Grado en Derecho
Trabajo de final de Grado (21067/22747)
Curso académico 2018-2019

LOS CIBERATAQUES EN EL DERECHO INTERNACIONAL PÚBLICO

Natalia Cinta Linares Barrio
NIA- 184901

Tutor del trabajo:
Ángel José Rodrigo Hernández

upf. Universitat Pompeu Fabra Barcelona

DECLARACIÓN DE AUTORIA Y ORIGINALIDAD

Yo, Natalia Cinta Linares Barrio, certifico que el presente trabajo no ha sido presentado para la evaluación de ninguna otra asignatura, ya sea en parte o en su totalidad. Certifico también que su contenido es original y que soy el único autor, no incluyendo ningún material anteriormente publicado o escrito por otras personas salvo aquellos casos indicados a lo largo del texto.

Como autora de la memoria original de este Trabajo de Fin de Grado autorizo la UPF a depositarla y publicarla en el e-Repositorio: Repositorio Digital de la UPF, http://repositori.upf.edu, o en cualquier otra plataforma digital creada por o participada por la Universidad, de acceso abierto por Internet. Esta autorización tiene carácter indefinido, gratuito y no exclusivo, es decir, soy libre de publicarla en cualquier otro lugar.

Natalia Cinta Linares Barrio

Barcelona, 3 de junio de 2019

RESUMEN DEL CONTENIDO

El presente trabajo analiza el fenómeno de los ciberataques en el Derecho Internacional Público. Dada su reciente aparición en el panorama internacional, tanto los estados como los organismos supranacionales han tenido poco tiempo de adaptación, lo cual se plasma a nivel normativo y práctico. Consecuentemente, la respuesta legislativa actualmente es escasa, y doctrinalmente presenta disparidades. Pese a ello, este trabajo tiene como objetivo tratar de categorizar los ataques cibernéticos en conjunto con el resto del Derecho Internacional aplicable.

El contenido de este trabajo se divide en 3 partes, todas ellas interconectadas. En la primera analizo varias fuentes bibliográficas con el objetivo de obtener una definición aplicable a estos nuevos sucesos. A partir de esta, y dependiendo de su determinación, examinaré qué requisitos y circunstancias se deben dar para poder equipararlos a un ataque armado.

En segundo lugar, y en base a las respuestas obtenidas en los apartados anteriores, identifico a qué posibles autores pueden atribuirse la realización de tales ataques informáticos, ya sean estatales o no estatales.

Por último, y para concluir esta investigación, determino cómo pueden responder aquellas víctimas que sufran los perjuicios de un ciberataque equiparable a un ataque armado y atribuible a un actor identificado, para ello basándome en fuentes doctrinales y jurisprudenciales.

ÍNDICE

1. Introducción

Este trabajo de final de grado versa sobre los ciberataques y su realidad en el mundo del Derecho Internacional Público.

Inicié este proyecto con la ayuda de mi tutor, el profesor Ángel J Rodrigo Hernández, quien amablemente me lo sugirió de entre otros. Elegí esta temática, primeramente por su relevancia práctica y científica. Conocía de los ataques cibernéticos que sufrió Estonia en 2007[1]. Posteriormente en 2016, las elecciones norteamericanas reavivaron el debate[2]. En 2018 Reino unido apuntó a Rusia como autor de los mayores ataques informáticos del 2017[3]. Alemania a finales de 2018 reportó ciberataques a sus sistemas de defensa nacionales[4]. Y hace apenas unos días la Unión Europea aprobó una reforma en materia de ciberseguridad[5]. Cada día nuevos casos se suceden, siendo las consecuencias cada vez mayores, por lo que me tomé el TFG como una oportunidad para tratar de resolver las dudas que me surgían.

El proyecto tiene como objetivo determinar cómo la comunidad internacional y el Derecho Internacional han evolucionado para adaptarse a esta nueva realidad. Cómo está cambiando el sistema tradicional de categorizaciones. La metodología seguida es bibliográfica, jurisprudencial y documental, con un objetivo sintetizador, tanto de material convencional como consuetudinario. Sin embargo, debo advertir al lector sobre la falta de cohesión doctrinal y literaria que actualmente presenta la materia, la cual puede verse plasmada en mi investigación.

La estructura del trabajo sigue el siguiente esquema lógico: en primer lugar, trato de identificar la definición de este nuevo reto. Seguido de un estudio acerca de su posible equiparación a un ataque armado. En segundo lugar, analizo su posibilidad de atribución, incluso si los actores no son estatales. Y finalmente, cómo pueden las víctimas responder ante aquellos ciberataques calificados como ataque armado.

---

[1] McGuinness, D. (2017, 6 mayo). *Cómo uno de los primeros ciberataques de origen ruso de la historia transformó a un país*. Recuperado 24 mayo, 2019, de https://www.bbc.com/mundo/noticias-39800133

[2] Pereda, C. F. (2016, 30 diciembre). Así se produjo el ciberataque ruso en la campaña electoral de EE UU, según el FBI. Recuperado 24 mayo, 2019, de https://elpais.com/internacional/2016/12/30/estados_unidos/1483119060_863004.html

[3] Ciberataques: el Reino Unido acusa a Rusia de ser un "Estado paria". (2018, 4 octubre). Recuperado 24 mayo, 2019, de https://es.euronews.com/2018/10/04/ciberataques-el-reino-unido-acusa-a-rusia-de-ser-un-estado-paria

[4] Alemania detecta un nuevo ciberataque proveniente de Rusia, según el 'Der Spiegel'. (2018, 30 noviembre). Recuperado 24 mayo, 2019, de https://www.europapress.es/internacional/noticia-alemania-detecta-nuevo-ciberataque-proveniente-rusia-der-spiegel-20181130104007.html

[5] Reforma de la ciberseguridad en Europa - Consilium. (s.f.). Recuperado 24 mayo, 2019, de https://www.consilium.europa.eu/es/policies/cyber-security/

2. Ciberataques y ataques armados

Las amenazas cibernéticas empezaron a suscitar el interés de la comunidad internacional a mediados de los años 90, cuando la importancia de las de los sistemas informáticos empezaba a incrementarse. Sin embargo, la idea parecía algo futurístico y lejano, y tras los atentados en Estados Unidos del 11 de septiembre de 2001, la idea se postergó de la agenda internacional. Y así se mantuvo hasta el año 2007, momento en el que Estonia (Estado miembro de la OTAN) sufrió numerosos ataques cibernéticos por parte de actores no estatales rusos[6]. Al año siguiente, mientras se desarrollaba el conflicto armado entre Rusia y Georgia[7], también se pudieron constatar numerosas operaciones informáticas contra infraestructuras cibernéticas[8] georgianas. Ese mismo año Lituania sufrió los mismos sucesos[9]. Parecía que aquello tan lejano necesitaba una respuesta inminente. Y ésta vino de la mano del Centro de Excelencia Cooperativa y Defensa Cibernética de la OTAN, el cual promulgó y propició en 2009 un gran proyecto de investigación centrado exclusivamente en examinar el Derecho Internacional Público aplicable a las amenazas cibernéticas. Para llevar a cabo tal aspiración, se creó un equipo de 20 académicos y juristas de renombre internacional, conocidos como "el Grupo de Expertos Internacionales" (GEI). Estos investigadores pasaron los siguientes 3 años (finalizó en 2012) redactando el que es hoy en día uno de los pocos documentos legales en la materia, el conocido como *Manual de Tallinn sobre el Derecho Internacional aplicable a la guerra cibernética*[10].

En la figura 1 se muestra una visión sintética del contenido de este primer bloque.

---

[6] Para más información véase: capítulo IV del Cuaderno de Estrategia nº 149, *Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio*, del Instituto Español de Estudios Estratégicos junto con Instituto Universitario "General Gutiérrez Mellado", 2010 http://www.ieee.es/Galerias/fichero/docs_informativos/2011/DIEEEI092011ConceptoCiberdefensaOTAN.pdf

[7] Tikk, E., Kasha, K., & Vihul, L. (2010). *International Cyber Incidents: legal considerations*. Cambridge, United Kingdom: Cambridge University Press, Recuperado de https://ccdcoe.org/uploads/2018/10/legalconsiderations_0.pdf

[8] El término "infraestructura cibernética" hace referencia a "comunicaciones, almacenaje y recursos informáticos sobre los cuales operan sistemas de información. Internet es un ejemplo de sistema de información global" Concepto extraído de Schmitt, M. N. Schmitt (2013). de *Manual On the International Law Applicable to Cyber Warfare,* Cambridge University Press, p 212 Recuperado de http://csef.ru/media/articles/3990/3990.pdf

[9] Tikk, E., Kasha, K., & Vihul, L. (2010). *International Cyber Incidents: Legal considerations* pp 50-66

[10] OOCDCE. (2017). *Manual de Tallinn 2.0 on the international law applicable to cyber operations* (2ª ed.). Cambridge, United Kingdom: Cambridge University Press.

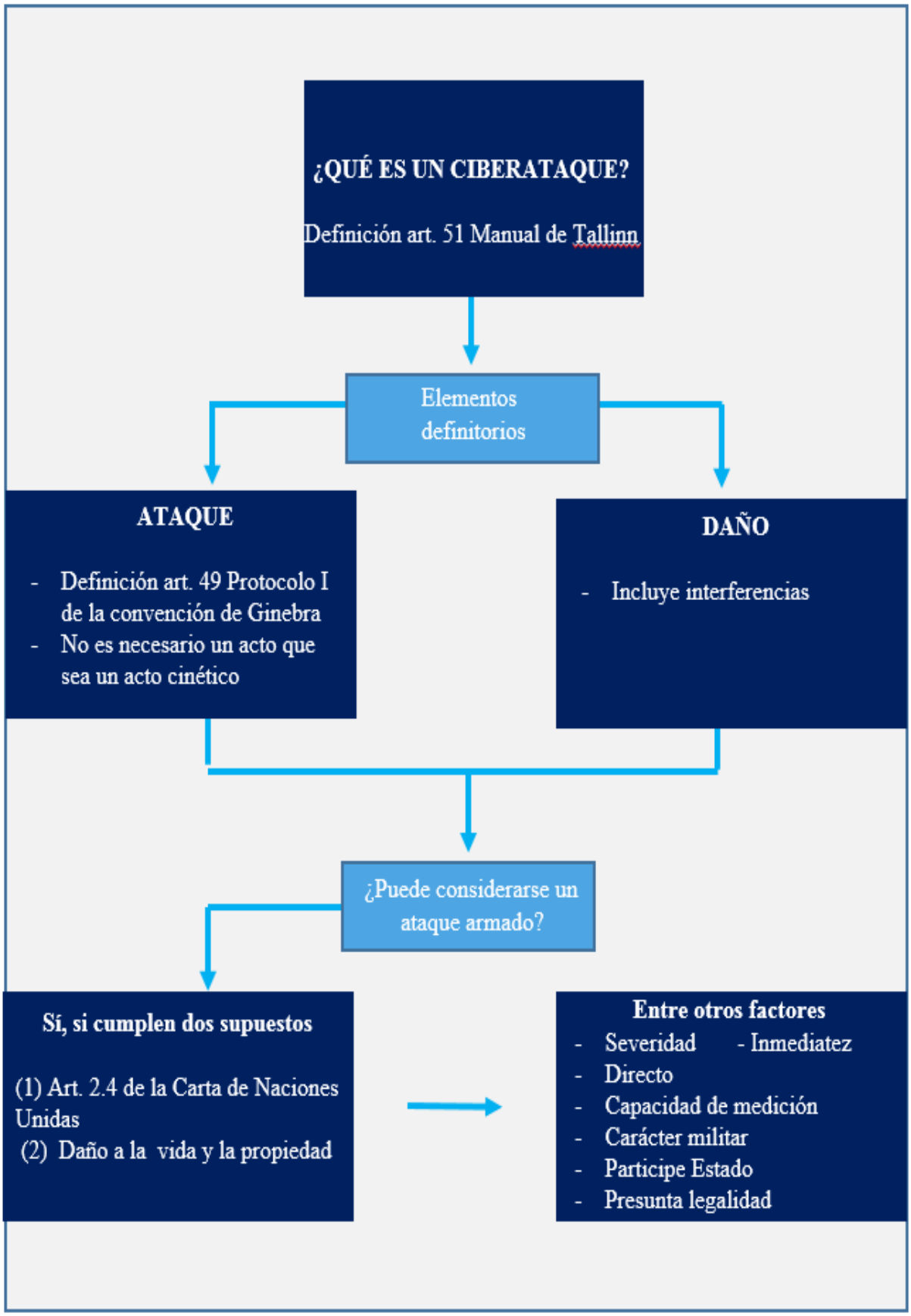

Figura 1: Cuadro sinóptico del contenido del primer capítulo.

