa. (2021). Decreto Supremo 005-2021-DE, que aprueba la

"Política Nacional Multisectorial de Seguridad y Defensa Nacional al 2030." In *Diario Oficial El Peruano*.

Ministerio de Relaciones Exteriores. (2010). Decreto Supremo No. 135-2010-RE, que aprueba el Reglamento de Organización y Funciones del Ministerio de Relaciones Exteriores. In *Diario Oficial El Peruano*.

Ministerio de Relaciones Exteriores. (2015). Plan Estratégico Sectorial Multianual (PESEM) de Relaciones Exteriores 2015-2021. In *Resolución Ministerial No. 1268-RE*. Ministerio de Relaciones Exteriores.

Ministerio de Relaciones Exteriores. (2019). Plan Estratégico Institucional 2020-2022. In *Resolución Ministerial No. 0536-RE*. Ministerio de Relaciones Exteriores.

Munteanu, R. (n.d.). *Saudi Arabia vs. Iran: From Proxy to Hybrid Warfare*. The Market for Ideas. Retrieved July 22, 2022, from https://www.themarketforideas.com/saudi-arabia-vs-iran-from-proxy-to-hybrid-warfare-a115/

Murphy, S. (2006). *Principles of international law* (4th ed.). West Academic Publishing.

Namihas, S. (2003). Antecedentes, origen y evolución histórica del Derecho Internacional Humanitario. In F. Novak (Ed.), *Derecho Internacional Humanitario*. Fondo Editorial de la Pontificia Universidad Católica del Perú.

NATO Cooperative Cyber Defence Centre of Excellence. (n.d.). *About us*. Retrieved October 6, 2022, from https://ccdcoe.org/about-us/

Ñaupas, H., Mejía, E., Novoa, E., & Villagómez, A. (2014). *Metodología de la Investigación Cualitativa-Cuantitativa y Redacción de la Tesis* (4th ed.). Ediciones de la U.

Ney Jr., P. (2020). *DOD General Counsel Remarks at U.S. Cyber Command Legal Conference*. https://www.defense.gov/News/Speeches/Speech/Article/2099378/dod-

general-counsel-remarks-at-us-cyber-command-legal-conference/

Office of the Secretary of Defense. (n.d.). *National Military Strategy*. Secretary of Defense. Retrieved November 2, 2022, from https://history.defense.gov/Historical-Sources/National-Military-Strategy/

Ohlin, J. D. (2015). Cyber Causation. In J. D. Ohlin, K. Govern, & C. Finkelstein (Eds.), *Cyberwar: Law and ethics for virtual conflicts* (pp. 37–54). Oxford University Press.

Organización del Tratado del Atlántico Norte. (2018, July). *NATO's response to hybrid threats*. https://www.nato.int/cps/en/natohq/topics_156338.htm

Paez, Á., & Ampuero, A. (2021, October 16). *Hackeo de secretos militares del Ejército es muy grave*. La República. https://larepublica.pe/politica/actualidad/2022/10/16/guacamaya-leaks-hackeo-de-secretos-militares-del-ejercito-es-muy-grave-fuerzas-armadas-comando-conjunto-vraem/

Pawlak, P. (2015). *Understanding hybrid threats*.

Payá, C., & Luque, J. M. (2018). Aproximaciones al concepto de amenazas híbridas. In C. Ardila & J. Jiménez (Eds.), *Convergencia de Conceptos: Propuestas de Solución a las Amenazas Actuales para la Seguridad y Defensa de Colombia*. Escuela Superior de Guerra "General Rafael Reyes Prieto"; Centro de Estudios Estratégicos en Seguridad y Defensa Nacionales.

Post Staff Report. (2011, March 26). *'Kinetic military action' is still hell* . New York Post. https://nypost.com/2011/03/26/kinetic-military-action-is-still-hell/

Presidencia de la República. (2010). Decreto Legislativo 1095, Decreto legislativo que establece las reglas de empleo y uso de la fuerza por parte de las Fuerzas Armadas en el territorio nacional. In *Diario Oficial El Peruano*. Diario Oficial El Peruano.

Presidencia de la República del Perú. (2012). Decreto Legislativo No. 1129,

Decreto Legislativo que regula el Sistema de Defensa Nacional. In *Diario Oficial El Peruano* (pp. 480165–480167).

