Hack Back en Costa Rica

Ciberseguridad Ofensiva: ¿Legítima Defensa?

Hack Back in Costa Rica

Offensive Cybersecurity: Legitimate Defense?

Luis Diego Flores Romero[1]

Recibido: 21/06/24 • Aceptado: 23/08/24

[1] Ingeniero en Sistemas con más de 15 años de experiencia en liderazgo de equipos de desarrollo, soporte técnico e infraestructura. Posee Maestrías en Gestión de Tecnología y Ciberseguridad, lo que le ha permitido desempeñarse en roles clave tanto en el ámbito académico como profesional. En el ámbito académico, ha sido profesor en la Universidad Autónoma de Centroamérica desde 2018, donde se enfoca en Redes y Telecomunicaciones y Sistemas Operativos. También ha impartido clases en la Universidad Latina de Costa Rica, especializándose en Gestión, Seguimiento y Control de Proyectos Informáticos. En su carrera profesional, ha desempeñado puestos gerenciales en el área de Tecnología para diversas empresas nacionales, donde ha sido responsable de la estrategia y operaciones TIC, implementación de proyectos tecnológicos y ciberseguridad. La formación académica incluye una Maestría en Ciberseguridad del Instituto Tecnológico de Costa Rica y una Maestría en Gestión de la Tecnología de la Universidad Fidélitas, además de una Licenciatura con énfasis en Administración de Recursos Tecnológicos de ULACIT y un Bachiller en Ciencias de la Computación de UMCA.
Correo: ldiego@floresit.net
ORCID:0009-0007-0195-1923
La elaboración de esta investigación fue realizada como parte de la maestría en Ciberseguridad del Instituto Tecnológico de Costa Rica en el año 2023.

Resumen: A medida que el panorama digital continúa evolucionando, también lo hacen las tácticas empleadas por los ciberdelincuentes. En respuesta a la creciente amenaza, ha surgido un concepto controvertido en el ámbito de la ciberdefensa: el hack-back. El hack-back se refiere a la acción retaliatoria tomada por entidades objetivo contra los atacantes cibernéticos, con el objetivo de interrumpir sus actividades, recopilar inteligencia o incluso lanzar contraataques.

Este artículo explora el concepto de hack-back en la ciberdefensa, discutiendo sus posibles beneficios y preocupaciones éticas. El hack-back se refiere a acciones retaliatorias tomadas por entidades objetivo contra los atacantes cibernéticos, con el objetivo de interrumpir sus actividades y recopilar inteligencia. Los defensores argumentan que el hack-back proporciona un enfoque proactivo para defender redes y activos, disuadiendo futuros ataques y promoviendo un entorno digital más seguro. Sin embargo, los críticos destacan los riesgos de las actividades cibernéticas ofensivas, incluyendo la escalada de conflictos, la identificación errónea de atacantes y los daños colaterales. La legalidad de las acciones de hack-back también es controvertida. Este artículo también aboga por una consideración cuidadosa de las implicaciones éticas, legales y prácticas, al tiempo que promueve un enfoque integral y colaborativo para combatir las amenazas cibernéticas.

La finalidad de esta investigación es analizar si la ciberdefensa activa, también conocida como Hack-back, puede ser considerada como un medio de defensa legítima frente a las agresiones cibernéticas en el contexto jurídico costarricense.

Palabras clave: Ciberdefensa, ciberseguridad, hack-back , defensa propia, infraestructura, redes, legítima defensa.

Abstract: As the digital landscape continues to evolve, so do the tactics employed by cybercriminals. In response to the growing threat, a controversial concept has emerged in the realm of cyber defense –. Hack-back refers to the retaliatory action taken by targeted entities against cyber attackers, aiming to disrupt their activities, gather intelligence, or even launch counter-attacks.

This article explores the concept of hack-back in cyber defense, discussing its potential benefits and ethical concerns and it . Hackback refers to retaliatory actions taken by targeted entities against cyber attackers, aiming to disrupt their activities and gather intelligence. Proponents argue that hack-back provides a proactive approach to defending networks and assets, deterring future attacks and promoting a safer digital environment. However, critics highlight the risks of offensive cyber activities, including escalation of conflicts, misidentification of attackers, and collateral damage. The legality of hack-back actions is also contentious. This article also advocates for careful consideration of ethical, legal, and practical implications while promoting a comprehensive and collaborative approach to combating cyber threats.

The purpose of this research is to analyze whether active cyber defense, also known as Hack-back, can be considered a legitimate means of defense against cyber attacks in the Costa Rican legal context.

Keywords: Cyber defense, cybersecurity, hack-back, self-defense, infrastructure, networks, legitimate defense.

INDICE

1. Introducción

En el contexto mundial se estima que casi el 90% de los activos corporativos son digitales lo que claramente indica que la información se encuentra en el ciberespacio.[2]

El mundo digital trae consigo grandes preocupaciones y muchos riesgos, los ciberataques han crecido de forma exponencial, Costa Rica no se ha escapado, el ciberataque del ransomware Conti a organismos gubernamentales de Costa Rica en abril de 2022 tuvo gran repercusión por el alcance y las consecuencias del incidente.[3]

Tanto la Unión Europea, la OTAN y el Senado de los Estados Unidos de América han venido a crear, desde sus perspectivas, una legislación para el uso de la técnica de *hack-back* como técnica de defensa.

La ejecución del *hack-back* se considera estrictamente ilegal en el contexto global, no obstante, en el transcurso de esta investigación se ha logrado determinar que existe un consenso general en cuanto a la posibilidad de considerar el *hack-back* como un mecanismo de legítima defensa, siempre y cuando se justifique la necesidad de responder a un ataque para evitar daños a un bien jurídico, pero para que la defensa emprendida sea justificada, es indispensable que se produzca una agresión ilegítima.[4] y que esta defensa vaya en consonancia con los principios de necesidad, de manera que se actúe bajo el supuesto de un peligro inminente; proporcionalidad, en el tanto no se exceda en la magnitud de la agresión e inmediatez en la respuesta defensiva, la cual define que la base fundamental para implementar una legítima ciberdefensa es que el ciberataque esté sucediendo simultáneamente o instantes previos al *hack-back*.[5]

¿Pero qué hace que este mecanismo de ciberdefensa sea altamente complejo?

El desarrollo de la investigación ha contribuido a respaldar que esta práctica de acceder de manera no autorizada a sistemas de terceros con el propósito de obtener información sensible, o causar daño, viola claramente las leyes y normativas establecidas en la mayoría de las jurisdicciones. Es claro que el acceso

[2] Internet Security Alliance. Manual de Supervisión de Riesgos Cibernéticos para Juntas Corporativas. 2017.
[3] Harán, M. "Detalles de cómo se produjo el ataque de Conti a organismos en Costa Rica." welivesecurity. July 22, 2022.
[4] Sinalevi. "Artículo 28: Legítima Defensa." Costa Rica, 1975.
[5] González, J. "Diálogos Punitivos." 22 Junio 2021.

no autorizado a sistemas informáticos está tipificado como un delito en muchos países, y conllevan sanciones desde multas hasta penas de prisión.

Adicional, viola los principios fundamentales de la ética y la integridad de la información en el plano digital, debe recordarse que la privacidad y la información son derechos fundamentales en nuestra sociedad, la obtención de estos sin el consentimiento no es aceptable y violan la privacidad de las personas y organizaciones, contribuyendo a generar un ambiente inseguro, de desconfianza, donde somos vulnerables.

A medida que los avances tecnológicos evolucionan, los desafíos por mantener un ecosistema digital seguro continúan, se hace cada vez más necesario que gobiernos y empresas trabajen en colaboración para atender los riesgos y colaborar en la detección y persecución de los delincuentes cibernéticos.

Para la elaboración de este artículo, se utilizó una metodología integral que combina varios enfoques. Primero, se realizó un análisis doctrinario para evaluar las contribuciones de autores reconocidos en el campo de la Ciberdefensa Activa/hack-back. Luego, se llevó a cabo una recopilación de aspectos legales para examinar la regulación de la Ciberdefensa Activa/hack-back a nivel general, con el fin de delimitar un marco jurídico y normativo aplicable en el contexto costarricense. Finalmente, se empleó un análisis deductivo para determinar la aplicabilidad de conceptos y estrategias del contexto físico al ciberespacio, evaluando similitudes y diferencias entre ambos entornos. Adicionalmente, se implementó una encuesta de diez preguntas para capturar las percepciones de expertos en áreas legales y técnicas.