2.1La definición de ciberataque

El *Manual de Tallin* es un instrumento no vinculante que explora la aplicabilidad del Derecho Internacional Público a los conflictos cibernéticos. Su proceso de creación fue complejo, pero se encontraba especialmente limitado por dos problemas esenciales. El primero era el ínfimo conocimiento que se tenía en 2009 acerca de los ciberataques[11]. La comunidad internacional era muy consciente de su creciente importancia, pero aún eran pocos los casos que se habían dado hasta entonces. Pero además, a este problema inicial se le debía añadir la escasa práctica estatal realizada hasta entonces por los Estados. Por lo tanto, las pautas aun no estaban claramente definidas. Bajo estas premisas, los expertos decidieron centrarse en las legislaciones existentes, no en futuras o eventuales reformas legislativas que se pudiesen llevar a cabo[12]. Y con estas ideas en mente, iniciaron su misión.

El paso previo a poder definir los ciberataques era determinar si el Derecho Internacional puede aplicarse en el ciberespacio. No hubo dudas a la hora de responder, todos los miembros del GEI lo consideraron el instrumento más adecuado para regular tales hechos[13]. Sin embargo, no podemos obviar el hecho de que el Derecho Internacional Público es de naturaleza dinámica. Su contenido, interpretación y aplicación evolucionan con el paso del tiempo como respuesta a la transformación del entorno al que se aplica. Esta característica se agudiza más aún en el ámbito de los ciberataques, puesto que *si bien los principios están bien establecidos y se aplican en el contexto del ciberespacio, también es cierto que la interpretación de estos cuerpos legales en el contexto de las actividades en el ciberespacio puede presentar desafíos nuevos y únicos que requerirá consulta y cooperación entre las naciones*[14].

Aun con estas dificultades, pero una vez delimitada la aplicación del Derecho Internacional, el GEI trató de dar una definición a los ataques cibernéticos. El punto de partida fue el propio

[11] Geers, K. (2007). *Cyberspace and the Changing Nature of Warfare*. Recuperado de https://ccdcoe.org/uploads/2018/10/Geers2008_CyberspaceAndTheChangingNatureOfWarfare.pdf

[12] Tikk, E. and Talihärm, A-M. (eds.), *International Cyber Security Legal & Policy Proceedings* 2010, Tallinn: NATO CCDCOE. Recuperado de https://ccdcoe.org/uploads/2010/01/LP_Proceedings_2010-2.pdf

[13] Schmitt, M. N. (2014). The Law of Cyber Warfare: Quo Vadis? Stanford Law & Policy Review, p 25 (2), 270. Recuperado de https://law.stanford.edu/publications/law-cyber-warfare-quo-vadis/

[14] Secretario General NU (2011), *Developments in the Field of Information and Telecommunications in the Context of International Security*: Rep. of the Secretary-General, pp 18-19, U.N. Doc. A/66/152

término "ataque" [15], el cual ha sido siempre un eje central del derecho de la guerra. La *Convención de Ginebra*, en 1949, y su consiguiente *Protocolo Adicional I*, artículo 49, define los ataques como *un acto de violencia ejercida contra un adversario, ya sea en defensiva o en ofensiva*. Esta concepción era suficiente en un momento histórico en el que los ataques eran casi exclusivamente ejercidos por medios cinéticos, y por lo tanto, eran de naturaleza dinámica. Sin embargo en el caso de las ciberoperaciones la definición debe ser interpretada diferentemente, puesto que no siempre generan efectos perjudiciales físicos.

Aun así, el artículo 49 fue el punto de partida para el GEI, con su aparejada necesidad de adaptación. Respecto a él, el grupo presentó ciertas disparidades. Algunos entendieron que la definición sólo comprendía aquellos actos con consecuencias físicas negativas, por lo que no debería comprender los ataques cibernéticos (actualmente esta posición ha sido muy moderada). Otros admitieron un punto de vista más amplio y entendieron que el concepto de "ataque" también puede incluir ciertos comportamientos *no destructivos pero igualmente perjudiciales* militarmente hablando[16]. Ambos puntos de vista tienen sus pros y sus contras, pero finalmente se optó por una interpretación más abierta del concepto "ataque", permitiendo así, que tras largas deliberaciones, los expertos redactaran el artículo 51.2 del *Manual de Tallinn*, pieza crucial de este entramado cibernético. Serán considerados ataques cibernéticos toda *operación cibernética, ya sea ofensiva o defensiva, que se espera razonablemente que cause lesiones o la muerte a personas o daños o destrucción de objetos*[17].

La primera característica que salta a la vista de esta definición es la referencia al *Protocolo I*, al hablar de cualquier *operación, ya sea defensiva u ofensiva*. Al aplicar una estructura tan similar a la del artículo 49 los expertos dan a entender no querían limitarlo a aquellos casos en los que hay *liberación de fuerza cinética*[18].

En segundo lugar, con esta definición se convierten en determinantes las consecuencias que se derivan de él. La existencia de un "daño" es condición necesaria para cualificar un hecho como

---

[15] Schmitt, M. N. (2012). *"Attack" as a Term of Art in International Law: The Cyber Operations Context*. Stanford Law & Policy Review, 25(2), p 289. Recuperado de https://ccdcoe.org/uploads/2012/01/5_2_Schmitt_AttackAsATermOfArt.pdf

[16] Schmitt, M. N. (2002). *Wired warfare: Computer network attack and jus in bello*. International Cometee of the Red Cross, p 25 (2), 84–846. Recuperado de https://www.icrc.org/en/doc/assets/files/other/365_400_schmitt.pdf

[17] CCDCOE. (2012b). *Tallinn Manual on international law applicable to cyber warfare*. Nato CCDCOE, Rule 30 91. Recuperado de http://csef.ru/media/articles/3990/3990.pdf

[18] Norries, M. J. (2013). In brief: *The Law of Attack in Cyberspace: Considering the Tallinn Manual's Definition of 'Attack' in the Digital Battlespace*. Inquiries Journal, p 5 (10), 1. Recuperado de http://www.inquiriesjournal.com/articles/775/the-law-of-attack-in-cyberspace-considering-the-tallinn-manuals-definition-of-attack-in-the-digital-battlespace

ataque cibernético. Sin embargo, esta segunda característica suscitó de nuevo discrepancias. Mientras que algunos miembros opinaron que aquellos ataques a la información contenida en infraestructuras cibernéticas son daños, la mayoría entendieron que hacer eso implicaba distorsionar la ley, al opinar que no hay suficiente práctica estatal en la materia[19]. El estado de la ley limita el concepto "daño" a una consecuencia causada tanto a personas como objetos físicos. Actualmente la normativa bélica utiliza la terminología "daño" o "perjuicio" en referencia a objetivos físicos "visibles y tangibles"[20]. Sin embargo, es difícil que este punto de vista perdure en el caso de ciberataques, puesto que las circunstancias son muy diferentes. En general, los ataques cibernéticos no requieren de los tradicionales movimientos dinámicos previstos en la mayoría de cuerpos legales, ya que normalmente los objetivos son sistemas y fuentes de información, sin que ello implique un daño menor. Por ejemplo, un ciberataque a los censos electorales es un impedimento más grave a la continuación de las funciones gubernamentales que la destrucción de sus equivalentes físicos. Consecuentemente, parece ilógico defender que si las operaciones van dirigidas contra sistemas informáticos, el daño producido a éstas no tiene cabida en la definición de ciberataque[21]. Dada la creciente importancia del mundo informático, una definición que limita los ciberataques únicamente a aquellos actos generadores de daño físico, no sobrevivirá al paso del tiempo[22].

No obstante, la definición no precisa qué magnitud debe tener el daño a efectos de poder ser considerado un ciberataque. A primera vista, tras leer la definición proporcionada por el GEI, parece que aquellos ataques dirigidos contra infraestructuras tecnológicas o informáticas, pero con consecuencias mínimas, no cumplen con el estándar de "daño" necesario según la definición. Estas interferencias pueden crear confusión, desorganización, e interrupciones, pero es improbable que causen daño físico a los objetos[23]. El GEI mantuvo una extensa discusión acerca de si esta "interferencia", entendida como la afección a la funcionalidad del objeto, constituye daño o destrucción de acuerdo con lo establecido en *el Manual*. Hubo opiniones de todo tipo. Algunos de ellos entendían que no, que a fecha de hoy, la práctica estatal no nos permite justificar que el causar inconveniencias esté prohibido por la normativa internacional[24] Sin embargo, la mayoría sí consideraron que la interferencia constituye un daño, siempre y

[19] Schmitt, M. N (2014) *The Law of Cyber Warfare: Quo Vadis*, p 285
[20]ICRC. (1987b). *Commentaries to Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts* (Protocol I), p 90. Recuperado de https://ihl-databases.icrc.org/ihl/INTRO/470
[21] Ibid p 90
[22] Schmitt, M. N (2014) *The Law of Cyber Warfare: Quo Vadis*, p 286
[23] Ibid, p 286
[24] Schmitt M. N.(2013*). Manual on the International Law applicable to cyber warfare*, p 221

cuando para reestablecer su funcionalidad se requiera reemplazar ciertos componentes. Este punto de vista era discutido en caso de que se pudiese solventar simplemente reiniciando el sistema[25]. Otros entendieron que la cuestión residía en si el objeto perdía o no su utilidad por completo. Ahora, debemos entender que hay diversas formas de interferir, ya sea de forma total, parcial, temporal o permanente[26]. Por ejemplo, en los ciberataques realizados contra Georgia o Estonia, las operaciones llevadas a cabo fueron interrupciones de tiempo muy breve, menos de 40 minutos, pero impidieron el acceso informático de altos mandos militares a sus ordenadores. Estos casos serían ejemplos de disrupción sin daño, los cuales puede ser comprensible que no tengan cabida en la definición. Pero ¿y si en vez de cuarenta minutos hubiesen sido cuatro días, y durante esos días los atacantes hubiesen obtenido información de importante valor estratégico? A primera vista no se obtiene ningún daño, por lo que no podríamos considerarlo un ciberataque. Sin embargo, las consecuencias que puede llegar a implicar son incalculables, por lo que la futura práctica internacional deberá necesariamente determinar en qué punto el daño *de minimis* se convierte en un ataque.

En base a estas precisiones, algunos expertos han comentado posibles mejoras a la definición de ciberataque aportada por el *Manual.* El autor Michael J Norries es partidario de expandir la definición e incluir, no sólo interrupciones, sino también la neutralización, ya sea temporal o definitiva, de la funcionalidad de un elemento tecnológico[27]. Siendo el concepto de "neutralización" no ajeno a previas redacciones internacionales, como el *Protocolo I*[28]. Otros autores, con puntos de vista más radicales, han desechado la definición del *Manual de Tallinn* y han tratado de dar su propia descripción a estos hechos, entendiendo los ciberataques como *una expresión que se utiliza para describir un conjunto de actividades nocivas que tienen lugar en el ciberespacio*[29], especialmente aquellas que persigan el objetivo de *degradar, interrumpir,*

[25] Ibid, pp 104- 108
[26] [26]Norries, M. J. (2013). *In brief: The Law of Attack in Cyberspace: Considering the Tallinn Manual's Definition of 'Attack' in the Digital Battlespace*. Inquiries Journal, p 7
[27] Ibid p 3
[28] ICRC. (1977). *Protocolo I adicional a los Convenios de Ginebra de 1949 relativo a la protección de las víctimas de los conflictos armados internacionales,* 1977. Art 52.2 Recuperado de https://www.icrc.org/es/document/protocolo-i-adicional-convenios-ginebra-1949-proteccion-victimas-conflictos-armados-internacionales-1977
[29] Cornish, P., Livingstone, D., Clemente, D., & Yorke, C. (2010). *On Cyber Warfare* A Chatham House Report. Chatham House, 8. Recuperado de https://www.chathamhouse.org/sites/default/files/public/Research/International%20Security/r1110_cyberwarfare.pdf

negar o destruir la información que reside en las computadoras, o comprometer las propias computadoras.[30]

Todas estas sugerencias son bienvenidas, pero hasta que tal redefinición ocurra, la comunidad internacional debe tratar de resolver las cuestiones que se plantean sin desestimar el importante papel que realiza el *Manual de Tallinn*. Primeramente, cabe recordar que la interpretación del *Manual* debe hacerse en base a su objeto y función (art 31 *Convención de Viena*)[31]. En el caso de los ciberataques una interpretación correcta de la definición debe basarse en el equilibrio entre las necesidades militares y las preocupaciones humanitarias globales, a la luz del día presente y de los valores que los Estados deseen proteger[32]. Y es justo esta naturaleza dinámica la clave para entender cómo el término ciberataque puede ser entendido en el futuro.

Lo más probable es una eventual extensión de la noción de "ataque" para incluir cualquier interferencia con aquellas infraestructuras que sean esenciales para la población civil. La dificultad que esto presenta es que como hemos visto, la definición se centra más en la naturaleza del daño producido, no el objeto que lo sufre. Por lo tanto, surgen dos posibles alternativas: (1) o bien emerge una nueva norma a través de un tratado, hipótesis muy complicada dada lo difícil que ya fue la creación del *Manual de Tallin*. O bien, (2) la cristalización de una norma consuetudinaria, que siempre es una cuestión indeterminada pero más plausible. Los Estados simplemente empezaran a tratar los ataques cibernéticos contra infraestructuras civiles básicas como ataques, por lo que crearan práctica estatal uniforme y generalizada, sobre la cual la interpretación del concepto evolucionará[33].