Presidencia del Consejo de Ministros. (2021). Decreto Supremo 029-2021-PCM, que aprueba el Reglamento del Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, y establece disposiciones sobre las condiciones, requisitos y uso de las tecnologías y medios electrónicos en el procedimiento administrativo. In *Diario Oficial El Peruano* (pp. 8–43).

Presidencia del Consejo de Ministros de la República del Perú. (2013). *Decreto Supremo No. 037-2013-PCM, Reglamento del Decreto Legislativo 1129, que regula el Sistema de Defensa Nacional* (pp. 492104–492108).

Real Academia de la Lengua Española. (2014). Ciberespacio. In *Diccionario de la Lengua Española*. Real Academia de la Lengua Española.

Salmón, E. (2014a). *Curso de derecho internacional público*. Fondo Editorial PUCP.

Salmón, E. (2014b). *Introducción al derecho internacional humanitario* (3ra ed.). Comité Internacional de la Cruz Roja.

Salmón, E. (2016). *Introducción al derecho internacional humanitario* (3ra ed.). Comité Internacional de la Cruz Roja.

Sánchez García, F. (2012). El conflicto híbrido: ¿una nueva forma de guerra? In Ministerio de Defensa (Ed.), *El enfoque multidisciplinar en los conflictos híbridos* (pp. 11–23). Centro Superior de Estudios de la Defensa Nacional.

Schmitt, M. N. (1999). Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework. *Columbia Journal of Transnational Law*, *37*, 885–936.

Schmitt, M. N. (2016). The Use of Cyber Force and International Law. In M. Weller (Ed.), *The Oxford Handbook of the Use of Force in International Law* (Vol. 1, pp. 1110–1130). Oxford University Press.

https://doi.org/10.1093/law/9780199673049.003.0053

Servicio Europeo de Acción Exterior. (2018). *A Europe that protects: Countering hybrid threats*.

Sharma, D. (2010). Integrated Network Electronic Warfare: China's New Concept of Information Warfare. *Journal of Defense Studies*, *4*(2), 36–49.

State Council Information Office of the People's Republic of China. (2015, May). *China's Military Strategy*. Ministry of National Defense of the People's Republic of China. http://eng.mod.gov.cn/publications/2021-06/23/content_4887928.htm

Sulmeyer, M. (2017, July 24). *Which Cyberattacks Should the United States Deter, and How Should It Be Done?* Council on Foreign Relations. https://www.cfr.org/blog/which-cyberattacks-should-united-states-deter-and-how-should-it-be-done

Tidy, J. (2022, April 12). *Ukrainian power grid "lucky" to withstand Russian cyber-attack*. BBC News. https://www.bbc.com/news/technology-61085480

Traynor, I. (2007, May 17). *Russia accused of unleashing cyberwar to disable Estonia*. The Guardian. https://www.theguardian.com/world/2007/may/17/topstories3.russia

Tribunal Penal Internacional para la ex-Yugoslavia. (1999). *Fiscal v. Tadic, Caso N° IT-94-1-T, Sentencia del 15 de julio de 1999*.

Vallance, C. (2022, March 28). *Ukraine war: Major internet provider suffers cyber-attack*. BBC News. https://www.bbc.com/news/60854881

Verizon. (n.d.). *¿Qué es un antivirus? - Definición, significado y explicación* . Retrieved July 10, 2022, from https://espanol.verizon.com/info/definitions/antivirus/

Verri, P. (2014). *Diccionario de derecho internacional de los conflictos armados*. Comité Internacional de la Cruz Roja.

Weiss, C. (2015). How Do Science and Technology Affect International Affairs?

Minerva, *53*(4), 411–430. https://doi.org/10.1007/s11024-015-9286-1

Wolff, J. (2021, July 6). *Understanding Russia's Cyber Strategy*. Foreign Policy Research Institute. https://www.fpri.org/article/2021/07/understanding-russias-cyber-strategy/

Wood, M. (2018). The Caroline Incident - 1837. In T. Ruys, O. Corten, & A. Hofer (Eds.), *The use of force in international law: A case-based approach* (pp. 5–14).

Zandee, D., van der Meer, S., & Stoetman, A. (2021). *Countering hybrid threats: Steps for improving EU-NATO cooperation*.

Zhang, L. (2012). A Chinese perspective on cyber war. *International Review of the Red Cross*, *94*(886).