2. Objetivos específicos de la investigación

1. Analizar la viabilidad del hack-back como mecanismo de legítima defensa en el contexto jurídico costarricense, evaluando si debe considerarse o no como una medida ante un incidente cibernético.
2. Investigar la complejidad de la atribución de ataques en el ciberespacio y sus implicaciones para la aplicación de la legítima defensa y el hack-back.
3. Determinar los principios aplicables del mundo físico al virtual en el contexto de la legítima defensa, con énfasis en la necesidad, inmediatez y proporcionalidad de las respuestas defensivas.
4. Determinar las implicaciones éticas y legales del hack-back en el ciberespacio.

3. Hipótesis

Las medidas de hack-back pueden ser aplicadas como legítima defensa contra agresiones cibernéticas en el contexto jurídico costarricense, siempre que se cumplan los principios de necesidad, inmediatez y proporcionalidad en el ámbito del ciberespacio.

4. Atribución cibernética

El reto de la atribución de los ciberataques es un desafío que se ha venido estudiando, revisando y analizando por especialistas geopolíticos, militares y académicos desde los años noventa[6] con el fin de comprender quién o quiénes son los que están detrás de estas operaciones, qué elementos se deben tener

[6] Cano, J. “Linkedin.” 3 Marzo 2022.

en cuenta, qué rastros hay que seguir, cómo se pueden perfilar, y claro está, sobre cómo es posible generar sanciones concretas y claras cuando es viable llegar a una atribución de un evento cibernético adverso.[7]

Así, por ejemplo, en 2018, durante los Juegos Olímpicos de Invierno en Pyeongchang, Corea del Sur, ocurrió el caso *Olympic Destroyer*, un ataque cibernético que buscaba interrumpir el evento. Este ataque, que utilizó un malware sofisticado para inutilizar sistemas informáticos, no ha sido atribuido de manera concluyente a ningún grupo o individuo específico.

Inicialmente, algunos expertos señalaron al grupo ruso APT28 (también conocido como Fancy Bear o Sofacy) como responsable. Sin embargo, surgieron informes contradictorios y especulaciones sobre la posibilidad de que el ataque fuera obra de otro grupo o incluso un acto de falsa bandera diseñado para desviar la atención de los verdaderos perpetradores.

El caso *Olympic Destroyer* destaca por su complejidad y por las dificultades en la atribución precisa de ciberataques, reflejando la naturaleza intrincada de la ciberseguridad moderna.

Tal y como se puede observar, los atacantes suelen utilizar técnicas avanzadas para ocultar su identidad y hacer que sea difícil rastrearlos con certeza.

Otro ejemplo de un caso más reciente que sigue sin resolverse es el ciberataque a la empresa SolarWinds en el 2020, que consistió en un sofisticado ataque a la cadena de suministro, donde atacantes respaldados por el gobierno ruso infiltraron malware en una actualización del software Orion de SolarWinds. Esta actualización infectada fue distribuida a unos 18,000 clientes, incluyendo agencias gubernamentales y grandes empresas, permitiendo a los atacantes espiar y robar datos durante varios meses antes de ser descubierto en diciembre de 2020. Este incidente subrayó la vulnerabilidad de las cadenas de suministro de software y la necesidad de mejorar la seguridad cibernética global.

Aunque han existido varias investigaciones y atribuciones realizadas por expertos en ciberseguridad y agencias de inteligencia, no se ha revelado públicamente una identificación definitiva de la parte responsable. El ataque mostró características comúnmente asociadas con operaciones cibernéticas respaldadas por el Estado, lo que llevó a especular que podría haber estado involucrado un Estado-nación. Sin embargo, la atribución específica sigue siendo incierta y la investigación está en curso, por lo que se mantiene como una de las grandes preguntas que aún siguen sin respuesta. Claramente ya se han apuntado algunos nombres, y se ha señalado a sospechosos habituales relacionados con Rusia, pero aún se está investigando incluso el propio vicepresidente de EEUU, Mike Pompeo, ha culpado directamente a los rusos de estar detrás de lo sucedido, pero De los Santos remarca que al día de hoy es difícil saber algo así a ciencia cierta. Es muy complicado porque es un trabajo muy cuidado y que no deja rastros.[8]

De acuerdo con el Informe Global de Riesgos 2020 del Foro Económico Mundial, la tasa de enjuiciamiento) en Los Estados Unidos es tan baja como el 0.05 por ciento. Esto confirma la complejidad y la carencia de recursos existente para poder contratacar cuando se identifica una amenaza, por ello, las empresas optan por acciones de carácter defensivo, y no ofensivo, tal y como lo expresa la siguiente frase: "somos mejores defendiendo y no tan buenos atacando".[9]

En resumen, la dificultad de probar la fuente de un ataque, conocido como el problema de la atribución, ha plagado la ciberseguridad prácticamente desde los inicios de internet. Los hackers suelen utilizar software seguro, como un servidor proxy, para ocultar su identidad y canalizar sus comunicaciones a través de muchos países diferentes con el fin de evadir la detección. Otras tecnologías como Tor y el cifrado les permiten añadir múltiples capas para enmascarar su identidad. La combinación de estas herramientas les permite cometer sus delitos sin ser detectados y en países donde saben que no pueden ser perseguidos.[10]

---

[7] Wheeler, D. A., and G. N. Larsen. "Techniques for Cyber Attack Attribution." 2003.
[8] Cid, G. "5 claves del 'hackeo' a SolarWinds: el ataque a un 'desconocido' que ha puesto en jaque a EEUU." El Confidencial, 22 Diciembre 2020.
[9] Torreblanca, J. I. Cybersecurity Summer Bootcamp. [Performance]. 2023.
[10] Mackay, J. "How Do Hackers Normally Get Caught." MetaCompliance. Julio 20, 2020.

Pero entonces ¿cómo pueden las organizaciones determinar la fuente de un ataque y tomar medidas apropiadas sin comprometer la seguridad de redes inocentes o provocar una escalada de conflictos internacionales?

Para responder esta pregunta se puede resaltar una caricatura del New Yorker de 1993 que presentaba dos perros conversando con el siguiente texto: “On the Internet, no one knows you’re a dog”, refiriéndose al hecho de que "En Internet, nadie sabe que eres un perro"[11], tal y como lo presentan podríamos afirmar que efectivamente es una verdad.

Desafortunadamente la capacidad de los atacantes para ocultar su identidad y desviar la atribución de responsabilidades es una preocupación creciente en el ámbito de las ciberamenazas. La falsificación de atribución dificulta la identificación de los verdaderos perpetradores, lo que plantea desafíos significativos para la respuesta y la seguridad cibernética en general. Abordar este problema requiere un enfoque multidisciplinario que combine la tecnología, la cooperación internacional y el fortalecimiento de los marcos legales para garantizar la identificación y persecución efectiva de los ciberdelincuentes.[12]

5. Legítima defensa en el ciberespacio

En el Derecho Internacional, la legítima defensa se basa en una respuesta del Estado frente a un uso de la fuerza en forma de ataque armado, (también calificado como uso mayor frente al uso menor de la fuerza), en los términos recogidos en el art. 51 de la Carta de las Naciones Unidas.

Para que la legítima defensa esté justificada no es suficiente con un mero uso de la fuerza menor, que sería el prohibido en el art. 2.4 de la Carta, sino que este debe alcanzar la gravedad suficiente, el grado máximo posible de uso de la fuerza; sin olvidar además la obligación del Estado de comunicar que está siendo víctima de un ataque armado.[13]

A diferencia del plano físico, se puede señalar que la soberanía se encuentra íntimamente ligada a la existencia de este espacio físico y es por ello por lo que en el ámbito del ciberespacio su aplicación no es tan clara.[14]

El ciberespacio se encuentra en todas y en ninguna parte al mismo tiempo; tal como lo señala (Zekos, 2007), el ciberespacio es un espacio amorfo que no ocupa un determinado lugar físico o geográfico. [15]

En Costa Rica, en relación con la Legítima Defensa, el Código Penal establece en su artículo 28:

“Artículo 28.-No comete delito el que obra en defensa de la persona o derechos, propios o ajenos, siempre que concurran las siguientes circunstancias:

a) Agresión ilegítima; y

b) Necesidad razonable de la defensa empleada para repeler o impedir la agresión.

Se entenderá que concurre esta causal de justificación para aquel que ejecutare actos violentos contra el individuo extraño que, sin derecho alguno y con peligro para los habitantes u ocupantes de la edificación o sus dependencias, se hallare dentro de ellas, cualquiera que sea el daño causado al intruso.”

(Así reformado por el artículo 1º de la ley Nº 5743 de 4 de agosto de 1975).

La legítima defensa, en todo caso, no puede ejercerse sin condiciones. El Derecho Internacional consuetudinario exige tres requisitos: necesidad, proporcionalidad e inmediatez.