Por otro lado, lo que entendemos como "daño" se extenderá obligatoriamente más allá de la estricta limitación a objetos físicos, independientemente de las distintas opiniones que se susciten a fecha de hoy. Hoy en día la importancia de las nubes de datos excede su manifestación física. Así, es prácticamente seguro que la definición se ampliará a medida que crezca su relevancia. Sin embargo, debemos tomar medidas para evitar exceso de amplitud en

---

[30] Joint Chiefs of Staff. (1998). Joint Publication 3-13 Information Operations. Recuperado de https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf

[31] Naciones Unidas. (1969). *Convención de Viena sobre el derecho de los tratados*, p 12. Recuperado de https://www.oas.org/xxxivga/spanish/reference_docs/convencion_viena.pdf

[32] Schmitt, M. N. (2010). *Military Necessity and Humanity in International Humanitarian Law: Preserving the Delicate Balance.* Virginia Journal of International Law, p 50 (4), 50. Recuperado de https://poseidon01.ssrn.com/delivery.php?ID=424069105013092068064027080006111112050024004033095068067067013076106064117076104022028097000118014120007090115103075105106007029055059029004092

[33] Schmitt, M. N. *The Law of Cyber Warfare: Quo Vadis?* (2014) p 296

la definición. Tratar toda afectación como daño podría conllevar un efecto de preclusión de cualquier operación que directamente afecte infraestructuras civiles[34].

Para terminar este apartado, debemos analizar la aplicación del concepto "uso dual" respecto a los ciberataques. Un objeto dual es aquel que puede ser utilizado tanto con fines militares como civiles. La comunidad internacional ha entendido que una vez un objeto empieza a ser utilizado militarmente, es calificable como objetivo militar legalmente válido[35].

El dilema consiste en que gran parte de la existente ciberestructura es de uso dual, y eso no va a cambiar en el futuro. En numerosas ocasiones comunicaciones militares se han realizado a través de canales civiles. Por ejemplo, redes sociales como Twitter o Facebook han sido utilizadas en conflictos para compartir información militar relevante[36]. Del mismo modo, hay ciertas armas que utilizan datos generados por sistemas GPS. Esta realidad fue otro punto de discusión para el GEI. Al final siguieron con la concepción tradicional, y concluyeron que todos los objetos de uso dual son considerados objetivos militares[37]. Cualquier tipo de protección respecto a ellos debe cumplir con los principios militares de proporcionalidad y distinción. No obstante, es difícil que este punto de vista se mantenga en el tiempo. La dependencia respecto de la infraestructura civil sigue creciendo, y será difícil justificar la financiación de nuevas redes separadas de las civiles o la adquisición de productos diseñados únicamente para objetivos militares. A fecha de hoy, es muy poco claro cómo se resolverá esta cuestión.

Tras estas explicaciones podría parecer que la utilidad del *Manual de Tallinn* ha quedado cuestionada. Nada más lejos de la realidad, las normas resultantes han sido bienvenidas y en general bien aceptadas tanto por Estados como por organizaciones internacionales[38]. Simplemente debemos interpretar la herramienta de forma coordinada con la evolución que realicen los Estados con el paso de los años. Las limitaciones mencionadas son resultado del momento histórico en que fue redactado. La propia tecnología estaba en fases menos evolucionadas que ahora. Hoy en día la informática representa uno de los pilares básicos de todo país, en todos los planos (gubernamental, económico, individual personal, profesional...).

---

[34] Ibid p 297
[35]Schmitt, M. N. (2013). de *Manual on the International Law applicable to Cyber Warfare*, p 112
[36] Schmitt, M. N (2014). *The law of cyber warfare: quo vadis?* p 298
[37] Ibid, p 113
[38] Schmitt, M. N. (2012b). *International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed.* Harvard International Law Journal 54. Recuperado de https://harvardilj.org/wp-content/uploads/sites/15/2012/12/HILJ-Online_54_Schmitt.pdf

La casi absoluta dependencia a toda infraestructura tecnológica [39] empieza a verse como un importante punto débil de nuestra seguridad. En aquellos momentos el *Manual* respondía a una necesidad incipiente. Su función fue la de abrir la vereda a nuevas redacciones, y debe ser entendido desde ese punto de vista. Aunque es cierto que toda legislación debe responder a un objetivo, el de mantenerse efectiva en el tiempo, esto puede resultar complicado en el ámbito cibernético, y después de todo, el *Manual de Tallinn* no pretendía crear legislación aplicable a un campo tan fluctuante como es el ciberespacio.

Tal y como remarcamos inicialmente, el Derecho Internacional es altamente dinámico. Siempre que ocurren cambios significativos emergen nuevas normas, expiran las antiguas, y la interpretación de las existentes varía. La dirección y velocidad a la que estos cambios legislativos se producen depende, en gran parte, de la influencia que ejercen diferentes fuentes: organizaciones internacionales, tribunales internacionales, grupos políticos… Sin embargo, el proceso aún está mayormente dominado por los Estados, tal y como se consagró en el caso *Lotus*[40]. Los elementos claves en estos procesos son tanto su consentimiento (*opting in*), como aquellas *opinio iuris* que eventualmente cristalicen en Derecho Internacional consuetudinario[41]. Además, de por supuesto, actuar conforme a sus intereses. A medida que los Estados se conviertan más dependientes cibernéticamente hablando, valoraran más el acceso y capacidad de explotación del ciberespacio. Además, utilizaran todas las posibilidades existentes para salvaguardar su ciberinfraestructura, puesto que se basan en ella. Así pues, cabe esperar un período de cambios continuados para el Derecho Internacional en lo referente a los ciberataques, puesto que las normas deberán adaptarse tanto a intereses de los Estados, como a circunstancias. Sin embargo, el éxito o fracaso de tales necesidades debe necesariamente partir de las normas desarrolladas en el *Manual de Tallinn*.

2.2 La noción de ciberataque como ataque armado (prohibición del uso de la fuerza)

[39] M. N. Schmitt (2013). De *Manual on the International Law applicable to Cyber Warfare* p 211, infrestructura teconológica entendida como *Los sistemas físicos o virtuales y las declaraciones bajo la jurisdicción de un Estado que son tan vitales que su incapacidad o destrucción pueden debilitar la seguridad, la economía, la salud o la seguridad públicas de un Estado o el medio ambiente*.

[40] Caso *Lotus*, CIJ, Recueil 1928, p 3 Recuperado de: https://www.dipublico.org/10984/s-s-lotus-1927-corte-permanente-de-justicia-internacional-ser-a-no-10/

[41] Asunto *Plataforma Continental del Mar del Norte*, ICJ Reparts 1969, p 60- 82 Recuperado de: https://www.dipublico.org/cij/doc/44.pdf

En el aparatado precedente he analizado la definición de ciberataque, la cual nos ha permitido encajarlo dentro de la categoría de aquello tradicionalmente conocido como operaciones de información.[42] Ahora debemos examinar la posible equiparación de estos ciberataques a un ataque armado.

El proceso de equiparación debe partir del artículo 2.4 de la *Carta de las Naciones Unidas* (CNU). Este proclama uno de los principios más importantes para el mantenimiento de la paz, la prohibición del uso de la fuerza en las relaciones internacionales. La propia Carta prevé dos excepciones a este artículo: el uso de la fuerza en legítima defensa, y la acción coercitiva decidida por el Consejo de Seguridad[43]. Ambas serán estudiadas en este trabajo más adelante.

El concepto "fuerza" mencionado por el artículo, ha sido precisado y refinado por la resolución 26/25 de la Asamblea General. Esta permite interpretar evolutivamente el concepto, incluyendo fuerza indirecta. Tal precedente se asentó en el caso *Nicaragua*, en el cual la Corte Internacional de Justicia (CIJ)[44] sentenció que el hecho de que un estado arme y entrene guerrilleros contra otro estado ya es suficiente como para ser calificado como violación de la prohibición del uso de la fuerza. La lógica de tal sentencia nos permite entender que incluso aquellos ataques cibernéticos que no conlleven consecuencias perjudiciales, pueden llevar la misma consideración. Por ejemplo, sería calificable como tal el hecho de proporcionar programario malicioso a un grupo rebelde y capacitar a sus miembros para que lo empleen de manera destructiva contra otro. Por otro lado, y para completar el artículo 2.4, otra resolución, en este caso la 33/14 define el concepto de agresión como *la fuerza armada contra la soberanía e independencia territorial de otro Estado*. Se prohíbe el uso de la fuerza entre Estados en sus relaciones internacionales, pero se permite entenderlo evolutivamente e incluir también a los actores no estatales.

Sin embargo, y aun con las resoluciones complementarias, la aplicación práctica del artículo 2.4 presenta incertidumbres, lo cual ha dificultado que la comunidad internacional haya podido identificar en qué momento un acto se convierte en un ataque armado. En general, se entiende que cuando los tradicionales ataques dinámicos pueden calificarse como ataques armados,

---

[42] Roscini, M. (2010), *World Wide Warfare- Jus Ad Bellum and The Use of Cyber Force,* Max Planck Yearbook of UN Law (14),p 102 Recuperado de: http://www.mpil.de/files/pdf3/mpunyb_03_roscini_141.pdf

[43] UN (1945) *Carta de las Naciones Unidas*, 1945, Capítulo 1, Art 2.4 Recuperado de: https://www.un.org/es/sections/un-charter/chapter-i/index.html

[44] Asunto *Actividades Militares y Paramilitares en Nicaragua*, ICJ Reparts 1986, p 212 Recuperado de: https://www.dipublico.org/cij/doc/79.pdf

también pueden serlo aquellos ataques cibernéticos que causen daños o perjuicios[45]. El problema interpretativo reside en si podemos aplicar la norma en el caso de aquellas ciberoperaciones que, pese a no provocar consecuencias destructivas, conllevan severas consecuencias no-físicas.

En el apartado anterior expliqué cómo el GEI rechazó interpretar de forma limitada el concepto de "ataque" de forma que lo limite a la fuerza física. Sin embargo, no todos los actos hostiles son susceptibles de ser calificados como uso de la fuerza. El artículo 2.4 por un lado prohíbe la amenaza y el uso de la fuerza, aunque sólo la fuerza armada (la fuerza política y económica no está prohibida, aunque supondría una violación al principio de no intervención). Consecuentemente, podríamos entender que aquellos ciberataques que tienen por objetivo coaccionar económicamente a un estado, no sería uso de la fuerza.

Por otro lado, y haciendo referencia al adjetivo "armado", debemos cuestionarnos si los ciberataques pueden considerarse ataques "armados". Armado, en el sentido más común de la palabra, significa equipado con un arma o instrumento utilizado o diseñado para hacer daño o matar a alguien[46]. La CIJ ya he especificado, en su Opinión Consultiva sobre la Legalidad del Uso de Armas Nucleares, que el art 2.4 de la Carta *no se refiere a armas específicas. Es aplicable a cualquier uso de la fuerza, independientemente de las armas empleadas.*[47] Por lo tanto, el uso de armas duales no cinéticas, como por ejemplo armas bacteriológicas, sin duda alguna sería considerado una prohibición del uso de la fuerza, puesto que dañan tanto la vida como la propiedad[48]. Y estas mismas características también las cumplen los ataques cibernéticos. Sin embargo, aparte de este límite, el resto de circunstancias son discutibles.

Frustrado el intento de dibujar una pauta que nos permitiese determinar con claridad qué características permitirían la equiparación de un ciberataque a un ataque armado, el GEI desarrolló un listado de características y factores (no exclusivos) que pueden ayudar a los Estados a determinar cuándo un ciberataque es muy probable que constituya una violación a la prohibición del uso de la fuerza. Estos ocho indicadores representan las mayores distinciones entre usos de la fuerza permisibles (económicos y políticos) y prohibidos (ataques armados).Cuantos más sean aplicables, más probable será que estemos ante un ataque armado[49].

---

[45] Schmitt (2014), *The law of cyber warfare: quo vadis?* p 279
[46] Roscini (2010), *World Wide Warfare- Jus ad bellum and the Use of Cyber Force*, p 106
[47] CIJ (1996), *Legality of the threat or use of nuclear weapons, advisory opinion,* p 22 Recuperado de: https://www.icj-cij.org/files/case-related/95/095-19960708-ADV-01-00-EN.pdf
[48]Brownlie, I. (1963). *International Law and the Use of Force by States*. Oxford, United Kingdom: Oxford, p 362
[49] Schmitt (2014), *The law of cyber warfare: quo vadis?,* p 280

El análisis consiste en el siguiente[50]:

- Severidad: aquellos ciberataques que suponen una amenaza física grave se aproximan más al ataque armado.
- Inmediatez: las consecuencias que se manifiestan rápidamente sin que dé tiempo a poder mitigar los daños o una solución pacífica es más probable que constituyan un uso prohibido de la fuerza.
- Directo: cuanto más directa es la conexión causal entre la ciberopración y las consecuencias, más probable será que los Estados la puedan equiparar al ataque armado.
- Invasividad: cuanto más perjudique a la integridad territorial o soberanía de un estado, más probable será que sea visto como un uso prohibido de la fuerza.
- Capacidad de medición: cuando las consecuencias que se deriven son fácilmente identificables y objetivamente cuantificables, más cerca estaremos de un ataque armado.
- Carácter militar: si la ciberoperacion es militar, más probable es la equiparación.
- Participación de un Estado: cuanto más cercano sea el nexo entre la ciberoperación y un Estado, más probable es que se caracterice como uso prohibido de la fuerza.
- Presunta legalidad: aquellas actividades que son legítimas fuera del ámbito cibernético, se mantienen así en él, por ejemplo: propaganda, operaciones psicológicas, espionaje…

Algunos otros factores adicionales que los expertos consideraron relevantes fueron: el ambiente político preexistente, la identidad del atacante, su registro de operaciones, y la naturaleza del objetivo.

