
UNIVERSIDAD
SAN IGNACIO
DE LOYOLA

**FACULTAD DE DERECHO**

**Carrera de Relaciones Internacionales**

# LAS IMPLICANCIAS DE LOS CIBERATAQUES DEL S. XXI EN AMERICA LATINA

**Trabajo de Investigación para optar el Grado Académico de Bachiller en Relaciones Internacionales**

**MAYRA ALEJANDRA VILLAR NIETO**

**Lima – Perú**
**2019**

**Tabla de Contenidos**

## Introducción

El ciberataque es considerado como la "guerra del siglo XXI" no solo por el avance tecnológico de su accionar, sino también a la presencia silenciosa y difícil de detectar. El Foro Económico Mundial ha publicado el estudio "Riesgos Globales (2019)" donde los ciberataques se encuentran en el quinto lugar del Top 5 de los Riesgos Globales en Términos de Probabilidad. Según dicho reporte, la inteligencia artificial será usada como "medio para el diseño de ciberataques más potentes", evidenciándose, en el 2018, que los ataques cibernéticos "plantean riesgos para la infraestructura crítica" en referencia a estados, por lo que se debe fortalecer la seguridad cibernética. En términos globales, se prevé que dichos ataques, crezcan entre un 89 y 82 por ciento en el presente año. Latinoamérica no ha sido ajena a estos ataques, ya que en el 2018 registraron 9 ataques por segundo (Forbes Staff, 2018).

"El mantra de finales del siglo XX es que la información es poder. Esto se ha convertido en una realidad", una afirmación hecha por Mark M. Pollitt del laboratorio del FBI (1998, p.8-10) que podría explicar la razón por la que los actores del sistema internacional realizan ataques cibernéticos. El hacker conoce de la importancia de la información para los gobiernos y empresas transnacionales, siendo esta invaluable y base para su accionar. De ese modo, el acceso al mismo le brindaría conocimiento de información confidencial, la cual podría usar según su conveniencia o la de los estados que lo contraten.

Debido a dicha necesidad de tener acceso a información confidencial, los ciberataques pueden ser efectuados por Estados mediante grupos privados, lo cual permite deslindarse de cualquier responsabilidad, estando en correlación con lo mencionado por un experto en ciberguerra de la OTAN: "Si quieres tener una cibercapacidad de negación plausible, necesitas ser capaz de aceptar cierto nivel de cibercrimen" (Klimburg, 2010: 43).

Durante esta investigación se buscará analizar cuáles son las implicancias para los actores de la comunidad internacional, no solo enfocándose en los ciberataques como hecho a corto

plazo, sino también explicando que los ciberataques no sólo representan una amenaza momentánea para las empresas y estados latinoamericanos, sino también pueden variar el curso político y económico de un país, e incluso afectar psicosocialmente a la población, tal como se ha visto en los últimos años.

Finalmente, este trabajo de investigación busca brindar a la población, empresas y estados un medio de fuente de información que pueda generar un impacto en la ciberseguridad de la región.

**Antecedentes de investigación**

Con el pasar del tiempo, los conflictos y guerras han evolucionado, y con ello la seguridad de los estados. Antes de la segunda guerra mundial, la sociedad estaba inmersa en un mundo multipolar. Sin embargo, tal como lo menciona Kenneth N. Waltz (1988): "En política internacional el éxito lleva al fracaso, el excesivo poder de un estado o coalición de estados, ocasiona la oposición de otros". Esta afirmación demuestra la causa de la segunda guerra mundial y el origen de la guerra fría entre Estados Unidos y la Unión Soviética. Durante la época de la guerra fría, se vivió un conflicto sin guerra directa en territorio de ambos estados, sin embargo, se originó un nuevo tipo de conflicto bélico llamado "Guerras Proxy"[1], y se afianzó el desarrollo económico de Estados Unidos de América.

Sin embargo, los tiempos han cambiado, tras la caída de la Unión Soviética y el ascenso de potencias regionales (especialmente China), la cooperación juega un rol más importante para repotenciar el desarrollo económico de las potencias tras el evidente fracaso de la política comunista con la caída de la URSS y actualmente, la penosa situación de Venezuela. Tal como menciona dicho autor, las economías en un mundo bipolar son menos interdependientes que

[1] La guerra proxy o guerra subsidiaria, es un tipo de guerra en la cual dos o más potencias utilizan a terceros (países, grupos insurgentes, movimientos revolucionarios e incluso grupos terroristas) a favor de sus intereses estatales, en lugar de enfrentarse directamente. Es usual que las potencias utilicen a países que se encuentran en un conflicto interno para brindar soporte a uno de los bandos, y de esa manera enfrentarse indirectamete.

en un mundo bipolar. Por ello, en la actualidad, se sabe que ante un conflicto se debe tener en cuenta dicha interdependencia y los efectos que traería económicamente, además de las consecuencias en el desarrollo de las empresas y del propio estado.

Kenneth N. Waltz (1988) mencionó que "si el interés y la ambición entran en conflicto, la ausencia de crisis es más inquietante que su presencia. Tanto el error como la sobrerreacción de las potencias son fuente de peligro", abriendo la puerta a la situación se ciberseguridad actual. Existe realmente una crisis, pero en un escenario que no es el físico, sino el virtual, por lo que es más difícil de percibir. De igual manera, sigue siendo inquietante. Ante estas crisis, los estados no deben sobrerreaccionar porque podría generar una crisis en el escenario físico, pero tampoco pueden seguir cometiendo errores en cuanto a atacar cibernéticamente ya sea por sus fuentes o por medios de terceros, a estados o empresas contrarias a sus filas.

Estamos inmersos en un conflicto de cuarta generación, donde no solo los estados son participes, sino también las empresas, minorías y los propios ciudadanos, y donde la principal arma es la tecnología, siendo muy complejo distinguir, en ciertos conflictos, entre delincuencia y un conflicto real. De ese modo, se debe tener prioridad sobre el tema dentro de la agenda de cada estado.