---

[11] Shortland, N. “On the Internet, Nobody Knows You’re a Dog.” 2016.
[12] Pérez, I. “La legítima defensa del Estado frente a ataques cibernéticos según el derecho internacional.” Global Strategy, 28 Mayo 2021.
[13] Llorens, M. P. “Los desafíos del uso de la fuerza en el ciberespacio.” México, 2017.
[14] Zekos, G. “State Cyberspace Jurisdiction and Personal Cyberspace Jurisdiction.” 2007.
[15] Quesada, J. G. “La legítima defensa en el derecho penal costarricense.” 1989.

5.1 Necesidad

Cuando se hace referencia al principio de la necesidad, se establece que la acción de defensa es necesaria cuando puede esperarse con seguridad la conclusión inmediata del ataque y garantizar de la mejor manera la eliminación definitiva del peligro, lo que debe tenerse presente es que, entre varias posibilidades de defensa igualmente eficaces, debe elegirse aquella que causa el daño menor. Se puede interpretar entonces la necesidad como aquella conducta necesaria para evitar un daño inminente e ilegítimo, en otras palabras, cuando no hay otra forma razonable de evitar el daño.[16]

En cuanto a la aplicación de este requisito con el *hack-bac*k, uno de los mayores problemas que se puede plantear es sobre la existencia o no de un marco jurídico internacional que se pueda aplicar a la legítima defensa en estos casos. La mayoría de las dudas existentes vienen referidas a la identificación de un uso de la fuerza tradicional con un uso de la fuerza cibernética, ya que a primera vista las características del segundo parecen hacer intuir que no cabe referirse a un uso de la fuerza o ataque armado mediante el uso de medios cibernéticos. Asimismo, puesto que la mayoría de ataques son llevados a cabo por actores no estatales, podría parecer de nuevo que no existe relación entre estos actos y el derecho internacional. (Sierra, 2021), estando regulado el uso de la fuerza en los artículos 2.4. y 51 de la Carta. El principio internacional es el no uso de la fuerza en las relaciones internacionales, sin embargo, cabe una excepción: la legítima defensa. Si un estado es atacado, puede defenderse del ataque sufrido.

- Una operación cibernética constituye un uso de la fuerza cuando su escala y sus efectos son comparables a las operaciones no cibernéticas que se elevan al nivel de uso de la fuerza.
- Una ciberoperación, o una operación cibernética de amenaza, constituye un uso ilegítimo de fuerza amenazadora, y si se lleva a cabo, sería un uso ilegal de la fuerza,
- Una operación cibernética constituye un uso de la fuerza cuando su escala y sus efectos son comparables a las operaciones no cibernéticas que alcanzan el umbral del uso de la fuerza.

Una operación cibernética o ciberataque es un término utilizado para describir un conjunto de acciones llevadas a cabo en el ciberespacio con el objetivo de influir, perturbar o dañar sistemas de información o infraestructuras digitales. En el contexto de la seguridad internacional, ha habido debates en torno a la clasificación de las operaciones cibernéticas como un uso de la fuerza.

Los ciberataques son intentos no deseados de robar, exponer, alterar, inhabilitar o destruir información mediante el acceso no autorizado a los sistemas.[17]

De lo anterior se interpreta que una operación cibernética puede considerarse un uso de la fuerza si sus dimensiones y consecuencias son similares a las alcanzadas por operaciones no cibernéticas, lo que destaca que el ciberespacio es un ámbito en constante evolución y las operaciones cibernéticas pueden tener un alcance y efectos amplios. Por ejemplo, un ataque cibernético masivo que cause daños extensos a infraestructuras críticas, como los sistemas de energía o transporte, puede equipararse a una operación militar convencional en términos de sus implicaciones y consecuencias.

Se ha logrado determinar que una operación cibernética amenazante constituye un uso ilegítimo de la fuerza. Esto implica que, incluso si una operación cibernética no alcanza el umbral de uso de la fuerza, pero es percibida como una amenaza creíble de uso de la fuerza, se consideraría un acto ilegal, las operaciones cibernéticas pueden ser clasificadas como un uso de la fuerza cuando su magnitud y efectos son comparables a las operaciones no cibernéticas que alcanzan el umbral del uso de la fuerza. Asimismo, las operaciones cibernéticas amenazantes, incluso si no cumplen con el umbral del uso de la fuerza, son consideradas ilegítimas y potencialmente ilegales. La clasificación y la evaluación de las operaciones

[16] International Law Commission. “Articles on State Responsibility.” 10 Agosto 2001.
[17] IBM. “¿Qué es un ciberataque?” Julio 20, 2023.

cibernéticas como un uso de la fuerza continúan siendo temas importantes en el ámbito de la seguridad y el derecho internacionales.

5.2 Proporcionalidad

Este principio implica que las consecuencias derivadas de la contramedida sean similares a las del ataque cibernético.[18]

La racionalidad de la defensa legítima determina que se excluyen de la legítima defensa los casos de lesiones inusitadas o aberrantemente desproporcionados. Aquí podemos citar el clásico ejemplo una escopeta por parte de un paralítico que tiene sólo esta arma al alcance de su mano, no disponiendo de ningún otro recurso para impedir que un niño se apodere de una manzana. La defensa será antijurídica no porque el bien jurídico vida sea de superior jerarquía al bien jurídico propiedad, sino porque el orden jurídico no puede considerar conforme a derecho que para evitar una lesión de pequeña magnitud, se acuda a un medio enormemente lesivo como un disparo mortal de arma de fuego.[19]

De lo anterior se puede determinar que la acción de disparar es necesaria, porque no existe otra menos lesiva para evitar el resultado, pero no cumple el requisito de racionalidad. En este caso, el paralítico que mata al niño no abusa del derecho ni se excede en el ejercicio del derecho de legítima defensa, sino que actúa antijurídicamente.

(Iriarte, 2016) en su artículo "EEUU prepara un ciberataque "proporcional" como represalia contra Rusia"resalta que como repuesta ante un reciente hackeo realizado por Rusia al Comité Nacional del Partido Demócrata en el que realizaron importantes filtraciones, públicamente declara el diseño de una respuesta proporcional a las acciones recibidas.[20]

En síntesis, la proporcionalidad establece restricciones en cuanto a la magnitud, el alcance, el tiempo y la intensidad de la respuesta necesaria para detener una situación que motivó la legítima defensa. No se puede emplear una fuerza mayor a la necesaria para repeler el ataque; no puede existir una desproporción entre la agresión y la defensa. [20] (Yoo, C. "Cyber Espionage or Cyber War?: International Law, Domestic Law, and Self-Protective Measures." Pennsylvania, 2015.)

5.3 Inmediatez

Una vez que la necesidad es justificada y que la respuesta a ejecutar sea proporcional a la agresión recibida, queda por responder la pregunta: ¿Cuándo puede lanzarse un mecanismo de *hack-back* para repeler un ataque cibernético?

La interpretación mayoritaria de la Carta de Naciones Unidas[21] sostuvo que, para poder ejercerse conforme al Derecho Internacional, la legítima defensa precisa de un ataque armado (de cierta gravedad) *in actu* o, al menos, que hubiese ya sido lanzado. No se considera posible su invocación si el ataque armado no ha sido al menos iniciado (esto es, no se consideraba conforme a Derecho lo que en doctrina se denomina legítima defensa preventiva).[22]

---

[18] Incibe_. "Bot Informático Bloquea Citas Online de Extranjería Para Su Venta." Incibe, 12 Mayo 2023.
[19] Zaffaroni, E. R. Manual de Derecho Penal Parte General. Buenos Aires: Editora AR S.A., 2006, p. 476.
[20] Iriarte, D. "EEUU prepara un ciberataque proporcional como represalia contra Rusia." El Confidencial, 20 Octubre 2016.
[21] La Carta de las Naciones Unidas, el instrumento constitutivo de las Naciones Unidas fue firmada el 26 de Junio de 1945. La misma delinea los derechos y las obligaciones de los Estados Miembros, y además establece los órganos principales y procesos de las Naciones Unidas. La Carta es un tratado internacional que codifica los principios básicos de las relaciones internacionales que van desde la igualdad soberana de los Estados a la prohibición del uso de fuerza en cualquier forma inconsistente con los propósitos de las Naciones Unidas.
[22] Gutiérrez, C. De la Legítima Defensa en el Ciberespacio. Granada: Comares, 2020.

El ejercicio de la legítima defensa en el ciberespacio, no es aplicable ante un "supuesto", o como lo cita el texto como una "defensa anticipada" o "inminente", no podemos suponer que seremos víctimas de un ciberataque, por lo que rechazaría su aplicación en casos de amenazas "latentes".