La forma en que estos factores se evalúan tiene un alto contenido circunstancial. Son útiles pero no determinantes, y no deben ser aplicados de forma mecánica. Deben ser entendidos en su contexto, en conjunto con aquellos otros elementos que puedan ser importantes. En todo caso, los expertos entendieron que el sistema es más útil en análisis posteriores, que no en operaciones presentes. Así pues, qué factores son más importantes, o cómo deben ser interpretados variará caso por caso[51], aunque sí llegaron a la conclusión de que de todos ellos, su severidad es la que más peso puede tener para cualificar una ciberoperación como uso de la fuerza. Por ejemplo, concluyeron que el daño sufrido en plantas nucleares iraníes en 2010 como resultado del virus Stuxnet superaba esa condición de daño mínimo necesario y podría haber sido equiparada a un

[50] Foltz, A. C. (2012). *Stuxnet, Schmitt Analysis, and the Cyber "Use-of-Force" Debate*. National Defense University Press, (67), p 43. Recuperado de https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-67/JFQ-67_40-48_Foltz.pdf
[51] Ibid p 43

ataque armado, pero no fue considerado como tal porque no fue realizado sin justificación legal[52].

La reacción de los Estados ante las ciberoperaciones, así como también la forma en que ellos mismos caracterizan sus propias ciberactuaciones, nos muestra cómo está evolucionando el proceso de calificación. Quizás se consiga idear alguna herramienta normativa que nos permita determinar con claridad cuándo podemos calificarlos como un ataque armado. O quizás mediante la práctica se creen una serie de presunciones. Por ejemplo, aquellas ciberoperaciones dirigidas contra determinadas categorías de objetivos (en particular, estructuras críticas para la población civil), tendrán la presunción de ataque armado cuando las consecuencias sean altamente disruptivas a nivel social, económico o gubernamental[53]. Actualmente es significativo el hecho de que numerosos países han incluido la cibertecnología en sus doctrinas militares, o han creado unidades especiales para la defensa de determinados *warfares*. Estos hechos también deben ser tomados en consideración en el momento de interpretar el artículo 2.4 de la CNU, puesto que según el artículo 31.3 b) de la *Convención de Viena sobre el Derecho aplicable a los Tratados*, debe ser interpretado incluyendo *cualquier práctica subsiguiente* que hayan realizado las partes en relación a su aplicación. Además, varios estados han comparado los ciberataques como si de un nuevo tipo de ataques armados se tratase. Por ejemplo, el programa de Estados Unidos "Joint Vision 2020" hace referencia expresa al uso de armas no-dinámicas en el área de las operaciones de información. Del mismo modo, la Federación Rusa ha apoyado durante muchos años la creación de un acuerdo de "desarme" de armas de información altamente peligrosas[54]. Entiende que estas armas de información pueden tener "consecuencias devastadoras equiparables a las armas de destrucción masiva"[55]. También el Reino Unido ha declarado que un ciberataque que dejase sin operatividad una central eléctrica (ejemplo de infraestructura civil crítica) sería considerado un ataque armado[56]. Y finalmente, Estonia, tras sufrir ciberataques que bloquearon sus puertos navales, ejemplificó el suceso como un tipo de agresión

[52] Schmitt, M. N. (2013). *De Manual on The International Law applicable to Cyber Warfare,* p 47
[53] Roscini (2010), *World Wide Warfare- Jus ad bellum and the Use of Cyber Force*, p 105
[54] Markoff, J. (2014, 29 octubre). *At Internet Conference, Signs of Agreement Appear Between U.S. and Russia.* Recuperado 28 mayo, 2019, de https://www.nytimes.com/2010/04/16/science/16cyber.html
[55] JOHNSON, P.A (2002)., *Is it Time for a Treaty on Information Warfare*?, International Law Studies, vol. 76, p. 443 Recuperado de: https://digitalcommons.usnwc.edu/cgi/viewcontent.cgi?article=1382&context=ils
[56] Doward, J. (2017, 2 diciembre). Britain fends off flood of foreign cyber-attacks. Recuperado 28 mayo, 2019, de https://www.theguardian.com/technology/2010/mar/07/britain-fends-off-cyber-attacks

3. La atribución de los ciberataques

El proceso de atribución de un ataque a un ente es una tarea compleja. Implica la sincronización de elementos tanto políticos como jurídicos, pero su determinación es clave. De él y de su resultado depende la asignación de un hecho prohibido por el Derecho Internacional, a un autor, y consiguientemente, permite a la víctima tomar acción contra él. El ejercicio ya de por si es dificultoso en los ataques convencionales, como por ejemplo hemos podido ver en el caso de los ataques terroristas. Sin embargo, la tarea se dificulta aún más en el caso de los ciberataques. Para que éstos puedan activar el derecho a la legítima defensa, es crucial poder descifrar al autor de los hechos, pero en el ámbito informático las cosas se complican aún más. Concretamente, hay 3 características que hacen especialmente difícil la atribución en el ciberespacio[57].

La primera es el "anonimato": los atacantes pueden fácilmente esconder su identidad mediante programas informáticos o elementos técnicos. La segunda es que los ciberataques pueden no venir de un solo foco, sino ser dirigidos desde diferentes puntos (varios ordenadores en varios lugares distintos, tanto territoriales como jurisdiccionales). Esta segunda característica podemos ejemplificarla con el suceso ocurrido en 1998, año en el que un ciberataque (bautizado como "Solar Sunrise"), accedió al sistema del Departamento de Defensa de Estados Unidos de América. Este acto fue perpetuado por un adolescente israelí y algunos estudiantes californianos, a través de un ordenador localizado en Emiratos Árabes[58]. La tercera característica es la velocidad a la que un ciberataque puede materializarse.

Por lo tanto, la tarea a desempeñar es crítica, y no sólo implica trazar desde qué lugar proviene el ataque o el lugar donde está el ordenador, sino que incluye tener que identificar no sólo la persona que está detrás de la pantalla, sino detrás de la operación en sí. Dado el ámbito a tratar, altamente informatizado, la tarea a desempeñar conlleva además, un alto nivel de especialización tecnológica[59]. Respecto a estos elementos técnicos, debemos destacar la importante evolución que se ha producido de los mismos. Hoy en día tenemos mecanismos que nos permiten geolocalizar prácticamente cualquier dispositivo electrónico, sin embargo, también han mejorado los mecanismos que permiten mantener el secretismo de sus usuarios.

---

[57] Tsagourias, N. (2012), *Cyber attacks, self-defence and the problem of attribution*, Journal of Conflict and Security Law, Oxford University Press, p 5

[58] Shackelford, S. J, *From Nuclear War to Net War: analizing cyber attacks in International Law*, Berkeley Journal of International Law 27 (1), pp 204-231 Recuperado de: https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1368&context=bjil

[59] Tsagourias, N. (2012), *Cyber attacks, self-defence and the problem of attribution*, Journal of Conflict and Security Law, p 6

Figura 2: Cuadro sinóptico muestra de forma sintética el contenido de este segundo apartado.

Así pues, aunque la atribución por medios tecnológicos es importante, no siempre nos va a permitir obtener resultados territoriales precisos o informar sobre quién operó los instrumentos[60]. Por lo tanto, será necesario que el procedimiento de atribución se desempeñe junto con el resto de elementos legales y políticos, para así poder dar información completa a la hora de identificar a los autores, o sus vínculos con Estados[61]. Por ejemplo, el clima político imperante o a quien benefició el ataque pueden ser buenos indicadores también debemos tomar en consideración.

Sin embargo, antes de entrar en materia, debemos aclarar un último elemento que se complica. Y es el de obtención de pruebas concluyentes cobre las cuales se basan las asunciones[62] de las cuales determinaremos la atribución de los hechos. En este sentido el derecho internacional no ha aclarado qué estándares probatorios debe cumplir[63] el Estado víctima. Sólo existe un único límite, *que aquellas reclamaciones contra un estado que involucren cargos de gravedad excepcional deban probarse con evidencia que sea completamente concluyente. Lo mismo se aplica a la prueba de atribución de tales actos.*[64] Sin embrago, y como cabía de esperar, esto es aún más complicado en el ámbito cibernético. Es muy difícil encontrar rastro alguno de operaciones, o aun si se obtienen, éstas se truncan[65] dada la rapidez, el anonimato y la posibilidad de que haya varios Estados implicados. Por lo tanto, este estándar se debe matizar de acuerdo con la jurisprudencia de la Corte Internacional de Justicia, concretamente en el caso *Corfú.* Cuando la CIJ entendió que las dificultades de obtención de material probatorio derivaban del hecho de que este material se encontraba en el territorio de otro Estado, la Corte permite *un recurso más liberal en las interferencias a los hechos y en la evidencia circunstancial*[66]. Aun así, los estándares referentes a material probatorio están poco definidos, pero debemos recordar que pese seguir estándares más laxos que otros procedimientos convencionales (responsabilidad penal de un individuo, por ejemplo), un Estado no puede

[60] Bobert, W. E. (2010) *A Survey of Challenges in Attribution in Proceedings of a Workshop on Deterring Cyberattacks*, National Academic Press, pp 43- 48. Recuperado de: https://www.nap.edu/read/12997/chapter/5#43
[61] Reisman, W. M. Armstrong, A. (2006) *The past and the future of the Claim of preemptive self-defense*, Yale Law School Legal Scholarship Repository, p 525. Recuperado de: https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1998&context=fss_papers
[62] Tsagourias, N. (2012), Cyber attacks, self-defence and the problem of attribution, p 7
[63] CIJ (2003) Opinión disidente del juez Higgins en el caso Plataformas Petroleras (República islámica de Irán v Estados Unidos), p 161
[64] Caso referente a la *aplicación de la Convencion sobre el procedimiento y castigo del crimen de genocidio* (Bosina Herzegovina v serbia), ICJ Reparts 2007, p 209
[65] Tsagourias, N. (2012), Cyber attacks, self-defence and the problem of attribution, p 7
[66] Caso *Canal de Corfú* (Reino Unido v Albania), CJI Recueil 1949, p18

acogerse a su derecho de legítima defensa sin haber recopilado numeroso material basado en elementos tanto políticos, como legales y tecnológicos.

En los próximos apartados determinaré cómo podemos atribuir el ciberataque prohibido al país que lo ha realizado o tolerado, según las normas de responsabilidad de los Estados, y consecuentemente, conllevar la aplicación del *jus ad bellum*. Seguidamente procederé a responder la misma cuestión en el caso de que los ataques hayan sido desarrollados por actores no estatales como grupos o individuos[67].

3.1 Ciberataques realizados por un actor estatal

Si tras combinar elementos legales, políticos y tecnológicos podemos atribuirle un ciberataque a un Estado, el Estado víctima sólo podrá tomar acción contra éste en legítima defensa si, además, cumple con los estándares de atribución fijados por el derecho internacional. En base a esto, de la práctica internacional podemos extraer tres grandes criterios a seguir para saber si cabe o no atribuirle un ataque cibernético a otro Estado. El primero, serían aquellos ataques perpetuados por órganos de un Estado, los cuales le son atribuibles a él. En segundo lugar, los ataques realizados por agentes estatales también son atribuibles al Estado. Y por último aquellos ataques realizados por entidades no estatales, pero toleradas por un Estado, serán asimismo atribuidos a dicho Estado[68]. En los próximos apartados desarrollaré los dos primeros criterios, en los cuales los autores son entes estatales.

3.1.1 Órganos estatales

En este apartado se incluyen órganos estatales *de iure,* por ejemplo en el caso de que un militar miembro de las fuerzas armadas de un país cometea un ciberataque, el Estado deberá responder a las consecuencias que se deriven. También incluye entidades a las que se las dota, legalmente, de poder o autoridad gubernamental[69]. En este sentido, y para ejemplificar, sabemos que varios países han empezado a crear ciberunidades en sus ejércitos. Israel, por ejemplo, ha creado una base militar especializada en ciberataques para contrarrestarlos[70]. Asimismo, Alemania tiene su propia unidad de operaciones de inteligencia informática[71].