Para culminar el antecedente de esta investigación, es necesario mencionar a A.F.K. Organski, quien en su libro World Politics, bajo una visión Racionalista, dio origen a la Teoría de Transición de Poder, mencionando que:

> Existe una potencia dominante, existiendo debajo grandes potencias, quienes apoyan a la potencia dominante a mantener el orden internacional, después las potencias medianas, que no se atreven en buscar mayor liderazgo y finalmente las potencias pequeñas que no son amenaza. (Organski, 1968)

Su implicación en este contexto, se da debido a que esta jerarquía también existe a nivel regional, pero siempre bajo la supervisión y subordinación de la jerarquía global. Se deduce de

dicha teoría que, en la búsqueda de poder, y con él, el conflicto, siempre está implicada alguna potencia global. Ante esto, ¿qué es poder? Según el autor, "es la habilidad para imponer o persuadir al oponente a cumplir con las demandas" (Organski, citado en Tammen, Power Transitions, p.8). Entonces los estados que no son potencias deben subordinarse a la potencia, y el estado que se opone, se verá obligado a hacerlo, y ya que, no podría usarse un "Hardpower"[2] e iniciar una guerra frontal, los sistemas informáticos son ahora el escenario para ello.

Y, ¿dónde quedan los actores privados? Ante ello, la teoría de Gilpin, en su libro War and Change in World Politics (1981), menciona "la teoría sociológica asume que el comportamiento individual es explicado por la naturaleza del sistema y el lugar que uno tiene en él, por lo tanto el sistema social es un determinante primordial de la conducta", (Gilpin, War and Change, ix) agregando además que "los individuos siempre buscan maximizar sus valores e intereses" (Gilpin, War and Change, x), pudiendo ser la base de la explicación de por qué la existencia de los hackers cibernéticos y ataques a empresas privadas que no tienen ningún vínculo con los gobiernos.

**Concepto de Seguridad Internacional**

Al dar inicio al desarrollo evolutivo del concepto de seguridad internacional, es imperativo partir desde la Paz de Westfalia, siendo este el inicio del estado-nación, con sus principios de territorio, población, gobierno y soberanía. A raíz de este suceso, el estado soberano, único actor en su momento de las relaciones internacionales, interactúa con sus pares bajo el precepto "rex est imperator in regno suo" (el rey es emperador en su reino) (Bartolomé, 2006, p. 25). De esa forma, la seguridad internacional durante este periodo se asociaba, tal como menciona

[2] "Hard Power" o Poder Duro, es un termino expresado por Joseph Nye en cuanto al balance de poder de los estados asentándose en la capacidad e imposición militar y económica como herramienta de ejercicio de poder de las potencias, teniendo como extremo la coerción.

Mariano Cesar Bartolomé citando a Nye, a “la ausencia de amenaza al estado” (2006, p. 25), en donde la única amenaza podría ser otro estado.

El concepto de seguridad realista de Morgenthau, asocia la seguridad del estado con el poder y la capacidad militar con el objeto de defender intereses y la búsqueda de poder, siendo en esta etapa el estado el ente protector y el concepto de seguridad alineado a dicho fin, además de que el poder “es universal en tiempo y espacio” y se convierte en el objetivo inmediato de cualquier nación” (Cujabante, 2009, p.96). Es así como la interacción se reduce al manejo de la búsqueda constante de poder y el mantenimiento de la paz y seguridad enfocada más que en un ámbito internacional como actualmente lo conocemos, como un ámbito de seguridad nacional (en defensa) y competencia por el poder.

Tras el desarrollo del tiempo y los sucesos de la Primera Guerra Mundial y Segunda Guerra Mundial, se empiezan a reconocer otros sujetos de la Comunidad Internacional como los Organismos Internacionales y actores no gubernamentales. Ello dio inicio a la teoría de la interdependencia (Muñoz, 2005) entre los sujetos, estando también enmarcada dentro de la seguridad internacional, en donde la seguridad en el ámbito militar y constante lucha de poder han cedido un porcentaje de su prioridad en comparación con años anteriores, debido a que surgen nuevos temas internos de cada estado e intereses en común, y ubicó a la cooperación como herramienta fundamental de las relaciones internacionales de los estados (Cujabante, 2009).

Ello no quiere decir que la búsqueda del poder haya sido dejada de lado. Como lo señala Daniel Gómez, existen cinco supuestos centrales, relacionados con el neorrealismo, que explican dicha lucha de poder (2017, p. 24). El primer supuesto menciona que “las grandes potencias son los principales actores en las políticas internacionales y operan en un sistema anárquico” (Mearsheimer, 2006, p. 73), el segundo supuesto menciona que “todos los estados poseen cierta capacidad militar ofensiva” (Mearsheimer, 2006, p.73), el tercero menciona que

“los estados nunca pueden tener certeza de las intenciones del otro estado” (Mearsheimer, 2006, p.73), de tal forma que los estados desean saber hasta qué punto están dispuestos a llegar con el fin de tener el poder. El cuarto supuesto señala que “el principal objetivo de los estados es la supervivencia” (Mearsheimer, 2006, p.74). Finalmente, el quinto supuesto menciona que “los estados son actores racionales para sobrevivir” (Mearsheimer, 2006, p.74).

Como se puede apreciar, incluso la definición de seguridad internacional ha ido evolucionando de acorde al desarrollo del escenario internacional, sin dejar el interés de los estados, pero sí modificando en cierto punto las prioridades de los sujetos del derecho internacional, desde ubicar al estado en el centro de la seguridad internacional a aceptar la incorporación de nuevos sujetos dentro del sistema internacional y, por ende, actores de la seguridad internacional.

**Ciberseguridad dentro de la seguridad internacional**

Jeimy Cano (p. 5), cita lo mencionado por Bill Clinton (Congreso de Estados Unidos, 1998), en el cual el expresidente identifica ocho sectores imprescindibles para el desarrollo de un estado, los cuales son “energía eléctrica, producción, almacenamiento y suministro de gas y petróleo, telecomunicaciones, bancos y finanzas, suministro de agua, transporte, servicios de emergencia y operaciones gubernamentales (mínimas requeridas para atender al público)” (Cano, p. 5). Ante ello, es necesario que el gobierno proteja dichos intereses y el correcto funcionamiento de sus operaciones.

Con el desarrollo tecnológico, las amenazas se han acrecentado, atacando también a nivel virtual. Un ataque masivo a dichos sectores ocasionaría graves pérdidas al estado o a la empresa afectada. Sin embargo, todavía no existe una definición consensuada de la ciberseguridad, ya que ella depende de la percepción del carácter de la amenaza del espacio cibernético (Lehto, Huhtinen & Jantunen, 2011). Esto, en otras palabras, significa que cada entidad privada o pública percibe de distinta forma y nivel de gravedad, la amenaza al ciberespacio, por lo que

dificulta la definición de un concepto globalmente aceptado cuando cada ente tiene distinta concepción de amenaza, y por ende de seguridad ante ella.