Estos requisitos resultan de aplicación problemática en el ámbito cibernético, principalmente por la dificultad de identificar a los atacantes (atribución) y por la falta de regulación del derecho a la legítima ciberdefensa que establezca los principios de proporcionalidad y necesidad. Y todo ello, con la dificultad que supone definir el concepto de inmediatez; cuando en un ciberataque hay una alta probabilidad de que la detección sea posterior a cuando este se produjo o se inició.[23]

Se deben considerar diversos factores, por ejemplo, la cercanía temporal entre el ataque y la respuesta, el tiempo necesario para identificar al atacante y el tiempo necesario para preparar una respuesta adecuada, de acuerdo a estadísticas una empresa puede tardar hasta siete meses en detectar un ataque cibernético, dado que las organizaciones están utilizando técnicas obsoletas para identificar a los atacantes, según un análisis de la empresa de ciberseguridad Lumu Technologies.[24]

6. Daños colaterales

El trabajo de atacar a los hackers debería ser dejado en manos de las autoridades gubernamentales que están mejor equipadas para llevarlo a cabo. Se plantea la cuestión de cuál sería la implicación legal si, en el ejercicio de la legítima defensa, una persona debe intervenir en la infraestructura de un tercero. Es importante tener claro que uno de los aspectos más negativos de cualquier ciberataque justamente son sus consecuencias.

Kim Zetter, periodista de la revista Wired, investigó el caso de Stuxnet y concluyó que Estados Unidos creó este virus como una arma cibernética precisa y legalmente justificada. Stuxnet fue diseñado para causar solo el daño necesario para cumplir su objetivo, reflejando preocupaciones sobre las posibles repercusiones legales de su uso. Este enfoque sugiere que países como China o Rusia, que teóricamente no valoran tanto la legalidad de las acciones de sus gobiernos, no son los sospechosos más probables. Sin embargo, el gobierno de EE.UU. niega tener pruebas concluyentes sobre quién estuvo detrás del diseño de Stuxnet.

Stuxnet es un virus informático descubierto en 2010, utilizado para sabotear las centrifugadoras nucleares de Irán y ralentizar su programa nuclear. Este ataque cibernético es considerado uno de los más sofisticados y exitosos de la historia. Stuxnet se introdujo en los sistemas iraníes a través de una memoria USB infectada, cruzando así cualquier barrera de seguridad física. Una vez dentro, el virus se propagó por la red, Stuxnet estaba programado para atacar software industrial específico, como Siemens PCS 7, WinCC y STEP7, y los controladores lógicos programables (PLC) de Siemens S7.Cuando encontraba su objetivo, Stuxnet modificaba el código de los PLC, causando que las centrifugadoras giraran a velocidades peligrosas mientras mostraba lecturas normales a los operadores, alteraba las señales de los sensores para que los sistemas no detectaran comportamientos anómalos. Esto permitía que el gusano cambiara la velocidad de rotación de las centrifugadoras, causando su desgaste y eventual destrucción.

Evidentemente el Ejecutivo de EE.UU. niega que existan evidencias o pruebas concluyentes de quién pudo estar detrás del diseño de Stuxnet.[25]

Finalmente, tras años de sanciones por parte de la ONU, el 14 de julio de 2015, Irán y seis potencias internacionales lograron en Viena un acuerdo que limitaba el programa nuclear iraní a cambio de un levantamiento de las sanciones. Además de poner fin a décadas de desencuentros entre Washington y Teherán, el acuerdo puede reordenar los equilibrios geopolíticos de poder en una región sacudida por el terror extremista.

---

[23] Olmo, S., M. Rufián, P. Martín, and N. Gudiño. "Ciberdefensa nacional: responsabilidad público-privada compartida." Redseguridad, 17 Noviembre 2021.
[24] Semana. "¿Cuánto tiempo tarda una empresa en detectar un ataque cibernético?" Semana, 10 Setiembre 2020.
[25] Oliveira, L. "¿Qué es Stuxnet?" NordVPN, 2 Febrero 2023.

Debemos tomar en cuenta que según las leyes estadounidenses y algunas extranjeras "Una organización victimizada no debe intentar acceder, dañar o perjudicar otro sistema que pueda parecer estar involucrado en la intrusión o ataque. Independientemente del motivo, hacerlo es probablemente ilegal, y podría resultar en responsabilidad civil y / o penal". Además, muchas intrusiones y ataques se lanzan desde sistemas comprometidos. En consecuencia, "hackear de nuevo" puede dañar o perjudicar el sistema de otra víctima inocente en lugar de la del intruso.

Lo que hace que el *hack-back* sea probablemente ilegal es la Ley de Fraude y Abuso Informático[26]. El Título 18, Sección 1030 dice claramente que usar una computadora para entrometerse o robar algo de otra computadora es ilegal, no obstante si se intenta detener a un hacker dentro de tu propia red, está bien, pero en el momento en que abandona su red para hackear otra computadora, se está involucrado en una actividad ilegal.

(Pattison, From defence to offence: The ethics of private cybersecurity, 2019), en su artículo, establece que la «ciberdefensa activa» (ACD) comprende medidas que van más allá de la infraestructura o red del afectado. Eso implica varias de estas medidas defensivas activas, que no son perjudiciales, así como algunas medidas ofensivas que son perjudiciales o significativamente intrusivas. Las medidas ofensivas del ACD incluyen 'botnets[27] takedowns' (la desactivación de los sistemas de los atacantes infectados), entrando en la red para obtener información sobre ellos (como capturar una imagen a través de su cámara web), y la posibilidad (ciertamente más especulativa) de ransomware[28] de sombrero blanco (malware para cifrar archivos en sistemas de terceros que requieren que devuelvan información robada para recuperar el acceso) y misiones de rescate para recuperar información robada. Más ofensivo aún, y más allá de ACD, el *hack-back*. Esto implica la intención de interrumpir o destruir la red atacada, en lugar de simplemente para defenderse contra el ataque o para recuperar datos robados.

Por lo tanto, para recapitular, hay: (1) medidas pasivas que se limitan estrictamente a la red del defensor; : (1) medidas pasivas que se limitan estrictamente a la red del defensor; (2) medidas defensivas de ACD que no interrumpan la red de defensores; (3) ofensiva medidas de ACD que implican una interrupción o intrusión notable en la red del defensor para reparar el ataque; y (4) hack-back.

Es importante resaltar que las medidas cibernéticas ofensivas son particularmente preocupantes porque pueden causar daños colaterales a terceros o redes inocentes, o a aquellos erróneamente atribuidos como la fuente del ataque.

Se reitera que la aplicación del *hack-back* se mantiene estrictamente como una acción ilegal, así lo establece la Ley de Fraude y Abuso Informático de 1986, sin embargo, amparados en el concepto de la legítima defensa, ¿Qué ocurre cuando para responder a un ataque se deben vulnerar infraestructuras de terceros, mayormente críticas donde el impacto de la defensa pueda ocasionar daños proporcionales e incluso mayores a los ocasionados por el agresor inicial?

Este es un tema que continúa en espera de una respuesta, se ha resaltado que la falta de legislación sobre el tema repercute de forma importante en un potencial contrataque, en una reciente entrevista (K. Moraga, comunicación personal, 30 de mayo de 2023) comenta que la aplicación del *hack-back* depende del atacante y el threat model. Si el atacante es un actor de estado, en definitiva respondería con un *hack-back* , si es individual o una organización delictiva no. Por otro lado, también depende que esté defendiendo, si es una persona jurídica no lo estaría, si se está defendiendo personas físicas sí.

En resumen, la complejidad de la atribución en el ciberespacio y los posibles daños colaterales asociados al *hack-back* plantean desafíos éticos y prácticos. Antes de considerar esta opción, es esencial

[26] La Ley de Fraude y Abuso Informático (Computer Fraud and Abuse Act, CFAA) es una legislación de Estados Unidos que se encuentra en el Título 18, Sección 1030 del Código de los Estados Unidos. Esta ley fue promulgada en 1986 y ha sido enmendada varias veces desde entonces. Su objetivo principal es combatir el acceso no autorizado a computadoras y sistemas informáticos, así como el fraude relacionado con la informática.

[27] Un botnet es una red de computadoras o dispositivos infectados con malware y controlados por un atacante. Estos dispositivos, también llamados “bots” o “zombis”, pueden ser utilizados para llevar a cabo actividades maliciosas como ataques distribuidos de denegación de servicio (DDoS), envío de spam, robo de datos y otras formas de cibercrimen.

[28] El ransomware es un tipo de malware que cifra los datos de alto valor de una organización, como archivos, documentos e imágenes y, a continuación, exige un rescate a la empresa a fin de restaurar el acceso a esos datos.

evaluar cuidadosamente las implicaciones y las posibles repercusiones para garantizar que cualquier acción tomada en respuesta a un ataque cibernético sea efectiva, ética y proporcional.

Una vez analizados los tres principios aceptados por la doctrina y la jurisprudencia, se puede concluir que el *hack-back* plantea una cuestión de gran relevancia en el ámbito jurídico, ya que su aplicación puede implicar la violación de leyes y normas, así como generar serios debates éticos y de seguridad.