---

[67] Barnett, R. W. (2001) *A Diferent Kettle of fish: Computer Network Attack*, International Law Studies (76), p 22 Recuperado de: https://digitalcommons.usnwc.edu/cgi/viewcontent.cgi?article=1401&context=ils

[68] Nicholas Tsagourias (2012), Cyber attacks, self-defence and the problem of attribution, p 8

[69] Roscini Marco (2010), *World Wide Warfare jus ad bellum and the use of cyber force*, p 98

[70] Eshel, D. (2010) Israel adds cyberattacks to IDF, Recuperado en: www.military.com/features/0,15240,210486,00.html

[71] Goetz, J. (2009, 11 febrero). *War of the Future: National Defense in Cyberspace*. Recuperado 28 mayo, 2019, de https://www.spiegel.de/international/germany/war-of-the-future-national-defense-in-cyberspace-a-606987.html

Pero además, a esta categoría se le incluyen también órganos estatales de *facto,* es decir, entidades asimiladas o absorbidas en el aparato estatal de un país.[72] El elemento fundamental de estos órganos es que dependen completamente del Estado, además de que éste ejerce control sobre dicho órgano. Este requisito de "completa dependencia", fue introducido en el asunto *Nicaragua*. Sin embargo, hay varias líneas jurisprudenciales en lo que a control se refiere. Nicaragua[73] entendió que para que pueda serle atribuido a un Estado, el control debía ser efectivo, y no limitarse a financiar, organizar, entrenar o equipar las atacantes. Posteriormente, el Tribunal Penal Internacional para la Antigua Yugoslavia (TPIAY), concretamente en el procedimiento *Tadic*, habló de un grado de control "difuso" en el caso de estructuras organizadas. Posteriormente la CIJ, en el caso del Genocidio de Bosnia, volvió a reiterar un grado de control "alto" o "estricto"[74], volviendo pues al control efectivo. Por lo tanto, en el caso de que los actores presenten cierto margen de independencia, la entidad no se podría considerar órgano de facto del Estado, como pasó en el mencionado caso *Nicaragua.*

En todo caso, debemos entender que un nivel de control alto es necesario, porque *equiparar las actuaciones de personas a las realizadas por un órgano estatal cuando éstas no tienen tal cualidad a los efectos del derecho internacional, debe ser excepcional*[75].

3.1.2 Agentes Estatales

Segundo grupo de actores estatales. Los agentes estatales son entidades que actúan bajo las instrucciones, dirección, o control de un Estado[76], por lo que sus ataques serán atribuidos a dicho Estado. Por ejemplo, individuos o grupos de empresas contratados por Estados para realizar ciberataques[77]. Un caso bien conocido es el de la "Russian Business Network", una empresa de delitos informáticos que se sospecha que ejecutó los ataques cibernéticos contra Georgia[78].

Tanto las instrucciones como direcciones son de determinación clara, exigen una relación *ad hoc* entre la entidad que realiza el ataque y el Estado[79], por lo que deben ser probadas en cada

[72] Nicholas Tsagourias (2012), *Cyber attacks, self-defence and the problem of attribution*, p 8
[73] Caso *Actividades Militares y Paramilitares en Nicaragua*, p 111
[74] Caso *Aplicación de la convención para la prevención y la sanción del delito de genocidio*, p 227
[75] Ibid, p 393
[76] NU (2001) *Responsibility of States for Internationally Wrongful Acts*, Artículo 8. Recuperado de: http://legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdf
[77] Roscini Marco (2010), World Wide Warfare jus ad bellum and the use of cyber force, p 99
[78] CCDCOE (2008) *Cyber Attacks Against Georgia, Legal Lessons Identified*, p 11 Recuperado de: http://www.ismlab.usf.edu/isec/files/Georgia-Cyber-Attack-NATO-Aug-2008.pdf
[79] Nicholas Tsagourias (2012), Cyber attacks, self-defence and the problem of attribution, p 9

específico ciberataque[80]. Por ejemplo, en el caso de los diplomáticos norteamericanos retenidos en la embajada de Irán, la CIJ entendió que los militantes actuaban en nombre del Estado, puesto que fueron encomendados por un órgano específico del Estado iraní para llevar a cabo tal específica actuación[81]

Sin embargo, el criterio de determinación del elemento "control" es más problemático, ya que ha divergencias jurisprudenciales. Primero fue *Nicaragua*, el cual como ya hemos comentado anteriormente, introdujo el test del "control efectivo". La Corte entendió que podíamos hablar de control efectivo cuando el Estado haya tenido influencia directa en el grupo o persona que ha perpetrado el ataque[82]. Entonces, qué diferencia hay entre un ataque realizado por un agente estatal y un órgano *de facto*? La primera es que no hay ningún tipo de requerimiento de dependencia en el caso del agente estatal. Y la segunda, es que la necesidad de control se proclama en todas y cada una de las actuaciones realizadas por la entidad, mientras que en el caso de los órganos de facto tiene carácter general[83].

Sin embargo, el caso *Tadic* introdujo un estándar de control más bajo. Aquí, el TPIAY distinguió entre aquellos ataques que eran cometidos por individuos y grupos desorganizados, en los cuales el requisito de control efectivo sigue imperando. Y aquellos grupos con estructura jerarquizada y organizados, en los que simplemente se requiere "control general"[84]. En las propias palabras del Tribunal: *un Estado ejerce el control general sobre el grupo, no solo al equipar y financiar, sino también al coordinar o ayudar en la planificación general de su actividad (...) no es necesario que el Estado también emita (...) instrucciones para la comisión de actos específicos contrarios al derecho internacional.*[85] Por lo tanto, "control general" hace referencia a una influencia genérica al grupo y sus actividades. Por ejemplo, si un Estado provee de material técnico o de soporte a un grupo de hackers, y organiza sus actos, aunque no se involucre directamente en el ataque, puede serle atribuido. Posteriormente, el criterio de "control general" fue criticado por la CIJ en el caso del *Genocidio de Bosnia*, y entendió que el único criterio aplicable en materia de control es el de "control efectivo" creado en el caso *Nicaragua*.

[80] CIJ (2007) *Caso referente a la aplicación de la Convencion sobre el Procedimiento y Castigo del Crimen de Genocidio* (Bosina Herzegovina v Serbia), p 395
[81] Caso *Miembros consulares de Estados Unidos en Teheran* (USA v Iran), ICJ Reparts 1980, p 58
[82] Nicaragua case, 116 y 117
[83] Nicholas Tsagourias (2012), Cyber attacks, self-defence and the problem of attribution p 10
[84] Ibid p 10
[85] CIJ (2007) Caso referente a la *aplicación de la Convencion sobre el procedimiento y castigo del crimen de genocidio* (Bosina Herzegovina v serbia), p 398

Hay autores a favor de este punto de vista[86]. Entienden que al aplicar un estándar más estricto, se evitará que se atribuya frívolamente a los Estados como autores de ciberataques. Otros, entienden que aplicar un estándar tan rígido en los ciberataques no resultará útil, puesto que el nivel de control variará según el contexto en el que se desarrolle la operación. El TPIAY divergió del criterio general porque así lo consideró más beneficioso dadas las circunstancias del caso, ya que trataba principalmente sobre la caracterización del conflicto como internacional o no-internacional[87]. Por otro lado, la CIJ mantuvo el criterio de "control efectivo" para evitar dar a entender que los criterios de atribución deberían cambiar en caso de tener que determinar cuándo un Estado es responsable por actos de genocidio[88]. Ambos actos de atribución son de naturaleza completamente diferente, y es lógico entender que no es razonable aplicar el mismo criterio en ambos casos[89].

Así pues, las líneas a seguir no están demasiado marcadas. En todo caso debemos ceñirnos a lo estipulado anteriormente. Todo acto de atribución conllevará un importante desarrollo probatorio, incluido el control, ya sea genérico o efectivo. En todo caso, deberá probarse suficientemente, al menos como para constatar obligatoriamente una *conexión entre la conducta de los órganos de un estado y su responsabilidad internacional*[90].

3.2 Los ciberataques realizados por actores no estatales

Al inicio del apartado anterior destacamos tres factores para determinar si es posible atribuirle a un Estado la realización de un ciberataque. Los dos primeros criterios ya han sido analizados (órganos estatales y agentes estatales), pero tienen en común un mismo elemento: el actor, o *mastermind* del plan, es una persona o grupo vinculado con un Estado. Es en este tercer estándar que se introduce una nueva circunstancia: en este caso es un actor no estatal el que realiza el ciberataque.

En primer lugar, brevemente explicaré por medio de una tabla, qué clase de actores no estatales han tomado parte en ciberataques a lo largo de las últimas dos décadas.

---

[86] Roscini Marco (2010), *World Wide Warfare jus ad bellum and the use of cyber force*, p 100
[87] ICTY-94-1-A 1999 Fiscal v Dusko Tadic (apelación)
[88]CIJ (2007) Caso referente a *la aplicación de la Convencion sobre el procedimiento y castigo del crimen de genocidio* (Bosina Herzegovina v serbia), p 401
[89]Nicholas Tsagourias (2012), *Cyber attacks, self-defence and the problem of attribution* p 11
[90]CIJ (2007) Caso referente a la *aplicación de la Convencion sobre el procedimiento y castigo del crimen de genocidio* (Bosina Herzegovina v serbia), p 406

ACTOR	MOTIVACIÓN	OBJETIVO	FORMA DE ATAQUE
Ciudadanos de a pie	Ninguna (generalmente)	Cualquiera	Indirecta o pasiva
Script Kiddies	Curiosidad, emoción, ego	Individuos, compañías, gobiernos	*Scripts* y herramientas previamente escritas.
Hacktivists	Cambio político o social	Políticos o víctimas inocentes	Destrucción de páginas web o ataques por medio de DDoS
Black hat hackers	Ego, beneficio económico	Cualquiera	Programación maliciosa, virus…
White hat hackers	Idealismo, respeto por el derecho	Cualquiera	Pruebas de penetración, *patching*
Grey hat hackers	Ambiguo	Cualquiera	Variante
Hackers patriotas	Patriotismo	Adversarios de la nación	Ataques de DDoS, destrucción
Cyber insiders (internos)	Beneficio económico, venganza	Empleador (empresario contratante)	Ingeniería social, manipulación
Creadores de malware	Beneficio económico, ego	Cualquiera	Vulnerabilidad de los atacados
Timadores cibernéticos	Beneficio económico	Individuos y compañías pequeñas	Ingeniería social
Grupos criminales organizados	Beneficio económico	Individuos, compañías	Fraude por medio de *malware,* robo de identidad, DDoS para chantajear
Corporaciones	Beneficio económico	Sistemas basados en ICT e infraestructuras (privadas o públicas)	Variadas técnicas de ataque u operaciones de influencia
Espionaje	Beneficio político y económico	Individuos, compañías, gobiernos	Técnicas de contenido variado para obtener información
Milicias ciberneticas	Patriotismo, desarrollo profesional	Adversarios de la nación	Depende de las capacidades del grupo
Terroristas cibernéticos	Cambios políticos o sociales	Víctimas inocentes	Violencia informática basada en ataques o destrucción

Tabla 1. Ejemplos de clases de actores no estatales que han participado en ciberataques en las últimas dos décadas. Modificada de Sigholm, J. 2016. [91]

[91] Sigholm, J. (2016) , *Non state actors in cyberspace operations*, Swedish National Defence College, p 11

Los actores no estatales aquí mencionados, puede que ataquen a un Estado. En ese caso, podemos cuestionarnos si se le puede atribuir al Estado o Estados involucrados por su localización (lugar desde el que operan). En general, la respuesta es no. Si un actor no estatal ataca otro Estado, es el actor no estatal el objetivo directo de los actos realizados en legítima defensa[92], no el Estado desde el que han dirigido la actuación. Por lo que las respuestas defensivas deberán ir dirigidas contra dicho actor, sin poder afectar al país. Al fin y al cabo, en el proceso de atribución a un Estado de un acto prohibido por el Derecho Internacional, la definición de "Estado" es mucho más estrecha y limitada, por eso sólo incluye aquellos órganos o entidades que están fuertemente vinculadas a él.[93] Por otro lado, aunque el concepto de "uso de la fuerza" está fuertemente vinculado a la idea de "Estado", y los autores actúen desde uno, la CIJ ha subrayado en numerosas ocasiones que es importante *entender la realidad de la relación entre la persona que comete la acción y el Estado*[94]. Por lo tanto, siempre que el Estado ejerza un mínimo control sobre el actor, será suficiente para que el ataque le sea atribuido y la víctima pueda actuar contra él en consecuencia. Esta respuesta fue cristalizada en el asunto *Caroline*, en el que se entendió que un Estado puede utilizar la fuerza, justificado por medio de la legítima defensa, directamente contra un actor no estatal[95]. En este mismo sentido, la CIJ ha entendido que el artículo 51 de la CNU permite la legítima defensa ante un ataque armado, en nuestro caso un ataque cibernético, como consecuencia de unos hechos, no de un autor[96].