Teniendo en cuenta lo mencionado, el presente estudio se enmarcará bajo un concepto más amplio de ciberseguridad, por lo que se tomará como punto de referencia, lo mencionado por Kevin Newmwyer: la ciberseguridad es un “conjunto de prácticas políticas, de entrenamiento y tecnología, diseñada para proteger el entorno cibernético con la finalidad de asegurar la integridad de la información y habilidad de conectar dispositivos para que operen según diseño” (2015, p.79).

Ahora bien, al enlazar la seguridad con los conceptos de poder explicado anteriormente, emergería el concepto de ciberpoder, el cual es "la capacidad de utilizar el ciberespacio para crear ventajas e influir en los acontecimientos en todos los entornos operativos y a través de los instrumentos de poder" (Stuart H. Starr en Franklin D. Kramer, Stuart H. Starr, Larry Wentz, "Cyber power and National Security", National Defense University, 2009).

Este poder es tomado en cuenta por los actores estatales, pasando a ser actores de ciberataques, ya sea como atacantes o como víctima. Si bien es casi imposible que un estado se atribuya la responsabilidad de un ciberataque, existen casos en el cual se confirma que un estado lo realizó ya sea de manera activa (por sus propios medios) o de manera pasiva (por medio de la subcontratación a un tercero, ya sea empresa de informática o un hacker independiente para realizar dicho ataque).

Cuando un estado pertenece a la fila de los atacantes, mayormente, es por dos razones: desestabilizar al estado enemigo mediante ataques a sistemas informáticos de organizaciones claves para su operación, o para robar información valiosa.

Si bien en el caso de Latinoamérica no existen precedentes probados que un estado ataque de manera cibernética a otro, cada país se encuentra previniendo ataques cibernéticos (ya sea

efectuado por otro estado o por terceros) por lo que la ciberseguridad forma parte de sus prioridades en las oficinas gubernamentales.

Estados latinoamericanos han sufrido de ciberataques en innumerables ocasiones durante los últimos años. Los más afectados han sido Brasil, Perú, Chile, Colombia, Venezuela, Ecuador y México, en donde hackers cibernéticos han atacado de diversas formas, desde la exposición de datos de millones de peruanos gracias a un ciberataque a la ONPE[3], hasta la sustracción de dinero del Banco Central de Chile.

En cuanto a los actores no estatales, los hackers pueden ser constituidos por asociaciones o solamente ser un hacker especializado en seguridad e informática. Pueden actuar por motivos y medios propios o, como fue explicado anteriormente, pueden ser contratados por empresas, instituciones e incluso estados que buscan obtener información de una manera ilícita o provocar algún daño en el sistema informático de su adversario.

**Ciberataques**

El ciberataque es cualquier acción premeditada en el sistema informático que busque manipular, dañar, modificar, alterar, robar o eliminar cualquier información, software o hardware ya sea en la red de computadoras o en networks (Peter J. Denning, Dorothy E. Denning, 2010). Estos, como se mencionó anteriormente, tienen como causa o efecto la ciberseguridad de los estados o de las empresas privadas, o simplemente un medio de competencia no ética entre sus pares. Si bien esta investigación se enmarca en un sentido político-social, es imprescindible tener como bases términos generales para su control.

En cuanto a sus manifestaciones, podemos ubicar la ciberdelincuencia como una acción informática ilegal o que busca dañar medios electrónicos, redes de internet y computadoras; el cibercrimen, como una acción informática ilegal enfocada en delitos de mayor alcance como

[3] ONPE: La Oficina Nacional de Procesos Electorales es la autoridad máxima de la República de Perú que se encarga de organizar y ejecutar distintos procesos electorales, de referéndum y otros tipos de consulta popular. http://www.onpe.gob.pe/nosotros/

el robo, falsificación, estafa, en donde se utiliza los medios digitales para dicho fin; el ciberterrorismo, siendo este un caso controversial ya que, para que se considere ciberterrorismo, es necesario que genere miedo en la sociedad, utilizando las redes informáticas para causar daños con fines políticos y/o religiosos.

Los ciberterroristas utilizan la red como fuente de financiamiento, medio de propagación de amenazas para expandir terror psicológico en la sociedad, reclutamiento, interconexión o comunicación entre los miembros de la organización y externos, coordinación entre los miembros, fuente de información y adoctrinamiento. Es imperante aclarar que si bien, el ciberataque puede ser parte accionar del ciberterrorismo como tal, no se debe generalizar los ciberataques como ciberterrorismo, tal como muchos medios de comunicación indican.

Finalmente, se encuentra la ciberguerra, la cual se define como un conflicto que utiliza la informática y telecomunicaciones como arma de guerra, usando como terreno de batalla el espacio cibernético como búsqueda de información o la destrucción del enemigo. Hasta el momento, se puede señalar que no ha existido ningún ataque perteneciente a esta categoría, ya que a pesar que los ataques cibernéticos han causado daños a ciertas oficinas de instituciones nacionales o información, no han tenido la magnitud necesaria de daño masivo para considerarse ciberguerra.

En cuanto a técnicas de ciberataques, según Ureña (2015, p.4), se puede identificar al virus informático, el más conocido por los usuarios cibernéticos, es el uso de programas informáticos con el objeto de infectar archivos para poder alterarlos o dañarlos. Esta reacción se produce, ya que el virus informático envía un código al archivo que busca dañar y, cada vez que se desea abrir el archivo, este virus se propaga entre otros archivos. El SPAM es otra técnica de ciberataques la cual se presenta mediante el envío de mensajes no deseados, recepcionado mayormente por medio de los correos electrónicos y mensajes de texto, se presenta por medios mayormente publicitarios para dañar el sistema de la computadora.

En el sector privado, el Spoofing es una de las más comunes y, además, peligrosas, basándose en la suplantación de identidad de otra máquina perteneciente a la misma red, en donde, aprovechando dicha confianza, logra el acceso a la información total del usuario, pudiendo incluso modificar o eliminar archivos.