7. Metodología

Para la elaboración de este artículo, en primer lugar, se realizará un análisis doctrinario para evaluar las contribuciones de autores reconocidos en el tema de estudio. Este enfoque permitirá examinar las ideas y teorías existentes en el campo de la Ciberdefensa Activa/*hack-back*.

En segundo lugar, se llevará a cabo una recopilación de aspectos legales para examinar los elementos de regulación en relación con la Ciberdefensa Activa/*hack-back* a nivel general, esto con la finalidad de determinar y comprender el criterio de algunos expertos consultados sobre el tema, lo que permitirá delimitar un marco jurídico y normativo para comprender su aplicación en el contexto costarricense.

Por último, se empleará un análisis deductivo para determinar la aplicabilidad de las posibles aplicaciones del contexto físico en el ámbito del ciberespacio. Esto conlleva la identificación de similitudes y diferencias entre los entornos físicos y virtuales, lo que permitirá evaluar la viabilidad de trasladar conceptos y estrategias utilizados en el ámbito físico al ámbito cibernético.

En conjunto, esta metodología proporcionará un enfoque integral para abordar la investigación, combinando la revisión de la literatura, el análisis legal y la aplicación deductiva. A través de este enfoque, se espera obtener una comprensión más profunda de la Ciberdefensa Activa/*hack-back* y su aplicabilidad en el ciberespacio.

Adicionalmente, se desarrolló e implementó una encuesta de diez preguntas utilizando Microsoft Office Forms. La encuesta incluyó diez preguntas que capturaron las percepciones de las iniciativas de *hack-back* y las interpretaciones éticas. Por lo tanto, esta encuesta busca obtener comentarios de expertos tanto en áreas legales como técnicas.

Tabla 1: Análisis de Frecuencias
Preguntas realizadas a expertos

Pregunta	Respuestas	Frecuencias	Porcentaje	Porcentaje válido
Q1. ¿Considera jurídicamente correcto para un particular o empresa objeto de un ataque cibernético invocar su derecho de legítima defensa y ejecutar un *hack-back* como medida defensiva?	Sería jurídicamente correcto pues el derecho a la legítima defensa existe	6	75,0	75,0
	para ataques físicos	1	12,5	12,5
	No Hay Marco que regule esta Gestión	1	12,5	12,5
	No, no se puede asegurar ataque de vuelta orientado atacante real.	8	100,0	100,0
	Total			

Q2. En caso de un ataque, ¿qué tan anuente estaría en contratar los servicios de un tercero para responder mediante *hack-back* ?	Si es jurídica No	1	12,5	20,0
	No contrataría en ningún caso	4	50,0	80,0
	Total	5	62,5	100,0
	No se les aplicó la pregunta	3	37,5	
	Total	8	100,0	
Q3. ¿Podría interpretarse que un ciberataque que mate o lesione personas, cause daños físicos o suponga la destrucción de bienes de manera significativa justifica la invocación del derecho de legítima defensa mediante el *hack-back* ?	Legítima defensa aplica durante el ataque	4	50,0	50,0
		1	12,5	12,5
	No aplica en una posición de proveedor	1	12,5	12,5
		2	25,0	25,0
	Si aplica siempre y cuando no se cometan otros delitos	8	100,0	100,0
	No Aplica			
	Total			
Q4. ¿Cuál es el marco legal y las posibles consecuencias penales y civiles para particulares o empresas que realizan actividades de hackeo defensivo en respuesta a un ataque cibernético?	No existe regulación	3	37,5	37,5
	N/A	5	62,5	62,5
	Total	8	100,0	100,0
Q5. ¿Cómo se aplica el concepto de legítima defensa en el plano físico en comparación con su aplicación en el ciberespacio?	Si aplica si la acción defensiva ocurre durante el ataque	4	50,0	50,0
		1	12,5	12,5
	Debería regirse por acuerdos Internacionales	1	12,5	12,5
	No aplicaría debido a la complejidad de la atribución del ataque	2	25,0	25,0
		8	100,0	100,0
	Si aplica siempre y cuando no afecte ni amenace infraestructura de terceros			
	Total			

Q6. ¿Cuándo considera Ud. que es proporcional y razonable emplear un mecanismo de legítima defensa ante un ciberataque?	Aplica si el objetivo es una persona física	2	25,0	25,0
	Cuando los daños realizados son mayores y financiados por grupos organizados	1	12,5	12,5
	Cuando este en riesgo la información o la disponibilidad de los servicios.	2	25,0	25,0
	Aplica la legitima defensa siempre y cuando se cumpla el principio de que ningún individuo tiene que soportar lo injusto	1	12,5	12,5
	No lo ve adecuado en ningún caso	1	12,5	12,5
	Cuando se cuente con un respaldo legal o jurídico de nivel nacional e internacional	1	12,5	12,5
	Total	8	100,0	100,0
Q7. ¿Cuándo considera Ud. qué estamos antes una agresión ilegítima en el ciberespacio que justifique la defensa legítima?	Aplica si el objetivo son personas físicas	2	25,0	25,0
	Aplica cuando el nivel de impacto sea menor	1	12,5	12,5
	Se justifica cuando exista una amenaza inminente a la vida, integridad física	1	12,5	12,5
	Cuando el origen del ataque provenga de cualquier medio electrónico o medio de intrusión no autorizada	2	25,0	25,0
	Cuando el nivel de impacto sea Mayor	1	12,5	12,5
	No en ningún caso	1	12,5	12,5
	Total	8	100,0	100,0
Q8. ¿Cómo se determina si la respuesta defensiva en el ciberespacio fue necesaria para evitar un daño mayor?	No es posible predecirlo	3	37,5	37,5
	Aplica si se logra determinar que estamos ante un caso de agresión ilegítima	4	50,0	50,0
	Teniendo una política y plan de ciberseguridad empresarial	1	12,5	12,5
	Total	8	100,0	100,0

Q9. Usted es el encargado de la seguridad de un Data Center en el que "n" cantidad de clientes hacen uso de su infraestructura para su gestión operativa, lo que supone que contar con alta disponibilidad de los servicios es imperante. Si su equipo detecta un ataque directo a la infraestructura o puntualmente a los servidores de uno de sus clientes ¿Cuál es la postura del Data center ante la agresión cometida? ¿Podría aplicarse el *hack-back* como legítima defensa?	No aplica legítima defensa sino más bien acciones reactivas	4	50,0	80,0
	La aplicación de la legítima defensa estaría sujeta al cliente siendo yo el proveedor	1	12,5	20,0
	No se les aplicó la pregunta	3	37,5	
	Total	8	100,0	

Q10. En un escenario en el que el reciba una orden del Estado solicitando acceso a su infraestructura para detener un ataque cibernético ¿estaría en la disposición de colaborar?	Si, siempre y cuando la solicitud provenga de una entidad autorizada por Ley	4	50,0	80,0
	No es viable puede afectar infraestructura de un tercero, depende de condiciones de seguridad	1	12,5	20,0
	No se les aplicó la pregunta	3	37,5	
	Total	8	100,0	

8. Análisis de frecuencias

Se encontró una interesante variación de opiniones entre los participantes con respecto a si es correcto jurídicamente invocar una legítima defensa mediante el uso del *hack-back*, de los encuestados todos de nacionalidad costarricense, con perfiles varios, desde técnicos, juristas y expertos en áreas de criminología la mayoría expresó que está de acuerdo en casos en los que la defensa en situaciones de ataques físicos, sostienen que, en casos de agresión física directa, es válido y legítimo utilizar medidas defensivas para protegerse a sí mismos o a otros ante ataques de índole físico.

Por otro lado, otro grupo menor de los participantes adoptó una posición más cautelosa en cuanto a la invocación del derecho de legítima defensa, basados en la complejidad inherente a la atribución del origen

o la identificación precisa del agresor real en determinadas situaciones. Estos participantes argumentaron que, dada la dificultad de establecer de manera concluyente la culpabilidad del agresor, podría resultar problemático invocar el derecho de legítima defensa sin una evidencia clara y fehaciente.

De las respuestas obtenidas es importante resaltar la posición de que ambas partes, técnicas y legales concuerdan ampliamente en que el uso de *hack-back* puede ser invocado, (A.Chirino, comunicación personal, 20 de junio 2023), refuerza su criterio apegado al artículo 28 del código Penal que permite aplicar la legítima defensa para defender cualquier bien jurídico, incluidos los protegidos a través de las estipulaciones de los delitos informáticos, por lo que una reacción idéntica o proporcional a la del riesgo provocado podría avalarse a través de la figura de la legítima defensa, lo que sugiere la existencia de un debate y una discusión activa en torno a la aplicación del derecho de legítima defensa en situaciones de ataques. Mientras que una mayoría significativa considera su invocación como legítima y justificada, existe una minoría que aboga por un enfoque más precavido debido a las complejidades y desafíos que pueden surgir al determinar la responsabilidad y la identificación del agresor. Estos resultados resaltan la importancia de continuar el análisis y el diálogo en el ámbito jurídico para abordar estos temas y proporcionar orientación clara en situaciones donde el derecho de legítima defensa pueda ser invocado en el ciberespacio.