La práctica actual de los Estados nos permitiría confirmar este punto de vista. Por ejemplo, en 2006 Israel actuó en base a su legítima defensa estatal contra Hizbollah, en el Líbano, después de que el grupo atacase al país y sin que el Líbano pudiese prevenirlo[97]. Líbano admitió no tener conocimiento sobre los ataques y declaró no condonarlos[98]. Por su parte, Israel declaró que los ataques no eran contra el Estado del Líbano, sino contra el grupo terrorista. De este ejemplo se podría constatar, no sin opiniones alternativas, que cabe responder en legítima defensa

[92] Nicholas Tsagourias (2012), Cyber attacks, self-defence and the problem of attribution p 5
[93] Ibid p 12
[94] CIJ (2007) Caso referente a la *aplicación de la Convención sobre el Procedimiento y Castigo del Crimen de Genocidio* (Bosina Herzegovina v serbia), p 392
[95] Ibid p 392
[96] CIJ (2004), Opinión consultiva sobre *las consecuencias de la construcción de un muro en territorio palestino ocupado*, p 62. Recuperado de: https://www.dipublico.org/cij/doc/148R.pdf
[97] Recomendación 1310 del Consejo de Seguridad de las NU (2000), Capítulo VIII. *Examen de asuntos relacionados con la responsabilidad del Consejo de Seguridad de mantener la paz y la seguridad internacionales*, p 650 Recuperado de: https://www.un.org/es/sc/repertoire/20002003/Chapter%208/Middle%20East/0003_8_32_Situation%20in%20the%20Middle%20East_Spanish.pdf
[98] Carta del Representante Permanente del Libano en las NU dirigida al Presidente del Consejo de Seguridad (17 mayo 1982), Recuperado en: https://www.refworld.org/docid/3b00f17013.html

también cuando el Estado no puede ejercer su autoridad sobre la totalidad del territorio o sobre el grupo en cuestión (doctrina *unable or unwilling*).

No obstante, de esta regla general hay una sola excepción. En el caso de que el país tolere que se proyecten ciberataques desde su territorio, y no coopera con los Estados víctimas, a dicho Estado permisivo se le puede atribuir el ataque. Este era el tercer y último estándar que hemos presentado al inicio del apartado, también conocido como *The Harbouring Doctrine*, nacida de los atentados terroristas del 11S. En el ámbito cibernético, y por ejemplificar, este tipo de suceso se produjo en 2008, cuando la Federación Rusa toleró los ataques informáticos realizados por actores no estatales residentes en su territorio, tanto contra infraestructuras georgianas como estonias. Posteriormente Rusia tampoco colaboró con Estonia cuando ésta trataba de rastrear el autor material de los hechos. Además, las partes tenían un proyecto de tratado bilateral de Asistencia Legal Mutua que fue rechazado por la Fiscalía Suprema de Rusia[99].

Para proceder a la atribución de estos casos, se ha desarrollado un "estándar de tolerancia". Éste se entendió sobrepasado por ejemplo, en los atentados terroristas del 11S, cuando el régimen Talibán se negó a entregar los líderes de Al-Qaeda pese a las previas peticiones del Consejo de Seguridad de las NU. EEUU respondió declarando que no debía distinguirse entre aquellos que perpetúan un ataque y aquellos que lo acogen[100]. Esta posición fue acogida por el Consejo en las Resoluciones 1368 (2001) y 1373 (2001), los cuales reafirmaron el derecho individual o colectivo a defenderse ante ataques. Según el derecho internacional, un Estado no puede permitir que su territorio sea usado para actos contrarios a los derechos de otros Estados[101]. Si no cumple con el nivel de diligencia debido, el Estado incurre en responsabilidad estatal internacional[102]. El criterio de diligencia debida existe tanto para proteger intereses comunes, como la paz y la seguridad, como para a la vez reforzar ciertas obligaciones, entre ellas la prohibición al uso de la fuerza. Parece ilógico no permitir al Estado víctima defenderse contra un ataque armado que ha sufrido por la falta de diligencia de otro Estado.[103]

[99] CCDCOE (2008) *Cyber Attacks Against Georgia, Legal Lessons Identified*, p 13
[100] EEUU (2001) *Discurso presidencial a la nación Bush: No Distinction Between Attackers and Those Who Harbour Them*, Recuperado de: https://archive.defense.gov/news/newsarticle.aspx?id=44910
[101] CIJ, *Caso Canal de Corfú*, p 22
[102] Nicholas Tsagourias (2012), *Cyber attacks, self-defence and the problem of attribution*, p 14
[103] Ibid p 14

4. La respuesta frente a los ciberataques considerados ataques armados

En caso de que nos encontramos ante un ataque cibernético atribuible y equiparable a un ataque armado, nos encontramos ante una violación al artículo 2.4 de la CNU. Este apartado final identifica cuatro posibles respuestas que tiene el Estado víctima ante los perjuicios sufridos.

4.1 Consejo de Seguridad de las Naciones Unidas

Si el Estado es miembro de las Naciones Unidas puede recurrir al Consejo de Seguridad[104], haciendo uso del derecho que le otorga el artículo 35.1 de la CNU para tratar de resolver la disputa de forma pacífica. El Consejo, por su parte, recomendará al Estado todos los métodos apropiados para resolver la controversia[105]. Tal consejo se dará tomando en consideración todas las circunstancias fácticas del caso y ponderando todo procedimiento que las partes hayan adoptado para el arreglo de la controversia[106]. Si el Consejo de Seguridad considera que tanto la situación como el ataque constituyen una amenaza para la paz, quebrantamiento de la misma o un acto de agresión, y lo cualifica como tal, podrá ejercer los poderes que le confiere el Capítulo VII de la Carta. En este sentido y en referencia a los ciberataques, en 2006[107], el Departamento de Defensa (DoD) de Estados Unidos realizó una publicación considerando que *un ataque a la red de ordenadores que cause daños generalizados, perturbaciones económicas y pérdida de vidas podría precipitar la acción del Consejo de Seguridad.*

Las posibles acciones a tomar serán las siguientes. En primer lugar, podrá adoptar las medidas provisionales que juzgue necesarias, pero que no prejuzguen los derechos de las partes. Éstas simplemente tienen por objeto evitar que la situación empeore[108]. En segundo lugar, puede adoptar medidas que no impliquen el uso de la fuerza, como por ejemplo sanciones. No tienen carácter general, siendo su ámbito tanto material como subjetivo limitado. Concretamente, el artículo 41 prevé que dichas medidas *podrán comprender la interrupción total o parcial de las relaciones económicas y de las comunicaciones (…), así como la ruptura de relaciones diplomáticas*. Lo que en el ámbito informático se traduciría en un bloqueo cibernético al Estado responsable del ataque para prevenir su continuación o repetición[109].

---

[104] Roscini (2010), *World Wide Wrafare, Jus ad bellum and the Use of Cyber force*, p 110
[105] Art 36.1 de la CNU
[106] Art 36.2 de la CNU
[107] US *National Military Strategy for cyberspace operations* (2003), Department of Defence, p 15. Recuperado de: www.dod.gov/pubs/foi/ojcs/06-F-2105doc1.pdf
[108] Art 40 CNU
[109] Roscini (2010), *World Wide Wrafare, Jus ad bellum and the Use of Cyber force*, p 111

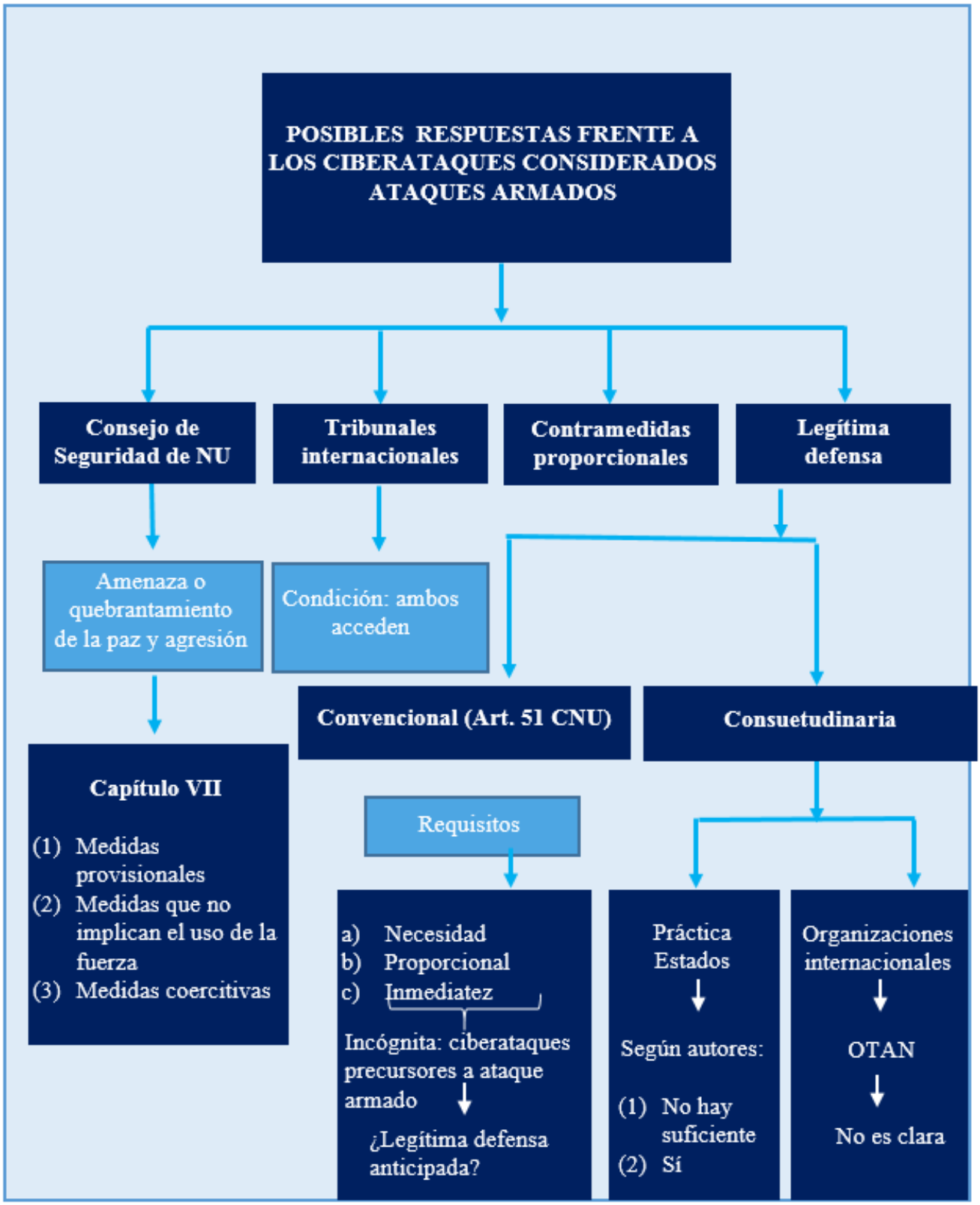

Figura 3. Cuadro sinóptico del desarrollo del capítulo.

Otra medida que no implica el uso de la fuerza sería la creación de un tribunal penal para el mantenimiento de la paz, a través de la teoría de los poderes implícitos. No se han dado casos en la práctica de los ciberataques, pero sería una posibilidad en el caso de que pretendiesen juzgar la responsabilidad criminal de Estados, individuos o actores no estatales. En este último caso, la "cláusula de liderazgo", que limita la responsabilidad penal a las personas que se encuentren *en una posición para ejercer efectivamente el control o dirigir la acción política o militar de un estado*[110], no excluiría enjuiciar a aquellos hackers que toman el control del sistema operativo de una país y lo utilizan para proyectar un ataque contra otro Estado[111]. Esta posibilidad ha sido considerada por varios expertos[112], pero en general, a fecha de hoy, parece algo arriesgada, dado que existe una prohibición de extensión por analogía en el derecho penal internacional[113].

La tercera opción a la que podría recurrir el Consejo de Seguridad, en caso de que las dos opciones anteriores no satisficiesen los objetivos, serían las medidas coercitivas que implican el uso de la fuerza *por medio de fuerzas aéreas, navales o terrestres, la acción que sea necesaria para mantener o restablecer la paz y la seguridad internacionales*[114]. Este es el tipo más gravoso. Un ejemplo serían las demostraciones o los bloqueos, ya sean autorizando a un Estado a realizarlos (más habitual), o imponiéndolos.

Fuera de estas tres acciones, un último recurso al que puede acceder el Consejo de Seguridad, junto con la Asamblea General, por medio de las Opiniones Consultivas de la CIJ, para que ésta pueda determinar la legalidad de los ciberataques, en consonancia con el artículo 96 de la Carta de las Naciones Unidas. Estas opiniones son discrecionales y no vinculantes, salvo que haya algún tratado que así lo disponga, pero pueden contribuir a la creación de una nueva regla de derecho internacional consuetudinario[115].

4.2 Tribunales Internacionales

Una segunda vía a la que puede acceder el país perjudicado sería la de someter la controversia a la jurisdicción de una Corte o Tribunal Internacional. Por ejemplo, la Corte Internacional de

[110] Ophard, J. A.(2010), *Cyber Warfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow's Battlefield,* 9 *D*uke *L*aw *& T*echnology *R*eview p 47
[111] Ibid p 47
[112] Ibid p 48
[113]Estatuto de Roma de la Corte Penal Internacional (1998), art 22 Recuperado de: https://www.un.org/spanish/law/icc/statute/spanish/rome_statute(s).pdf
[114] Art 42 CNU
[115] Ibid

Justicia puede otorgar a la víctima un derecho de reparación frente al país que ha infringido el artículo 2.4 y el principio de no intervención[116].