A su vez, existen otras técnicas como el Pishing, el cual consta del envío masivo de correos electrónicos o mensajes que permite que algún usuario crea en la información vertida en el correo y acceda a brindar datos personales que servirá a los hackers para obtener cuentas bancarias, información sensible, entre otros; los Keyloggers, que son archivos espías que logran grabar las teclas pulsadas e incluso los clicks del mouse como fuente de información para después ser usada por la persona u organización que ha instalado dicho archivo, hardware o software espía, permitiendo así grabar usuarios, contraseñas e incluso obtener información; los Archivos BOT del Internet Relay Chat, los cuales permiten que el sistema pueda ser controlado remotamente sin que la persona u organización permita o se dé cuenta de que esto está sucediendo. Su espacio de acción es mayormente los chats de conversación de forma activa, por lo que es casi imposible poder identificarlos.

Asimismo, se emplean los Rootkits, que son herramientas que permiten ocultar el acceso no autorizado o ilícito a un sistema, las cuales no permiten la visibilidad, detección ni identificación de la persona o programa no autorizado; el Stuxnet, un gusano informático que espía y pude controlar modificar la información de un sistema. Su presencia es casi imposible de detectar ya que, a diferencia de la mayoría, el Stuxnet utiliza firmas digitales legales, lo que reduce el nivel de confiabilidad en los softwares de seguridad comunes. (Matrosov, Rodionov, Harley, Malcho, 2011); y el Ransomware, el cual es un virus que, al ingresar al sistema, limita su acceso para el usuario y pide dinero a cambio, “secuestrando” la información hasta que se realice el pago del “rescate”. Este virus ha atacado a empresas internacionales con sede en Latinoamérica en los últimos años, como Mondelez y Telefónica.

En la era de la globalización, el internet es un elemento clave para la innovación y el desarrollo económico, generando incluso dependencia de sectores como el de transporte, energía y minas, el financiero para realizar operaciones bancarias (Nieva Machín y Manuel Gazapo, 2016) además de alto grado de uso por parte las empresas transnacionales para poder comunicarse y pactar negocios internacionales. A mayor dependencia, crece la necesidad de alinear dicha realidad con medidas de seguridad, teniendo en cuenta que la necesidad de tratar adecuadamente la información es uno de los mayores desafíos globales.

El factor principal que dificulta la ciberdefensa de las entidades privadas es la consumerización, permitiendo mayor alcance de difusión y penetración entre la población, los individuos, los consumidores y ciudadanos para posteriormente propagarse hacia las organizaciones comerciales y gubernamentales. Esto corresponde a un desafío, ya que se presenta en la adquisición de un software que permite que la gestión de las empresas sea más sencilla, pero no tienen conocimiento de que esto incrementa la posibilidad de que la empresa pueda ser víctima de ciberataques.

A su vez, existen otros factores como el intercambio de información sensible vía online; las actividades e información completa (incluyendo la información sensible) de la empresa localizada en una nube compartida (cloud) por los miembros de la compañía en la red; y la búsqueda de nuevos mercados internacionales sin medidas de seguridad confiables.

En cuando a los estados, estos han sido y siguen siendo víctimas (y atacantes) de los ciberataques. Como fue mencionado en líneas anteriores, el escenario internacional se ha desarrollado en el tiempo, al igual que una evolución en el conflicto; lo que tiene como consecuencia que la seguridad de los estados deba ir a la par con el desarrollo de las amenazas.

Según el Instituto Español De Estudios Estratégicos, en cuanto a la auditoria de ciberataques a estados, se podría clasificar en (Instituto Universitario «General Gutiérrez Mellado», 2010):

i. Ataques impulsados por Estados: Debido a que los conflictos han sido trasladados al ciberespacio, estados han sido víctimas de ataques por parte de países, cuyos objetivos son específicos y estratégicos, siendo un claro ejemplo del fin del ciberataque, el ciberespionaje.

ii. Servicios de inteligencia y contrainteligencia: Los cuales son empleados por los estados para poder analizar la información de otro estado y poder procesarlo.

iii. Terrorismo y grupos extremistas: Usan el sistema informático para planificar sus acciones, darlas a conocer, reclutar y como herramienta de financiación.

iv. Delincuencia organizada: Usan el ciberespacio como medio de obtención de información sensible para cometer fraude, estafa y chantaje.

v. Ataques de perfil bajo: Civiles que realizan ciberataques por motivación personal y cuentan con conocimientos en tecnología de la información.

**Mirada panorámica sobre las implicancias en los actores**

Teniendo en cuenta que el objetivo de esta investigación es brindar una base para analizar las implicancias de los ciberataques en los actores del escenario latinoamericano, los ciberataques “deben ser considerados como una grave amenaza emergente” (Francisco Ureña, 2015), ya que genera implicancias psico-sociales, económicas y políticas a los estados, al sector privado y a la ciudadanía.

Las implicancias que originan los ciberataques a las empresas latinoamericanas han aumentado a la par del desarrollo tecnológico. En el caso de las mismas, se han registrado mediante el robo de tarjetas de créditos, infiltraciones a los sistemas de información de compañías, filtraciones, robo y alteraciones de información, espionaje e incluso chantaje. Las implicancias pueden generar incluso consecuencias a largo plazo, como el caso de la ejecución de daños a las tecnologías de información especializadas en seguridad, pudiendo causar daños materiales a los objetos que contengan dichas tecnologías que se han visto previamente alteradas/dañadas adrede.

Los hackers especializados en ciberataques vienen alterando la seguridad de los usuarios tecnológicos, impartiendo incluso, temor en la población civil (y en caso de grupos terroristas que usan este medio, impartiendo terror). Dichas acciones pueden generar desde la pérdida monetaria de un civil, pérdidas económicas y daños de reputación en una empresa, hasta ataques terroristas a distancia, por lo que las implicancias pueden medirse según el nivel de ataque y a quién se encontraría dirigido.

En cuanto a los estados, pueden registrarse desde apropiación de información, implicancias económicas e incluso implicaciones políticas, afectando a la estabilidad política de un estado o de la región. Dicha apropiación de información, tal como lo menciona Jimeno (2019), "supera las vulneraciones de los derechos de Protección de Datos o la mera violación de los mismos a la privacidad", por lo que incluso la propiedad intelectual y la propia información confidencial de civiles se ve expuesta ante dichos ataques cibernéticos.