En relación a la contratación de un tercero como garante para responder mediante un *hack-back* se observa en su mayoría una inclinación negativa , específicamente asociada a la dificultad que representa lograr atribuir el origen del ciberataque. Por ejemplo, (H.Vargas, comunicación personal, 15 de junio de 2023), considera que es relativamente sencillo para un atacante suplantar “las huellas” para que parezca que el ataque provino de un tercero, mientras que (M. Jiménez, comunicación personal, 3 de junio de 2023), gerente de nube del Grupo Modular Avanzado, considera que bajo ninguna circunstancia contrataría los servicios de un tercero.

Es importante entender que en el contexto de la legítima defensa criminal, existe una figura que se denomina posición de garante. Se entiende por posición de garante aquellas personas que, de forma imperativa y jurídicamente obligatoria, asumen la prevención de un riesgo mediante el resguardo activo de los bienes jurídicos que les han sido confiados por otra persona. Todo aquel sobre el cual recae la obligación jurídica de impedir un resultado prohibido, asume la posición de garante. La obligación jurídica correspondiente es impedir, mediante una realización activa, que se produzca la lesión del bien jurídico en peligro.[29] Ejemplo de posiciones de garante son los guardaespaldas, los salvavidas, entre otros custodios. Para establecer una analogía de la posición del tercero garante en el plano físico en relación con el ciberespacio puede imaginarse el ciberespacio como una playa llena de personas disfrutando del mar y el sol. Aunque todos están allí para divertirse y relajarse, siempre existen posibles riesgos de que alguien necesite ser socorrido, justamente aquí es donde aparece la figura del tercer garante.

En este contexto, el tercer garante puede ser visto como el salvavidas en la playa. Al igual que un salvavidas, cuyo rol principal es estar atento y preparado para intervenir en caso de que surjan problemas o emergencias observando a la distancia; de forma proactiva y vigilante, en el ciberespacio, el tercer garante puede estar representado en la figura de las empresas que se dedican a garantizar la seguridad y la protección de los usuarios y sus datos, desde empresas de ciberseguridad que monitorean y previenen amenazas cibernéticas, así como proveedores de servicios que implementan medidas de seguridad para proteger la privacidad y la integridad de los datos de sus clientes.

Un ejemplo práctico de un tercer garante en el ciberespacio es un proveedor de servicios de correo electrónico que implementa medidas de seguridad, como cifrado de extremo a extremo, autenticación en

[29] Gullock, R. Fundamentos Teóricos Básicos del Delito de Omisión y su Aplicación en el Derecho Penal Costarricense. Heredia, 2008.

dos pasos y filtros antispam para proteger la información de sus usuarios de posibles amenazas cibernéticas.

Así como los salvavidas en la playa permiten que las personas disfruten del mar con tranquilidad, el tercer garante en el ciberespacio se preocupa por ofrecer un entorno más seguro y confiable para que los usuarios naveguen, interactúen y aprovechen las ventajas del mundo virtual sin temor a ser víctimas de delitos cibernéticos o violaciones de su privacidad.

En virtud de que la mayoría de encuestados no avalan la contratación de un tercero garante, pone en cuestionamiento si esta figura del Derecho Penal resulta aplicable o no en el ciberespacio. Tal y como se indicó, la no contratación de un tercero garante tiende a estar vinculada con la dificultad y/o complejidad que conlleva lograr identificar el autor de un ataque cibernético, lo cual en el ciberespacio está mayormente asociado a contratar servicios de protección, de tipo preventivo, reactivo y no ofensivo.

Cabe mencionar que, según (K. Moraga, comunicación personal, 30 de mayo de 2023) la invocación de la legítima defensa se justifica cuando el ataque afecta la vida o integridad de las personas. En este contexto, el uso del hack-back se considera justificado únicamente si se emplea durante el ataque y no después de que ha ocurrido, ya que en ese caso se convertiría en una venganza. (M. Jiménez, comunicación personal, 3 de junio de 2023) desde una posición de proveedor de servicios no aplicaría el uso de *hack-back* como mecanismo de defensa.

En lo que respecta a la existencia de un marco legal y las posibles implicaciones legales y civiles para individuos o empresas que llevan a cabo actividades de *hackeo* defensivo como respuesta a un ataque cibernético, la totalidad de los encuestados sostiene que no existe una regulación que permita abordar de manera adecuada la ciberdefensa a través del uso del *hack-back*. (A. Chirino, comunicación personal, 20 de junio de 2023) afirma que si es viable la aplicación del *hack-back* para impedir o repeler una agresión sobre todo ante graves afectaciones a la vida o la integridad corporal o ante la eventual afectación de bienes jurídicos patrimoniales importantes. Por su parte (R. Cordero, comunicación personal, 13 de mayo de (2023) respondió que la legítima defensa establece principios específicos para su aplicación: que exista una agresión ilegítima, una necesidad razonable y que sea empleada para repeler o impedir la agresión. Dentro de las acciones que se realicen no pueden cometerse otros delitos. Si la herramienta usada en el *hack-back* está diseñada y opera dentro de esos parámetros, se puede estar ante una justificación permitida por la normativa, sin embargo, aclara que ello no ha sido aún abordado por la jurisprudencia nacional.

Los hallazgos sugieren posibles y múltiples implicaciones y consideraciones legales y civiles. Algunas de estas sugieren que existe ambigüedad legal, al no existir claridad sobre qué acciones son legales y cuáles no lo son cuando se trata de responder un ciberataque. Sin directrices claras, las organizaciones o individuos que toman decisiones sobre aplicación de hackeos defensivos se encuentran en un terreno legal incierto, con posibilidades de enfrentar consecuencias imprevistas, incluyendo acciones criminales y civiles.

Así por ejemplo, se pueden presentar escenarios de errores de atribución y/o de escalada en el conflicto. Si se realiza una acción defensiva en respuesta a un ataque se corren riesgos de provocar una respuesta aún más agresiva por parte del atacante original. Si no es posible identificar el origen real del ataque, se podría estar tomando represalias contra un inocente.

Con relación a la aplicación del concepto de legítima defensa en el plano físico en relación al ciberespacio, los criterios son amplios y diversos. (K. Moraga, comunicación personal, 30 de mayo de 2023) sostiene que debe existir un correlación entre la agresión y el ataque; la legítima defensa debe ser aplicada desde la perspectiva de defensa y no como mecanismo ofensivo, resalta que la defensa debe suceder durante el ataque. Por su parte (H.Vargas, comunicación personal, 15 de junio de 2023) sugiere

la necesidad de apoyarse en tratados internacionales para poder justificar un ataque de esta naturaleza. se plantea que la única diferencia entre el plano físico del plano cibernético son los medios para ejercer la defensa, así como el carácter sutil e incruento de su ejercicio. En todos los demás aspectos, la legítima defensa guarda los mismos elementos en el plano físico y en el virtual (A. Chirino, comunicación personal, 20 de junio de 2023).

(R. Cordero, comunicación personal, 13 de mayo de 2023) sugiere que debe aplicarse por analogía. La agresión debe procurar algún daño, eso es fácilmente demostrable. El establecimiento de la necesidad puede puede encausarse si el *hack-back* es una línea secundaria de defensa, es decir, cuando ya hayan sido violentadas otras medidas. Debe ser suficientemente agresiva como para repeler o impedir la agresión, pero no para causar daños. Finalmente, debe poder garantizarse la identificación plena del responsable, de manera tal que no se afecte a terceros, no amenace otras infraestructuras y tenga total registro de la actividad con fines forenses.

En cuanto a la proporcionalidad y razonabilidad del uso del *hack-back* como legítima defensa los entrevistados concuerdan en que es proporcional y razonable cuando los daños afectan infraestructuras físicas o existan peligros que atenten contra vidas humanas y se considera que el *hack-back* es permitido siempre y cuando la agresión implique una afectación de tal nivel que habilite el principio de que nadie tiene que soportar lo injusto, y frente a una situación límite, donde lo único que pueda emplearse es un mecanismo de *hack-back* que permita establecer una racionalidad del medio empleado. (H. Segura, comunicación personal, 18 de junio de 2023), no visualiza ningún caso en que sea adecuada la aplicación de un mecanismo de legítima defensa ante un ciberataque. Estas diferencias de criterio jurídico refuerzan la necesidad de un marco legal apropiado para el *hack-back*.