Sin embargo, esta vía presenta dos dificultades. La primera es la cuantificación de los daños causados por los ciberataques. ¿Cómo puede el tribunal medir el perjuicio causado cuando, en la mayoría de casos, las infraestructuras afectadas son confidenciales?[117] Hablamos, por ejemplo, de sistemas estatales de alto contenido privado. El segundo límite, es bien conocido, y es que la CIJ sólo podrá conocer del caso si ambos Estados acceden a someterse a su jurisdicción. Como el resto de tribunales internacionales, su competencia no es obligatoria. Además, aquí también sería de aplicación lo explicado en el apartado anterior sobre la responsabilidad criminal de individuos en los ataques cibernéticos. En este sentido simplemente recordar que tales actos también pueden ser enjuiciados por los tribunales internos de los países implicados[118].

4.3 Contramedidas

El Estado víctima tendría una tercera vía a la que acceder, las contramedidas no militares (no implican el uso de la fuerza) contra el atacante[119]. Las contramedidas consisten en incumplimiento de una obligación internacional que el Estado víctima tenía con el Estado atacante. Concretamente, hablamos de la adopción de medidas que en principio serían ilícitas (contrarias al derecho internacional), contra un Estado que previamente ha incumplido sus obligaciones internacionales, para inducir el cumplimiento de la obligación violada por el Estado atacante. Por lo tanto, no podría responder ante ciberoperaciones que el derecho internacional no considere ilícitas, como es el caso del ciberespionaje.

El único límite sustantivo que refiere a las contramedidas es el de la proporcionalidad[120]: que las consecuencias derivadas de la contramedida sean similares a las del ataque cibernético. Esto puede ser complicado de determinar en el ámbito informático, puesto que tal y como ya hemos comentado anteriormente, la cuantificación de los daños en el ciberespacio es dificultosa. El resto de limitaciones tienen carácter general y hacen referencia a la aplicación material de las contramedidas. Estas serían las condiciones de aplicabilidad[121], además de las contramedidas prohibidas (límite material): aquellas contramedidas que implican la amenaza o el uso de la

[116] Roscini (2010), *World Wide Wrafare, Jus ad bellum and the Use of Cyber force*, p 112
[117] CCDCOE (2008) *Cyber Attacks Against Georgia, legal lessons identified*, p 17
[118] Roscini (2010), *World Wide Wrafare, Jus ad bellum and the Use of Cyber force*, p 111
[119] Ophard, J. A.(2010), *Cyber Warfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow's Battlefield,* 9 Duke Law & Technology Review p 50
[120] NU (2001) *Responsibility of States for Internationally Wrongful Acts*, Artículo 22
[121] Ibid artículos 49, 51 y 52

fuerza, una violación grave de derechos fundamentales o la violación de obligaciones de carácter humanitario que prohíben las represalias, u otras normas de derecho internacional imperativo. En todo caso, el Estado que adopta las contramedidas no quedará exento de la obligación de respetar las normas de solución pacífica de controversias y las normas diplomáticas.

4.4. La legítima defensa

La legítima defensa, individual o colectiva, es la cuarta posible respuesta ante un ciberataque equiparable a un ataque armado, ya sea perpetrado por un actor estatal o no estatal. Esta es una institución clásica, de naturaleza tanto convencional como consuetudinaria.

Primeramente, conviene analizar su vertiente convencional, el artículo 51 de la Carta de las Naciones Unidas. Éste prevé el uso de la legítima defensa siempre que se cumplan ciertos requisitos: la respuesta debe ser necesaria, inmediata y proporcional al ataque.

Respecto al primer requisito, la necesidad, implica identificar el autor, verificar que el ciberataque no ha sido un accidente, y que no haya otra forma menos intrusiva de responder ante tal ataque[122]. Por ejemplo, evitar que los hackers accedan a las páginas web objetivo, por medio de sistemas informáticos de defensa. El mayor problema en este sentido, surge en el momento de identificar el agresor, puesto que como ya hemos constatado en apartados anteriores, debe enfrentarse al reto del anonimato. En este sentido, algunos autores[123] han llegado a opinar que *la ley debe permitir una respuesta activa basada en el objetivo del ataque, independientemente de la identidad del atacante.* Este punto de vista es ilógico y peligroso, puesto que si no se ha podido identificar el atacante, no se podrá determinar contra quién se dirigirá la legítima defensa. Esta vertiente ha sido rechazada por miembros de la comunidad internacional, entre ellos el Departamento de Defensa de los Estados Unidos[124].

El segundo requisito es la proporcionalidad de la medida. En el ámbito cibernético se complica, puesto que por ejemplo, el Estado víctima puede no ser suficientemente avanzado tecnológicamente como para poder responder proporcionalmente al ataque sufrido. A parte de este límite material que variará en cada Estado, se plantea la cuestión sobre si sería aplicable la doctrina de la "acumulación de eventos"[125]. Según esta, ciberataques realizados en menor escala

[122] Roscini (2010), *World Wide Wrafare, Jus ad bellum and the Use of Cyber force*, p, 119
[123] Hoisington M. (2009), *Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense*, 32 B.C. Int'l & Comp. L. Rev. 439, p 32. Recuperado de https://lawdigitalcommons.bc.edu/iclr/vol32/iss2/16
[124] United States DoD (1995), *An assesment of International legal Issues in Information Operations*, p 21 Recuperado de: http://www.au.af.mil/au/awc/awcgate/dod-io-legal/dod-io-legal.pdf
[125] Roscini (2010), World Wide Wrafare, Jus ad bellum and the Use of Cyber force, p 120

pueden considerarse uno a la hora de valorar la proporcionalidad de la respuesta[126]. Esta teoría ha sido utilizada en numerosas ocasiones por Estados Unidos e Israel, en casos respuesta a ataques terroristas, pero es controversial[127] La CIJ, en el caso *Plataformas Petroleras*, no lo rechazó expresamente, pero no lo consideró aplicable[128], por lo que dudaríamos a la hora de utilizarlo a la hora de cuantificar la respuesta a un ataque cibernético.

Finalmente, el último requisito es el de la inmediatez. La legítima defensa debe ser inmediata al ataque armado, reflejando así su verdadera naturaleza: la legítima defensa no pretende castigar al atacante, sino repeler el ataque armado[129]. No obstante, la aplicación de este criterio en el ámbito cibernético debe ser flexible. Por ejemplo, es posible que el ciberataque deje inoperativos los sistemas informáticos de defensa de un país, por lo que su respuesta no podrá ser inmediata. O bien, el daño puede aparecer mucho después del ataque, lo cual puede retrasar la respuesta estatal. Así pues, ante este último requisito aparecen algunas incógnitas. Por ejemplo, sería discutible si se puede actuar en legítima defensa ante un ciberataque no equiparable a un ataque armado, pero que es precursor de un verdadero ataque armado. Este suceso se dio en 2008, cuando justo antes de que fuerzas rusas invadieran Georgia, varios ciberataques apagaron páginas web estatales cruciales para la comunicación de las autoridades georgianas[130]. Jurisprudencialmente, la CIJ ha sido consciente de los intereses de protección de los Estados, y en el caso *Operaciones Armadas en el Territorio del Congo*, la Corte entendió que *el artículo 51 de la Carta puede justificar el uso de la fuerza en defensa propia solo dentro de los estrictos confines allí establecidos. No permite el uso de la fuerza por parte de un Estado para proteger intereses de seguridad percibidos más allá de estos parámetros*[131]. Por lo tanto, parece que la idea es descartada. Sin embargo, a nivel doctrinal autores como Marco Roscini[132], cuestionan tal respuesta, y lo harían depender según el grado de inmediatez del ataque armado. El artículo 32 de la *Convención de Viena sobre el Derecho Aplicable a los Tratados* nos indica que la interpretación de los requisitos del artículo 51 no puede ser manifiestamente absurda o poco razonable. Y según el mencionado autor, parece poco realista suponer que los Estados esperarán a que sucedan todos los acontecimientos antes de reaccionar. Si el peligro es

[126] Ibid p 120
[127] Zemanek K (2010), *Armed Attack* Max Planck Encyclopedia of Public International Law, p 7
[128] Caso *Plataformas Petroleras*, ICJ Reparts 2003 p 27. Recuperado de: https://www.dipublico.org/cij/doc/145.pdf
[129] Roscini (2010), *World Wide Wrafare, Jus ad bellum and the Use of Cyber force*, p 120
[130] CCDCOE (2008) *Cyberattacks Against Georgia, Legal Lessons Identified,* p 15
[131] Asunto *Actividades armadas en el territorio del Congo*, CIJ Recueil 2006 p 16. Recuperado de: https://www.dipublico.org/cij/doc/159.pdf
[132] Roscini (2010), *World Wide Wrafare, Jus ad bellum and the Use of Cyber force*, p 121

instantáneo, abrumador, y no permite otra opción ni un momento de deliberación, el Estado víctima debería poder invocar su derecho a la legítima defensa[133]. La misma opinión es compartida por Michael N. Schmitt, Concretamente, él introdujo tres factores a considerar para determinar si un Estado tiene derecho a responder anticipadamente a un ciberataque que no constituye un ataque armado. El primero (1) Si el ciberataque es parte de una operación mayor, que culminará en un ataque armado. (2) Si el ciberataque es un paso irrevocable antes de un inminente y probablemente inevitable ataque armado. (3) El Estado víctima está *reaccionando antes del ataque en sí mismo durante el última umbral de oportunidad disponible para contrarrestar efectivamente el ataque.*[134] Si estos 3 factores se cumplen, podríamos matizar este requisito de inmediatez. Concretamente, en el caso de los ciberataques, el carácter inminente *depende de la intensidad del ataque, el objetivo del ataque, el tiempo de reacción requerido para prevenir el ataque con éxito y la velocidad con la que el daño puede moverse a través de las redes informáticas*[135], puesto que la inminencia del ataque no depende sólo del facto tiempo, sino también de las circunstancias de cada caso. En todo caso, toda respuesta deberá ser proporcionada no sólo al ciberataque, sino a ataque en su conjunto, del cual el ciberataque es solo la primera parte[136].

Al principio del apartado mencionamos como la legítima defensa no es una institución creada por el derecho convencional, sino que ya existía con anterioridad a su plasmación en la CNU. Por lo tanto, existe la posibilidad de que la interpretación actual de la legítima defensa en el ámbito cibernético cambie como consecuencia de una práctica extensiva y uniforme. Algunos autores, como M N Schmitt, entienden que no hay suficiente *usus* en la materia, por lo que no hay derecho consuetudinario al que referirse[137]. Otros, como M Roscini, están en desacuerdo con esa corriente, al entender que *el paso de solo un corto período de tiempo no es necesariamente, o de por sí, un obstáculo para la formación de una nueva regla del derecho internacional consuetudinario*[138]. Por ejemplo, las normas consuetudinarias referentes al derecho aplicable en el espacio aéreo, aparecieron rápidamente a medida que los Estados actuaron como respuesta a la nueva situación. Además, este autor nos recuerda que dentro de

[133] Ibid ,p 122
[134] Schmitt, M. N. (2002). *Wired warfare: Computer network attack and jus in bello*, pp 932- 933.
[135] Joyner C y Lotrionete C, Joyner and Lotrionete, *information warfare as international coertion*, European Journal of International Law 12 (2001), p 860 Recuperado de: http://www.ejil.org/pdfs/12/5/1552.pdf

[136] Schmitt, M. N. (2002). *Wired warfare: Computer network attack and jus in bello*, p 933
[137] Schmitt, M. N., (2012) *The Law of Cyberwarfare: Quo vadis?,* p 281
[138] CIJ (1969), *Caso Plataforma Continental del mar del Norte*, p 103

"práctica estatal", se incluyen también otros actos verbales, no físicos, como *por ejemplo, declaraciones diplomáticas, declaraciones de política, comunicados de prensa, manuales oficiales, instrucciones para las fuerzas armadas, comentarios de gobiernos sobre proyectos de tratados, legislación, decisiones de tribunales nacionales y autoridades ejecutivas, alegatos ante tribunales internacionales, declaraciones en organizaciones internacionales y las resoluciones de esos órganos*[139].

En este sentido, diversos Estados han expresado sus puntos de vista a cerca de la legítima defensa como respuesta a los ciberataques. Estados Unidos[140], Reino Unido[141] y Rusia[142] se han mostrado favorables a la posibilidad de responder a ciberataques mediante el uso de la fuerza. Pero no es razonable pretender que a fecha de hoy todos los países se pronuncien a cerca de la cuestión. Sólo aquellos Estados afectados o con mayor poder e influencia dominan la cuestión[143]. Lo mismo ocurrió en su momento con el espacio exterior, cuando sólo dos países tenían la suficiente tecnología como para explotarlo, sus actuaciones facilitaron la creación de derecho consuetudinario[144]. En el caso de los ciberataques, sólo aquellos países que se han desarrollado militarmente en ámbitos informáticos pueden crear práctica estatal general aceptada como derecho consuetudinario, y parece que aquellos que cumplen con tal requisito entienden que es posible responder mediante la legítima defensa contra aquellos ciberataques que son equiparables a ataques armados.