Un punto a enfatizar es la dependencia a nivel global, en donde los afectados por las implicancias de los ciberataques pueden afectar a actores indirectos o terceros, que no fueron blanco directo de dichos ataques. Es así como la dependencia "socioeconómica" (Jimeno, 2019) del siglo XXI, la interacción entre usuarios cibernéticos y la interconexión de sistemas informáticos en el mundo, hace del ciberespacio una plataforma vulnerable con implicancias a todo usuario.

Torres (2017) analizó un factor determinante entre el estado y los ciberataques que podría generar implicancias a dicho estado y, en consecuencia, desestabilizar a la región. Utilizó el término "Hackeando la democracia" (Torres, 2017, p.1) para poder describir el accionar de estados potencias, desarrollado por ataques cibernéticos, para poder cambiar el camino de las elecciones presidenciales de otros estados, favoreciendo así a partidos políticos que, una vez en el poder, los beneficiarían.

Dichos ciberataques pueden no se percibidos por la sociedad, siendo un claro ejemplo el uso de “bots, cuentas semiautomatizadas y trols profesionales para ampliar el alcance y relevancia de ciertas posturas, y como mecanismo de hostigamiento a usuarios que discrepen con dichas ideas” (Torres, 2017, p. 5) en redes sociales como Twitter por parte de Rusia, o con portales de noticias falsas y bots para desinformar a los civiles, por parte de Estados Unidos (Torres, 2017). Se demuestra así, que el uso de ciberataques puede estar inmerso incluso en la política, ya sea para desprestigiar al oponente, o para tomar ventaja desinformando al votante.

Si bien muchos tendrían conocimiento general sobre las implicancias de los ciberataques a los estados y a sector privado, es imperativo mencionar que no es necesario separar el sector privado del público ya que, en América Latina, se han visto relacionado en cuanto a las implicancias de los ciberataques, siendo el caso más resaltante el de Panama Papers.

Dicha filtración informática a la firma Mossack Fonseca, en donde se filtró 2,6 terabytes de información al periódico alemán Süddeutsche Zeitung, puso al descubierto a países de los 5 continentes, entre ellos Argentina, Brasil, Bolivia, Chile, Colombia, Ecuador, Paraguay, Uruguay, Venezuela, Perú, entre otros estados latinoamericanos; además de a Organismos Internacionales de envergadura mundial, en los cuales altos funcionarios y personalidades internacionales se veían expuestas ante casos de evasión tributaria y ocultamiento de activos y propiedades, revelando que “solo del 2004 al 2013, América Latina perdió 1.4 billones de dólares a causa de los Flujos Financieros Ilícitos (Olivares, 2016, p.3).

Si bien fueron personalidades jurídicas privadas las que se encuentran procesadas por dichos sucesos, el impacto y controversia a nivel de estado ha generado un gran impacto en América Latina, generando que la operación Lava Jato cambie el curso de las investigaciones, de un tema evasión de impuestos, a un caso de corrupción interestatal. Ello ha generado un impacto psicosocial tras manifestaciones de desconfianza en la población con respecto a sus autoridades. Mauricio Macri, actual presidente de la República Argentina; los expresidentes de

la República del Perú Alan García, Alberto Fujimori y Alejandro Toledo; Michel Temer, expresidente de Brasil; políticos brasileros, entre otros que ha dejado en el desconcierto político a la sociedad latinoamericana. Además, ha generado inestabilidad política y una amenaza de reducción de las inversiones del sector privado en esta región.

Se puede comprender en líneas anteriores que el impacto de los ciberataques en América Latina genera una serie de sucesos que pueden afectar a largo plazo a toda una región, en donde estado, población y sector privado se encuentran volubles y pueden ser afectados de manera relacional por los mismos.

## Casos de estrategias de ciberseguridad en países de América Latina

### Perú

Si bien la República del Perú no cuenta con una Política Nacional en el tema, en el presente año se aprobó la ley de ciberseguridad, con la finalidad de brindar un marco legislativo en ciberseguridad en el país (María Cárdenas, Diario Gestión, 2019), y la ley de ciberdefensa, que busca brindar un marco normativo en materia de ciberdefensa (Ley N.º 30999, Diario el Peruano, 2019), considerando sus capacidades y el desarrollo y ejecución de las operaciones militares en el ciberespacio.

Durante la ley de ciberdefensa, se menciona que el Comando Conjunto de las Fuerzas Armadas es el encargado de velar y ejecutar los planes de ciberdefensa.

En la ilustración posterior elaborada por el "National Cyber Security Índex", el Perú se encuentra en el puesto número 66 en cuanto a la ciberseguridad aplicada por el gobierno con un puntaje de 40.26 (e-Governance Academy Foundation, 2018), por lo que a pesar de no contar con una Política de Ciberseguridad, dicho estado se encuentra por encima de países latinoamericanos que si cuentan con una política aplicada la ciberseguridad de estado, como México que se encuentra en el puesto número 70.

Asimismo, tras la necesidad de digitalizar las operaciones estatales de forma segura que permita cierto control al estado, el gobierno ha creado la "Secretaría de Gobierno Digital", el cual se define, mediante el Decreto Supremo N° 022-2017-PCM, Art. 47, como "el órgano de línea, con autoridad técnico normativa a nivel nacional, responsable de formular y proponer políticas nacionales y sectoriales, planes nacionales, normas, lineamientos y estrategias en materia de Informática y Gobierno Electrónico" (Secretaría de Gobierno Digital, 2019), además de encabezar el plan de modernización de las instituciones públicas y sus servicios, adaptándose a la nueva era tecnológica.

Entre sus funciones, engloba la aprobación de normas y estándares concerniente a la seguridad de la información, asignando a la Subsecretaría de Transformación Digital, según el Art. 51 del Decreto Supremo N° 022-2017-PCM, "Formular y proponer normas y estándares para el desarrollo e implementación de la seguridad de la información, infraestructura de datos espaciales, datos abiertos, interoperabilidad, portales del Estado, entre otros, de las entidades públicas del Estado" (Secretaría de Gobierno Digital, 2019).

**Chile**

La República de Chile cuenta con una Política Nacional desde el año 2017, la cual fue planificada desde el 2015 con miras a proyectar objetivos para el 2022, estando a cargo del Ministerio de Defensa.