Asimismo, en relación a la necesidad de adoptar medidas defensivas en el ciberespacio con el fin de evitar daños significativos, los resultados obtenidos revelan que los participantes consideran que la respuesta defensiva es apropiada siempre y cuando se pueda determinar de manera concluyente que se está frente a un caso de agresión ilegítima.

En el ámbito del ciberespacio, la adopción de medidas defensivas para prevenir daños significativos es crucial. Según los resultados obtenidos, se considera apropiada una respuesta defensiva siempre que se pueda concluir que se enfrenta a una agresión ilegítima. En este sentido, existe un consenso general en torno a la justificación de la legítima defensa para proteger bienes o evitar un inminente daño. Sin embargo, también es importante reflexionar sobre situaciones más complejas, como los riesgos que podrían surgir en el futuro con vehículos autónomos. ¿Qué sucedería si los llamados "crackers" lograran modificar a distancia el software de un vehículo, poniendo en peligro vidas humanas? Con la expectativa de que para el año 2030 haya más de 700 millones de vehículos conectados circulando, la industria está trabajando para salvaguardarlos de ciberataques y asegurar que no se conviertan en un objetivo vulnerable. La protección en el ciberespacio sigue siendo una cuestión de suma importancia y atención en el desarrollo tecnológico.[30]

Claramente a medida que la conectividad se incrementa, se amplia también la exposición de los sistemas a posibles intrusos malintencionados que busquen violar la seguridad de la conducción autónoma, por ende, se hace imperante tomar acciones para la detección y contención de amenazas que le permitan a los usuarios conducir en entornos seguros. Lo que obliga a revisar temas asociados a cuáles son las implicaciones legales en el caso de un hackeo de un vehículo, y de quien será la responsabilidad.

En este sentido, debe enfatizarse en la importancia de adoptar enfoques proactivos de seguridad, que incluyan medidas preventivas y la implementación de estrategias sólidas para mitigar los riesgos asociados

[30] Blázquez, L. “Ciberataques a coches: precauciones.” Coches.com, 30 Mayo 2022.

a los ciberataques. En resumen, este grupo de entrevistados sostiene que la incertidumbre inherente a los ciberataques hace que su predicción sea impracticable, y abogan por una combinación de enfoques de seguridad que abarquen tanto la prevención como la respuesta adecuada para minimizar los daños potenciales.

Sobre el tema, algunos opinan que solo se debería recurrir a medidas defensivas si la organización cuenta con políticas y planes formales de ciberseguridad, adoptar estrategias en las que se fortalezca una postura defensiva debe prevalecer antes que la ofensiva, reforzando esquemas de recuperación, con tiempos mínimos que permitan recuperar garantizar la continuidad operativa de negocio y no entrar en una confrontación para intentar repeler una agresión en el ciberespacio. Los ataques cada vez se vuelven más sofisticados, deben reforzarse las barreras defensivas contra vectores de ataque y adoptar tecnologías que respondan automáticamente a los ataques, que permitan ralentizar al atacante y ganar tiempo para que los defensores puedan responder.

¿Pero qué ocurre cuando el escenario es que el encargado de un centro de datos detecta y debe enfrentarse a un ataque contra uno de sus clientes?, surge la interrogante sobre la postura que se tomaría frente a este incidente.

La mayoría de los entrevistados indicó que optaría por adoptar acciones reactivas en respuesta al ataque, enfocándose en defenderse de manera proactiva y mitigar los daños, pero descartando la aplicación de mecanismos de *hack-back* como forma de legítima defensa. Por otro lado, el porcentaje restante considera que en su rol de proveedor de servicios, delegaría la responsabilidad en sus clientes y se ajustaría a las decisiones que estos tomen en relación con el incidente, (M. Jiménez, comunicación personal, 3 de junio de 2023), señala que un centro de datos y en general un proveedor de servicios es un "protector" de los intereses de sus clientes, tal y como lo comenta la posición del data center es bloquear los accesos por donde se detectan los ataques, como proveedor de servicios neutrales, resalta que la empresa se esfuerza por ayudar a sus clientes en caso de cualquier eventualidad, incluyendo posibles incidentes de seguridad cibernética, para lo que cuentan con esquemas de respaldo y servicios de ciberseguridad diseñados para asistir a los clientes en su proceso de recuperación y proteger su información y sistemas ante posibles ataques o vulnerabilidades. Asimismo, (H. Vargas, comunicación personal, 15 de junio de 2023) sugiere que lo adecuado sería notificar al cliente afectado para que sea la organización la que decida cómo proceder, sin embargo, no siempre es sencillo, fundalmentalmente porque una acción de este tipo requiere de una atribución indudable del atacante, lo cual puede ser incierto. Además, es altamente probable que en la mayoría de los casos los atacantes tengan mayores capacidades técnicas que sus víctimas, por lo que podrían desencadenarse ataques más agresivos. Las labores de hackeo deben dejarse a los especialistas, no hacerlo así puede causar riesgos extensos e innecesarios.

Estos resultados reflejan una tendencia mayoritaria hacia una estrategia de defensa reactiva y colaborativa, donde el enfoque principal radica en proteger la infraestructura y los intereses de los clientes sin recurrir a tácticas ofensivas que en base a los criterios recopilados, es comprensible la postura que adoptan los entrevistados, son muchos los desafíos asociados a la complejidad de atribuir los ataques y a las importantes implicaciones éticas y legales que se involucran. La aplicación de medidas ofensivas en respuesta a ciberataques podría acarrear costos significativos en escenarios de defensa activa.

Debe resaltarse que en relación a la disposición de colaborar con el Estado en caso de un evento, los criterios varían. Mientras algunos consideran que es posible la colaboración siempre que exista una solicitud formal emitida por una entidad autorizada según la legislación costarricense, otros consideran que esta colaboración no sería factible, ya que implicaría una posible violación a la infraestructura de terceros.

Esta colaboración debe darse en varias vías. Sin voluntad política, difícilmente los ciudadanos se van a poder establecer medidas y lineamientos que permitan fortalecer la ciberseguridad en el país. Por ello, para lograr reforzar la confianza digital, elevar la ciberseguridad y la resiliencia se necesita del apoyo del gobierno y el sector tanto público como privado, por lo resulta fundamental contar con canales de comunicación ágiles y efectivos que le permitan a la ciudadanía denunciar incidentes, y que estos incidentes escalen y sean atendidos adecuadamente por las entidades respectivas.

9. Conclusiones

Estos hallazgos muestran la diversidad de opiniones y perspectivas existentes en cuanto a la aplicación de la legítima defensa y el *hack-back* en situaciones de ataques físicos y cibernéticos. Los resultados destacan la importancia de continuar el debate y el análisis en el ámbito académico y jurídico para abordar estas cuestiones de manera más precisa y proporcionar orientación clara en situaciones donde se pueda invocar el derecho de legítima defensa. Además, subrayan la necesidad de contar con marcos legales adecuados que regulen las acciones defensivas en el ciberespacio, considerando tanto la proporcionalidad y razonabilidad de dichas respuestas como los posibles impactos éticos y legales.

La variedad de opiniones permite reforzar que el uso del *hack-back* no es un mecanismo de defensa que deba considerarse como el primer medio ante un incidente cibernético. El uso de mecanismos de prevención y defensa mediante el uso de la tecnología para protegerse ante las amenazas avanzadas debe prevalecer como parte del arsenal de defensa en nuestras organizaciones; una acción desmedida podría desencadenar consecuencias terribles que a largo plazo podrían representar pérdidas mayores para la organización.

Durante la investigación y formulación de este artículo se ha logrado reiterar en numerosas ocasiones que la atribución de un ataque en el ciberespacio presenta un alto grado de complejidad que no es equivalente al que encontramos en el plano físico, donde lograr determinar quien realizó un ataque está delimitado por la presencia física y las pruebas tangibles. En el ciberespacio, la identificación precisa del agresor y la atribución de responsabilidad son desafíos significativos debido a la naturaleza abstracta y enmascarada de las actividades cibernéticas. Esta dificultad para establecer de manera concluyente la autoría de un ataque plantea interrogantes sobre la aplicación de la legítima defensa y el *hack-back* en el ámbito digital.

De forma general, los principios que aplican para el mundo físico si aplican en el mundo virtual, pero parecen estar condicionados a la existencia de legislación y claridad sobre las posibles implicaciones y consideraciones legales y civiles, que presenta nuestra jurisprudencia.

En relación a la necesidad, por ejemplo, la aplicación del *hack-back* no puede ser ejecutada sin la presencia de una amenaza actual o inminente, o derivada de una sospecha solamente.

En relación a la inmediatez, la base fundamental para aplicar medidas de ciberdefensa es que el ciberataque esté sucediendo en el momento mismo o instantes previos al que se aplica el *hack-back*, caso contrario podría estarse aplicando una especie de “venganza personal” al momento de implementar la ciberdefensa.