Pero aparte de la práctica estatal, también debemos tomar en consideración los usos propios de las organizaciones internacionales, especialmente, la OTAN. La posición de la OTAN al respecto no es clara. En 2010, tras los ataques informáticos a Estonia, dicho Estado colaboró junto con la OTAN para crear un *Memorándum de Entendimiento* que facilita el intercambio de información y crea un mecanismo de asistencia en caso de ciberataque a uno de sus Estados miembros[145]. Otros países como Eslovaquia, Reino Unido o Estados Unidos, también han

---

[139] International Law Association (2000), *Committee on formation of customary (general) international law*, p 66. Recuperado de: https://www.law.umich.edu/facultyhome/drwcasebook/Documents/Documents/ILA%20Report%20on%20Formation%20of%20Customary%20International%20Law.pdf

[140] Sanger, D., & Bumiller, E. (2014, 9 septiembre). *Pentagon to Consider Cyberattacks Acts of War*. Recuperado de https://www.nytimes.com/2011/06/01/us/politics/01cyber.html

[141] UK Office of Cyber Security, (2009) *Cyber Security Strategy of the United Kingdom safety, security and resilience in cyber space,* Cabinet. Recuperado de: https://webarchive.nationalarchives.gov.uk/+/http:/www.cabinetoffice.gov.uk/media/216620/css0906.pdf

[142] Roscini (2010), *World Wide Wrafare, Jus ad bellum and the Use of Cyber force*, p 127

[143] Ibid, p 125

[144] Cassese A (2005), *International Law*, Oxford University Press (2), p 158

[145] NATO. (2010, 23 abril). *NATO and Estonia conclude agreement on cyber defence*. Recuperado de https://www.nato.int/cps/en/natolive/news_62894.htm

firmado acuerdos similares. Sin embargo, este acuerdo no hace mención alguna a la posibilidad de que un ciberataque pueda activar el deber de asistencia en legítima defensa colectiva, previsto en el artículo 5 del Tratado de la OTAN. Por lo tanto, la posición del grupo es algo vaga, quizás intencionalmente. En 2010, el informe que realizaron el Grupo de Expertos para la Nueva Estrategia de la OTAN, mantiene esta ambigüedad, según la cual se refieren a los ciberataques como "amenazas menos convencionales a la Alianza" las cuales pueden o no llegar al nivel de ataque previsto en el artículo 5[146]. Pero esta ambigüedad podría cambiar en el futuro, a medida que los ataques se convierten en más sofisticados. Después de todo, Estonia no consideró la aplicación del art 5 porque no superó el umbral del ataque armado, ya que fue una interrupción sin daños[147].

Por lo tanto, como conclusión acerca de la posibilidad de creación de una norma consuetudinaria en materia de legítima defensa como respuesta a un ciberataque equiparable a un ataque armado, la respuesta no es clara, puesto que la práctica estatal es incipiente y la práctica organizacional es vaga. Sólo la magnitud de los sucesos futuros determinará cómo reaccionará la comunidad internacional.

[146] NATO (2010): *NATO 2020: assured security; dynamic engagement*, p 9. Recuperado de: https://www.nato.int/strategic-concept/strategic-concept-report.html
[147] Shackelford, S. J, *From Nuclear War to Net War: analizing cyber attacks in International Law*, p 194

5. Conclusiones

Al iniciar este trabajo me propuse como objetivo estudiar la forma en la que los ciberataques han transformado el Derecho Internacional. La cuestión, de naturaleza transversal, ha sido un reto de difícil categorización, cuestionando los esquemas tradicionales del Derecho. Tales dificultades justifican la falta de unidad que presenta la comunidad internacional a la hora de enfrentarse al problema. Y esta falta de consenso ha sido característica determinante no sólo durante mi investigación, sino que también se ha visto reflejada en el propio resultado.

Aun así, he tratado de dar respuesta a las preguntas que me formulé al iniciarlo. Y para ello, el *Manual de Tallinn* fue uno de los pocos documentos legales que aportó cohesión en la materia. No sólo define los ciberataques en su artículo 51, sino que además, en conjunción con el artículo 2.4 de la CNU, establece una serie de factores que ayudan a los Estados a equiparar un ciberataque como un posible ataque armado. Este documento fue de gran ayuda para responder a las primeras hipótesis de mi trabajo, y debo agradecer a mi tutor, Ángel J Rodrigo Hernández, su recomendación de consulta. Las siguientes fases de mi trabajo se respondieron de forma más o menos precisa, según el grado de práctica internacional que presentasen. En general, todos los Estados están de acuerdo al afirmar que los ciberataques son uno de los mayores desafíos actuales. Consecuentemente, su atribución es necesaria, siempre que se pruebe extensamente y cumpla con los imprescindibles requisitos legales, políticos y tecnológicos. Un vez estos ciberataques equiparables a ataques armados son atribuidos, se abre la posibilidad de que los Estados víctimas puedan responder, ya sea mediante las UN, Cortes internacionales, contramedidas, o mediante la legítima defensa. Siendo este último medio de respuesta el más debatido y en el que menos práctica estatal unificada pude encontrar.

A nivel funcional, las implicaciones efectivas de este trabajo son importantes, pero inicipientes y su interpretación variará en los próximos años. Tal y como dijo Barak Obama en 2009 “So cyberspace is real. And so are the risks that come with it”[148]. Por ahora la comunidad internacional ha podido responder a los riesgos que la evolución tecnológica ha hecho surgir, pero sólo los futuros acontecimientos determinarán cuál será la posición definitiva de los actores internacionales. Como conclusión y recomendación a los futuros investigadores de esta materia, les recomendaría que sigan de cerca la actualidad política internacional, porque los ciberataques ya no son un acontecimiento futuro, sino nuestra nueva realidad.

[148] Obama, B. (2015, 20 enero). Text: Obama's Remarks on Cyber-Security. Recuperado 24 mayo, 2019, de https://www.nytimes.com/2009/05/29/us/politics/29obama.text.html

6. Bibliografía

- Rodrigo, A. J, & Casanovas, O. (2018). *Compendio de derecho internacional público* (7ª ed.). Madrid, España: Editorial Tecnos (Grupo Anaya).
- Rodrigo, A. J, & Casanovas, O. (2016). *Casos y textos de derecho internacional público* (7ª ed.). Madrid, España: Editorial Tecnos (Grupo Anaya).
- OOCDCE. (2017). *Manual de Tallinn 2.0 on the international law applicable to cyber operations* (2ª ed.). Cambridge, United Kingdom: Cambridge University Press.

7. Fuentes documentales

Artículos y Trabajos

- Instituto Español de Estudios Estratégicos & Instituto Universitario General Gutiérrez Mellado (2010), *Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio*, Cuaderno de estrategia nº 149, Capítulo IV.
- Tikk, E., Kasha, K., & Vihul, L. (2010). International Cyber Incidents: Legal Considerations. Cambridge, United Kingdom: Cambridge University Press
- Schmitt, M. N. (2013). *Manual on the International Law Applicable to Cyber Warfare* Cambridge University Press.
- Geers, K. (2007). *Cyberspace and the Changing Nature of Warfare,* Cambridge, United Kingdom: Cambridge University Press.
- Tikk, E. and Talihärm, A-M. (eds.) (2010), *International Cyber Security Legal & Policy Proceedings*, Tallinn: NATO CCDCOE.
- Schmitt, M. N. (2014). *The Law of Cyber Warfare: Quo Vadis?* Stanford Law & Policy Review, 37.
- Schmitt, M. N. (2012). *"Attack" as a Term of Art in International Law*: The Cyber Operations Context. Stanford Law & Policy Review.
- Schmitt, M. N. (2002). *Wired warfare: Computer network attack and jus in bello*. International Cometee of the Red Cross 25 (2).
- Norries, M. J. (2013). In brief: *The Law of Attack in Cyberspace: Considering the Tallinn Manual's Definition of 'Attack' in the Digital Battlespace*. Inquiries Journal, 10, (1).
- Schmitt, M. N. (2010). *Military Necessity and Humanity in International Humanitarian Law: Preserving the Delicate Balance.* Virginia Journal of International Law, 50 (4).

- Joint Chiefs of Staff. (1998). *Joint Publication 3-13 Information Operations*, United States Department of Defense.
- Schmitt, M. N. (2012b). *International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed*. Harvard International Law Journal, 54.
- Roscini, M. (2010), *World Wide Warfare- Jus Ad Bellum and The Use of Cyber Force,* Max Planck Yearbook of UN Law (14).
- Brownlie, I. (1963). *International Law and the Use of Force by States*. Oxford University Press.
- Foltz, A. C. (2012). *Stuxnet, Schmitt Analysis, and the Cyber "Use-of-Force" Debate*. National Defense University Press, (67).
- JOHNSON, P.A (2002)., *Is it Time for a Treaty on Information Warfare?*, International Law Studies, 76.
- Tsagourias, N. (2012), *Cyber attacks, self-defence and the problem of attribution*, Journal of Conflict and Security Law, Oxford University Press.
- Shackelford, S. J, *From Nuclear War to Net War: analizing cyber attacks in International Law*, Berkeley Journal of International Law 27 (1).
- Bobert, W. E. (2010) *A Survey of Challenges in Attribution in Proceedings of a Workshop on Deterring Cyberattacks*, National Academic Press.
- Reisman, W. M. Armstrong, A. (2006) *The past and the future of the Claim of preemptive self-defense*, Yale Law School Legal Scholarship Repository.
- Barnett, R. W. (2001) *A Diferent Kettle of fish: Computer Network Attack*, International Law Studies (76).
- CCDCOE (2008) *Cyber Attacks Against Georgia, Legal Lessons Identified,* NATO: CCDOE.
- Sigholm, J. (2016), *Non state actors in cyberspace operations*, Swedish National Defence College.
- Ophard, J. A.(2010), *Cyber Warfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow's Battlefield,* Du*ke L*aw *& T*echnology *R*eview, 9.
- Hoisington M. (2009), *Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense*, 32 B.C. Int'l & Comp. L. Rev. 439.

- Zemanek K (2010), *Armed Attack* Max Planck Encyclopedia of Public International Law, 7.
- Joyner C y Lotrionete C, Joyner and Lotrionete (2001), *Information Warfare as International Coertion*, European Journal of International Law, 12.

1

Páginas web

- The NATO Cooperative Cyber Defence Centre of Excellence**:** https://ccdcoe.org/
- Commentaries to Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I): https://ihl-databases.icrc.org/ihl/INTRO/470
- 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
- Convención de Viena Sobre el Derecho de los Tratados: https://www.oas.org/xxxivga/spanish/reference_docs/convencion_viena.pdf
- UN (1945) *Carta de las Naciones Unidas* **:** https://www.un.org/es/sections/un-charter/chapter-i/index.html
- Responsibility of States for Internationally Wrongful Acts: http://legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdf
- Estatuto de Roma de la Corte Penal Internacional (1998): https://www.un.org/spanish/law/icc/statute/spanish/rome_statute(s).pdf

Resoluciones de las Naciones Unidas

Identificación	**Fecha**	**Título**
A/RES/66/152	15 de julio de 2011	Developments in the Field of Information and Telecommunications in the

		Context of International Security
A/RES/33/14	3 de noviembre de 1978	Financiación de la Fuerza Provisional de las Naciones Unidas en el Líbano
A/RES/26/25	24 de octubre de 1970	Principios de derecho internacional referentes a las relaciones de Amistad y la cooperación entre los estados de conformidad con la Carta de las Naciones Unidas
S/RES/1368	12 de septiembre de 2001	Sobre las amenazas a la paz y la seguridad internacionales creadas por actos de terrorismo.
S/RES/1372	28 de septiembre de 2001	Sobre las amenazas a la paz y la seguridad internacionales creadas por actos de terrorismo.

8. Jurisprudencia

- Caso *Lotus*, CIJ, Recueil 1928.
- Asunto *Plataforma Continental del Mar del Norte*, ICJ Reparts 1969.
- Asunto *Actividades Militares y Paramilitares en Nicaragua*, ICJ Reparts 1986.
- Caso referente a la *aplicación de la Convencion sobre el procedimiento y castigo del crimen de genocidio*, ICJ Reparts 2007.
- Caso *Canal de Corfú,* CIJ Recueil 1949.
- Caso *Miembros consulares de Estados Unidos en Teheran*, ICJ Reparts 1980.
- Caso *Plataformas Petroleras*, ICJ Reparts 2003.
- Caso ICTY-94-1-A, *Fiscal v Dusko Tadic* (apelación), TPIAY 1999.

- Asunto *Actividades armadas en el territorio del Congo*, CIJ Recueil 2006.
- Opinión consultiva sobre *Legality of the threat or use of nuclear weapons, advisory opinion,* CIJ 1996.
- Opinión consultiva *sobre las consecuencias de la construcción de un muro en territorio palestino ocupado*, CIJ 2004.
- Opinión disidente del juez Higgins en el caso *Plataformas Petroleras,* CIJ 2003.