El sustento del gobierno para la planificación de dicha medida se amparó en el artículo 51 de la Carta de las Naciones Unidas, en donde manifiesta que el estado puede emplear medios que considere apropiados para ejercer su legítima defensa. Ello se traslada a una aseveración con respecto a que Chile considera que los ciberataques podrían afectar su soberanía, el ejercicio libre de sus derechos como estados, sus intereses, y el de toda su población, incluso de la misma medida que un ataque armado (Pedro Huichalaf, 2018).

Dicha Política Nacional, basada en “el modelo de gobernanza y la estructura organizacional moderna” cuenta con 5 objetivos, los cuales son:

- Contar con una infraestructura de la información robusta y resiliente
- El estado protegerá los derechos de las personas en el ciberespacio
- El desarrollo de una cultura de ciberseguridad basada en la educación y responsabilidad.
- Establecimiento de relaciones de cooperación en materia de ciberseguridad.
- Promoción del desarrollo de la industria de ciberseguridad.

Para lograr dichos objetivos, la política cuenta con 41 medidas las cuales engloban a diversas instituciones estatales gubernamentales, enfocándose cada una de ellas a un objetivo definido (Gobierno de Chile, 2017).

**México**

Los Estados Unidos Mexicanos cuentan con una Estrategia Nacional de Ciberseguridad basada en los principios de “perspectiva de los derechos humanos, enfoque basado en gestión de riesgos y colaboración multidisciplinaria y de múltiples actores”. A continuación, se presenta un gráfico elaborado por el Gobierno Mexicano, en el cual se enmarca dicha estrategia nacional.


*Figura 1:* Objetivos Estratégicos de la Estrategia Nacional de Ciberseguridad de México

Dicha estrategia, la cual se encuentra a cargo de la Subcomisión de Ciberseguridad de la Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico CIDGE, tuvo como base la Estrategia Digital Nacional enmarcada en el Plan Nacional de Desarrollo 2013 – 2018, la cual buscaba la digitalización del estado.

La necesidad de fomentar la ciberseguridad en los Estados Unidos Mexicanos se basa en que dicho país se encuentra entre los primeros lugares en recepción de ataques cibernéticos en América Latina (NOTIMEX, 2019), y dentro de los 10 países con más ataques cibernéticos a nivel mundial. Asimismo, “el 83% de las empresas es perjudicado por un ciberataque por lo menos una vez al año, incrementándose un 40% los casos entre 2017 y 2018, llegando a representar en dicho país el 59% de fraudes cibernéticos” (Anónimo, 2019).

**Cooperación regional en materia de ciberseguridad**

En el marco de cooperación regional, la ciberseguridad viene siendo impulsada por la Organización de Estados Americanos, en donde tuvo como inicio la resolución AG7RES. 2004

(XXXIV-O/04), mediante la aprobación de la "Estrategia Interamericana Integral para Amenazas a la Seguridad Cibernética" (OEA, 2017), fomentando una red de cooperación regional en cuanto a seguridad cibernética. Si bien, según el alcance con el que se cuenta para la recolección de información, hasta el 2017 solo existían seis estados (OEA, 2017) que contaba con políticas de ciberseguridad, la mayor parte de estados cuenta con estrategias de ciberseguridad.

Asimismo, existe un Programa de Ciberseguridad, el cual se tiene como pilares "el desarrollo de políticas, desarrollo de capacidades e investigación y divulgación" (Comité Interamericano contra el Terrorismo, 2019). Este programa, implementado por el Comité Interamericano contra el Terrorismo – CICTE, ha logrado que en la actualidad un promedio de 20000 ciudadanos y oficiales del sector público y privado hayan sido entrenados en temas de seguridad cibernética, ha apoyado en la creación de 11 Estrategias Nacionales de Ciberseguridad, ha realizado 14 "Ciber ejercicios" y ha apoyado para el aumento de 4 a 21 Certs nacionales[4] (Comité Interamericano contra el Terrorismo, 2019).

Leiva (2015) asegura que esto se debe a "la falta de recursos dedicados a este tema", y "la carencia de experiencia práctica y conocimientos especializados para diseñar e implementar este tipo de medidas", a lo que Hernández (2018) agrega la "no exclusividad en cuanto a seguridad cibernética de la región", ello ya que este es un tema que se atribuye tanto a públicos como privados a nivel mundial.

Hernández (2018), menciona la importancia de ejercer plazos en cuando al establecimiento de políticas públicas, tal como lo hizo Chile con plazo límite el 2022, con el fin de optimizar y hacer más viable una política nacional de ciberseguridad efectiva, enfatizando la necesidad de que los países latinoamericanos implanten políticas más que compromisos para poder hacer frente a los ciberataques en la región. Si bien, "una estrategia de Ciberseguridad no garantizará

[4] CERTS: Equipo de Respuesta ante Emergencias Informáticas

que se puedan repeler todos estos ataques, una ausencia de la misma, lo hará menos" (Hernández, 2018, p.5)

**Conclusiones**

Los ciberataques son el medio más atractivo para obtener o alterar información de estados, ya que es el más barato, con herramientas accesibles y la mayor ventaja es que la fuente puede no ser identificada.

Un ataque masivo a sectores claves como son la energía eléctrica, producción, almacenamiento y suministro de gas y petróleo, telecomunicaciones, bancos y finanzas, suministro de agua, transporte, servicios de emergencia y operaciones gubernamentales; generaría cuantiosas pérdidas privadas y estatales. Ante ello, es imprescindible ejecutar un plan de ciberseguridad, pudiendo definirse generalmente como un "conjunto de prácticas políticas, de entrenamiento y tecnología, diseñada para proteger el entorno cibernético con la finalidad de asegurar la integridad de la información y habilidad de conectar dispositivos para que operen según diseño" (Newmwyer ,2015, p.79). Se menciona el término "generalmente", debido a que cada institución/organización define la ciberseguridad según el grado de amenaza que posee.

A su vez, existe relación entre la ciberseguridad y el ciberpoder, el cual se podría definir como "la capacidad de utilizar el ciberespacio para crear ventajas e influir en los acontecimientos en todos los entornos operativos y a través de los instrumentos de poder" (Stuart H. Starr en Franklin D. Kramer, Stuart H. Starr, Larry Wentz, "Cyber power and National Security", National Defense University, 2009). Ello debido a que muchos consideran que "el ciberataque es un recurso que puede ser utilizado, como medio para incidir en las relaciones de poder, para contrarrestar y balancear la emergencia de un actor potencialmente peligroso para la seguridad." (Daniel Gómez, 2017, p.28).