En relación a la proporcionalidad del ciberataque, resulta más difícil determinar en el ciberespacio en comparación con el plano físico. Esto se debe a que se vuelve un asunto técnico que requiere que alguien pueda determinar si el uso de la fuerza en el contrataque es acorde al ataque recibido.

En relación a la atribución, en un sentido práctico, existe una dificultad real para rastrear de manera precisa la fuente exacta de origen de un ciberataque. Para determinar si el *hack-back* es una medida legítima de defensa, es necesario establecer una analogía entre el mundo físico y el virtual, teniendo en cuenta los principios relacionados con necesidad, inmediatez y proporcionalidad.

El campo de acción en el ciberespacio como un entorno global e interconectado, donde los ataques pueden originarse en cualquier parte del mundo y traspasar las fronteras nacionales le añade otra capa de complejidad a la atribución y a la respuesta defensiva, ya que las jurisdicciones y los marcos legales pueden variar ampliamente entre países.

Es evidente que para abordar de forma apropiada un incidente cibernético debemos emplear un enfoque multidisciplinario, donde participen gobiernos, organizaciones internacionales, expertos en materia de seguridad informática y protección de datos, entre otros profesionales, que contribuyan al desarrollo de marcos legales y normativos que permitan delimitar y establecer regulaciones sobre el uso de la legítima defensa en el ciberespacio como mecanismo activo de protección.

No podemos dejar de mencionar la importancia e imperante necesidad de continuar reforzando la conciencia y la educación sobre la importancia de la ciberseguridad y el uso de las plataformas digitales. La prevención temprana y los mecanismos adecuados para atender un incidente cibernético continúan siendo elementos claves para mitigar riesgos y minimizar los daños derivados de un ataque.

En conclusión, la aplicación de la legítima defensa y el *hack-back* en el ciberespacio plantea desafíos significativos debido a la dificultad de atribuir los ataques y a las implicaciones éticas y legales involucradas. Es fundamental seguir investigando y debatiendo sobre este tema para desarrollar marcos legales claros y orientaciones precisas que promuevan una respuesta defensiva proporcional y razonable en el ámbito digital. La colaboración entre diferentes actores y disciplinas resulta crucial para abordar de manera efectiva los desafíos de la ciberdefensa y garantizar la seguridad y la integridad de los sistemas digitales.

10. Bibliografía

Gerke, Kristina (2021). Canadian hack-back?: A consideration of the canadian legal framework for private-sector active cyber defence.

Álvarez Rodríguez, I. (2019). El Derecho del ciberespacio. Una aproximación. *IDP: Revista de Internet, Derecho y Política*, (30). https://www.researchgate.net/publication/339640455_El_Derecho_del_ciberespacio_Una_aproximacion

Álvarez Rodríguez, I. (2018) Apuntes sobre el Derecho del Ciberespacio. *Sego-Bit: Revista de la Escuela de Ingeniería Informática de Segovia*, (7). https://d1wqtxts1xzle7.cloudfront.net/57980401/SEGOBIT-V05-N07-P004-libre.pdf?1544634328=&response-content-disposition=inline%3B+filename%3DApuntes_sobre_el_Derecho_del_Ciberespaci.pdf&Expires=1676310822&Signature=KCF7ERpqlDAAl2VvCUnch7kt1G7H3uP93BP7VytiaGzhIxVIvc5TAi6BzZradkj7fHB~VBA9zhkdwjuMN5E9wduhOd2cqH9h~EA-iA6C9vOB8ii1JIRnQiAlNwFM916q8w38WH5FSDMJUrNUfDHXatWH~uJGqmcOB3kXn1xc66pFE6mteLDri2cNC6cHf8PQjOirwQOlOVNkOIUq2KIGu~VgSbECd8GMgiw3FKQ9pPDIBKxLAPp7JcI4LC-

oJ2qQl7BFVMGgt2YvKzobTXWJ7gxtgJR4dQ2Lswcd8ReZrBfL5WE16lOxGRx77P66xpr35hB4OwJI9S-9AFwmGnwtCA__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA

Álvarez Valenzuela, Daniel. (2018). Ciberseguridad en América Latina y ciberdefensa en Chile. *Revista chilena de derecho y tecnología*, *7*(1), 1-2. https://dx.doi.org/10.5354/0719-2584.2018.50416

Calderón, F. A. C., Barraquel, J. E. Q., Martínez, M. D. A., & Bonilla, S. F. F. (2019). Desafío de la ciberseguridad ante la legislación penal. *Dilemas contemporáneos: Educación, Política y Valores*. https://dilemascontemporaneoseducacionpoliticayvalores.com/index.php/dilemas/article/view/1236

Eaton, Thomas. (2021). Self-Defense to Cyber Force: Combatting the Notion of 'Scale and Effect. *American University International Law Review* 36 (4): 697–771. https://search.ebscohost.com/login.aspx?direct=true&db=lgs&AN=151988785&lang=es&site=ehost-live.

García Vázquez, B. (2022). La legítima defensa preventiva contra los actores no estatales en el ciberespacio: estudio comparativo de las posiciones de los miembros permanentes del Consejo de Seguridad de Naciones Unidas. *Revista De La Facultad De Derecho De México*, 72(283), 245–270. https://doi.org/10.22201/fder.24488933e.2022.283.83165

González Porras, Andrés José. (2016). Privacidad en internet: los derechos fundamentales de privacidad e intimidad en internet y su regulación jurídica. La vigilancia masiva. Universidad de Castilla-La Mancha. https://ruidera.uclm.es/xmlui/handle/10578/10092

Gutiérrez Espada, C. (2020). De la legítima defensa en el ciberespacio. ISBN: 978-84-1369-047-6 (Libro)

Kesan, Jay P., and Carol M. Hayes. (2012). Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace. Harvard Journal of Law & Technology 25 (2): 415–529. https://search.ebscohost.com/login.aspx?direct=true&db=lgs&AN=79450372&lang=es&site=ehost-live.

Kinast Werner, R. (2021). Disuasión y uso de la legítima defensa en el ciberespacio. *Cuadernos de Difusión,* (45), 103 - 122. https://publicacionesacague.cl/index.php/cuadernos/article/view/238

Jaunarena, Horacio. (2021). *Ciberdefensa.* http://repositorio.ub.edu.ar/handle/123456789/9584

Llorens, M. (2017). Los desafíos del uso de la fuerza en el ciberespacio. *Anuario Mexicano de Derecho Internacional*, vol. XVII, enero-diciembre, pp. 785- 816. https://www.redalyc.org/articulo.oa?id=402750094023

Meyer, Jonathan M. (2018). Crossing the Line: The Law of War and Cyber Engagement - An Introduction. *International Lawyer* 51 (3): 587. https://search.ebscohost.com/login.aspx?direct=true&db=lgs&AN=135640058&lang=es&site=ehost-live.

Miaoui, Y., & Boudriga, N. (2019). Enterprise security economics: A self-defense versus cyber-insurance dilemma. *Applied Stochastic Models in Business & Industry,* 35(3), 448–478. https://doi.org/10.1002/asmb.2451

Navarrete Saavedra, Fernando. (2014). El ciberespacio: Nuevo escenario de confrontación. *Anuario mexicano de derecho internacional*, 14, 863-868. http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-46542014000100027&lng=es&tlng=es

Payne, Christian & Lorraine, Finlay. (2017). Addressing Obstacles to Cyber-Attribution: A Model Based on State Response to Cyber-Attack. *George Washington International Law Review* 49 (3): 535–68. https://search.ebscohost.com/login.aspx?direct=true&db=lgs&AN=123655890&lang=es&site=ehost-live

11. Entrevistas personales

Stel, Enrique. (2014). *Seguridad y defensa del ciberespacio*. Editorial Dunken. (Libro)

Moraga, K. (2023). Entrevista personal. MSc. Ing. Kevin Moraga, profesor Maestría en Ciberseguridad, Escuela de Computación, Instituto Tecnológico de Costa Rica.

Esquivel Vargas, H. (2023). Entrevista personal. Dr. Herson Esquivel Vargas, profesor Maestría en Ciberseguridad, Escuela de Computación, Instituto Tecnológico de Costa Rica.

Jiménez, M. (2023). Entrevista personal. Miguel Jiménez, Gerente de nube, Grupo Modular Avanzado.

Segura, H. (2023). Entrevista personal. Hernando Segura, Administrador de empresas, Gerente General True-sec.

Campos Cordero, R. A. (2023). Entrevista personal. Master Rodrigo A. Campos Cordero, profesor Maestría en Ciberseguridad, Escuela de Computación, Instituto Tecnológico de Costa Rica.

Chirino, A. (2023). Entrevista personal. Dr. Alfredo Chirino, AG Legal.