Por lo antes mencionado, podría señalarse que los ciberataques pueden ser manifestaciones de ciberseguridad por parte de los estados, ya que cada estado diseña la seguridad cibernética

según su realidad, defensa de la protección de sus ciudadanos y del propio estado (José María Molina Mateos, 2013), siendo esta elaborada además según la percepción de amenaza influenciada por la geopolítica y su visión contemporánea (Lester Cabrera Toledo, 2017). Si no es por su propia seguridad, el estado lo hace por desequilibrar al estado enemigo o rival; o para robar información confidencial y así, obtener ventaja.

Asimismo, en el caso de los hackers que ejecutan dichos ciberataques, podría señalarse que, según la teoría sociológica, puede ser debido a la percepción del lugar o rol de dicha persona en su entorno, o sencillamente por la ambición que todo ser humano posee.

Las implicancias más comunes que podría generar los ciberataques en la región son, para los actores privados, perdidas económicas, daños de reputación en una empresa, alteración de la información, hurto de información, acceso a información confidencial, y la implantación de un virus que dañe su sistema de tecnología de información. Para los actores públicos, podría evaluarse desde la apropiación ilícita de información (confidencial), generando implicancias económicas y políticas que podría afectar la estabilidad de un estado o de la región a largo plazo, como el caso de los "Panama Papers", siendo este un ejemplo tangible de cómo los ciberataques al sector privado, pueden afectar a un estado o a un conjunto de estados, por lo que se encontrarían relacionados. Finalmente, podría implicar una "manipulación de la democracia" ocultando información y alterando datos en redes sociales ante elecciones presidenciales, para beneficiar o perjudicar a un sector o partido político.

Las medidas de prevención y ciberseguridad lo complican la vulnerabilidad de los sistemas y la vulnerabilidad de la sociedad, principalmente por la facilidad e ingenuidad al momento de compartir información vía internet, y a nivel estatal debido a que muchos todavía no consideran necesaria la ciberseguridad en estados que no sean potencias y en empresas pequeñas o medianas.

La ciberseguridad en Latinoamérica se encuentra en progreso ya que, si bien no se encuentra desarrollada igual que potencias regionales como los Estados Unidos de América, los organismos públicos vienen implementando estrategias de seguridad para la prevención y detección de los ciberataques, y en casos como Chile, se vienen implementando políticas de ciberseguridad con metas establecidas a un periodo de tiempo.

**Referencias**


A.F.K. Organski. (1968). En World Politics. Estados Unidos : The University of Michigan.

Agencia EFE. (2018). Ataques informáticos aumentan un 60% en Latinoamérica en 2018. El Comercio

Aleksandr Matrosov, Eugene Rodionov, David Harley, Juraj Malcho (2011). Stuxnet, Under the Microscope. Eset. Recuperado de http://static4.esetstatic.com/us/resources/whitepapers/Stuxnet_Under_the_Microscope.pdf

Anónimo. (2019). México en el top 10 de ciberataques. Idc Online. Recuperado de https://idconline.mx/corporativo/2019/06/11/mexico-en-el-top-10-de-ciberataques

Bárbara Alejandra Muñoz Petersen. (2005). La corrupción como amenaza a la seguridad nacional tras la transición democrática en México, Capítulo 1. Colección de Tesis Digitales, Universidad de La Americas Puebla. Recuperado de http://catarina.udlap.mx/u_dl_a/tales/documentos/lri/munoz_p_ba/capitulo1.pdf

Comité Interamericano contra el Terrorismo. (2019). Programa de Ciberseguridad. Organización de Estados Americanos. Recuperado de http://www.oas.org/es/sms/cicte/prog-ciberseguridad.asp

Daniel Alejandro Gómez Llinás. ( 2017). Análisis del Ciberataque para la Seguridad de Los Estados Y Su Incidencia En La Transformación Del Status Quo: Stuxnet El Virus Informático. Universidad Colegio Mayor De Nuestra Señora Del Rosario facultad de relaciones internacionales Bogotá, D.C. Recuperado de https://core.ac.uk/download/pdf/86434151.pdf

Edgardo Aimar Gago. (2017). “El enfoque argentino sobre Ciberseguridad y Ciberdefensa”. Universidad de la Defensa Nacional. Recuperado de http://www.cefadigital.edu.ar/bitstream/123456789/1088/1/La%20defensa%20cibernetica_TI%20LRRII%202017_Ortiz_6.pdf

E-Governance Academy Foundation. (2018). Peru. National Cyber Security Index. Recuperado de https://ncsi.ega.ee/country/pe/

El Presidente de la República, la Comisión Permanente del Congreso de la República. (20119). Ley Nº 30999. Diario El Peruano. Recuperado de https://busquedas.elperuano.pe/normaslegales/ley-de-ciberdefensa-ley-n-30999-1801519-5/

Forbes Staff. (2018). América Latina registra 9 ciberataques por segundo. Forbes. Recuperado de https://www.forbes.com.mx/america-latina-registra-9-ciberataques-por-segundo/

Francisco Uruena . (2015). Ciberataques, la mayor amenaza actual. Instituto Español de Estudios Estrategicos. Recuperado de http://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO092015_AmenazaCiberataques_Fco.Uruena.pdf

Gilpin, R. (1981). War and Change in World Politics. Cambridge: Cambridge University Press. doi:10.1017/CBO9780511664267

Gobierno de Chile. (2017). Política Nacional de Ciberseguridad. Gobierno de Chile. Recuperado de https://www.ciberseguridad.gob.cl/media/2017/05/PNCS-CHILE-FEA.pdf

Gobierno de México. (2017). Estrategia Nacional de Ciberseguridad. Gobierno de México. Recuperado de https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf

Instituto Español de Estudios Estratégicos, Instituto Universitario «General Gutiérrez Mellado». (2010). Ciberseguridad. Retos y Amenazas a la Seguridad Nacional en el Ciberespacio. España : Ministerio de Defensa.

Javier Ulises Ortiz, Claudia Fonseca, Ansorena Gratacos,. (2017). La Defensa Cibernética, Alcances estratégicos, proyecciones doctrinarias y educativas. Universidad Nacional de la Defensa. Recuperado de http://www.cefadigital.edu.ar/bitstream/123456789/1088/1/La%20defensa%20cibernetica_TI%20LRR

Jeimy J. Cano. (.). Ciberseguridad y ciberdefensa: dos tendencias emergentes en un contexto global. 03/07/2019. Editorial. Recuperado de http://52.0.140.184/typo43/fileadmin/Revista_119/Editorial.pdf

Jesús Jimeno Muñoz. (2019). Cyber Risks: Liability and Insurance. InDret. Recuperado de https://www.raco.cat/index.php/InDret/article/viewFile/354516/446502

Jorge Izaguirre Olmedo, Fernando León Gavilánez. (2018). Análisis de los Ciberataques realizados en América Latina. Universidad de Rioja. Recuperado de https://dialnet.unirioja.es/servlet/articulo?codigo=6778118

José Carlos Hernández. (2018). Estrategias Nacionales de Ciberseguridad en América Latina. Grupo de Estudios en Seguridad Internacional / Universidad de Granada. Recuperado de http://www.seguridadinternacional.es/?q=es/content/estrategias-nacionales-de-ciberseguridad-en-am%C3%A9rica-latina

José María Molina Mateos. (2013). CYBERDILEMMA. Instituto Español de Estudios Estratégicos. Recuperado de http://www.ieee.es/Galerias/fichero/docs_opinion/2013/DIEEEO1152013_Cyberdilemma_JM.MolinaMateos.pdf

Juan Alsina Rodriguez. Recomendaciones para prevenir ciberataques. Universidad Piloto de Colombia. Recuperado de http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2922/00002056.pdf?sequence=1

Leiva E. (2015). Estrategias Nacionales de Ciberseguridad: Estudio comparativo basado en

Enfoque Top-Down desde una visión global a una visión local. Revista Latinoamericana de Ingeniería de Software, 3(4). pp. 161-176, ISSN 2314-2642. Recuperado de http://sistemas.unla.edu.ar/sistemas/gisi/papers/relais-v3-n4-161-176.pdf

Lester Cabrera Toledo. (15 de abril de 2017). La vinculación entre geopolítica y seguridad: algunas apreciaciones conceptuales y teóricas. Revista Latinoamericana de Estudios de Seguridad, 20, 111-125.

Manuel R. Torres Soriano. (2017). Hackeando la democracia: operaciones de influencia en el ciberespacio. Instituto Español de Estudios Estratégicos. Recuperado de http://www.ieee.es/Galerias/fichero/docs_opinion/2017/DIEEEO66-2017_Hackeand

María Cárdenas. (2019). Ley de Ciberseguridad: Comisión Permanente aprobó dictamen del proyecto de ley. Diario Gestión. Recuperado de https://gestion.pe/peru/politica/ley-ciberseguridad-comision-permanente-aprobo-dictamen-proyecto-ley-274047-noticia/

Mariano César Bartolomé. (2006). La Seguridad Internacional en el Siglo XXI, más allá de Westfalia y Clausewitz. Buenos Aires: Academia Nacional de Estudios Políticos y Estratégicos. MINISTERIO DE DEFENSA NACIONAL.

Mark M.Pollitt. (1998). Cyberterrorism — fact or fancy?. Science Direct. Recuperado de https://www.sciencedirect.com/science/article/pii/S1361372300870098

Agencia EFE. (2018). Ataques informáticos aumentan un 60% en Latinoamèrica en 2018 . El Comercio. Recuperado de https://www.elcomercio.com/tendencias/seguridadinformatica-ciberataques-latinoamerica-kaspersky-informe.html.

Newmeyer Kevin, Andres Cubeiro,Sánchez Martha. Ciberespacio, Ciberseguridad y Ciberguerra, ponencia presentada en el II Simposio Internacional de Seguridad y Defensa, Perú 2015. Escuela Superior de Guerra Naval.Lima:22 al 24 de Abril.

Nieva Machín y Manuel Gazapo. (2016). La Ciberseguridad como factor crítico en la seguridad de La Unión Europea. Revista UNISCI , 42, 50-51.

NOTIMEX. (2019). México, entre los países con más ciberataques en AL. Excelsior. Recuperado de https://www.excelsior.com.mx/nacional/mexico-entre-los-paises-con-mas-ciberataques-en-al/1311199

OEA. (2019). Seguridad Cibernética. Organización de Estados Americanos. Recuperado de https://www.sites.oas.org/cyber/Es/Paginas/default.aspx

Omar Olivares. (2016). El paraiso de la Evasión Fiscal: Papeles de Panamá: Latinoamérica saqueada. América Latina en Movimiento, 516, 3-5.

Pedro Huichalaf . (2018). Nueva Política de Ciberdefensa de Chile. Huichalaf.cl. Recuperado de https://huichalaf.cl/nueva-politica-de-chile/

Peter J. Denning and Dorothy E. Denning. (2010). The Profession of IT  Discussing Cyber Attack. Viewpoints, 53, 1.

Secretaría de Gobierno Digital. (2019). ¿Quiénes somos?. Consejo de Ministros. Recuperado de https://www.gobiernodigital.gob.pe/quienes/segdi_quienes.asp

Vidal Vega, J., & Romero Portillo, J. (2010). La denuncia social en Internet: Wikileaks y la filtración de documentos secretos. In La Comunicación Social, en estado crítico. Entre el mercado y la comunicación para la libertad. II Congreso Internacional Latina de Comunicación Social (20 pp.). La Laguna (Tenerife): Sociedad Latina de Comunicación Social, SLCS. Recuperado de https://idus.us.es/xmlui/bitstream/handle/11441/31091/36Vidal.pdf?sequence=1&isAllowed=y

Waltz, K. (1988). The Origins of War in Neorealist Theory. The Journal of Interdisciplinary History, 18(4), 615-628. doi:10.2307/204817

World Economic Forum. (2019). The Global Risks Report 2019 14th Edition. World Economic Forum. Recuperado de https://es.weforum.org/reports/the-global-risks-report-2019

Ximena Cujabante. (2009). La Seguridad Internacional: Evolución de un Concepto. Revista de Relaciones Internacionales, Estrategia y Seguridad. Recuperado de http://www.redalyc.org/pdf/927/92712972007.pdf