CIBERSEGURIDAD COMO HERRAMIENTA FUNDAMENTAL, ANTE LA INMINENTE AMENAZAGLOBAL.

Cybersecurity as A Fundamental Tool In The Face Of The Imminent Global Threat.

Carolina Dibarrat Daniel[1]

Resumen Terminada la Guerra Fría y post atentado al World Trade Center, el mundo sufrió un cambio a nivel digital, gracias al desarrollo de las tecnologías de la información y su expansión debido a la globalización. Las redes computacionales, Internet, Intranet y servicios de inteligencia artificial han visto avances y progreso significativos, traduciéndose en un nuevo escenario político, económico y social, y originando una nueva forma de conflicto. Esto, facilita el surgimiento de un nuevo orden fundamental de estudiar y analizar para descifrar la importancia, gravedad e impacto de esta inminente amenaza. Este estudio se centra en el paradigma de la ciberguerra y su desequilibrio en el sistema internacional como herramienta fundamental de poder, generando una amenaza inminente a nivel global.

Palabras claves: Ciberseguridad - Sistema internacional – Globalización – amenaza - inteligencia artificial.

Abstract After the Cold War and after the World Trade Center's attack, the world underwent a change at the digital level, due to the development of information technologies and their expansion through globalization. Computer networks, the Internet, Intranet, and artificial intelligence services have seen significant advances and progress, creating a new political, economic, and social scenario,and originating a new form of conflict. This, allow the emergence of a new order that is essentialto study and analyze to decipher the importance, severity and impact of this imminent threat. This study focuses on the cyberwar paradigm and its imbalance in the international system, as a fundamental tool of power, generating an imminent threat at a global level.

Key words: Cybersecurity - International system – Globalization – threat - artificial intelligence.

[1] Cientista Política con mención en políticas públicas, diplomada en seguridad internacional y estudios estratégicos. Actualmente se desempeña como Coordinadora de Admisión e investigadora en el CERI en la Universidad del Desarrollo,además de ayudante del ramo de seminario de grado de la misma universidad. Correo electrónico: cdibarratd@udd.cl

Introducción

Durante el periodo de la Guerra Fría existía un dilema de seguridad, que era manejable y evidente frente a conflictos y situaciones riesgosas. Se producía un equilibrio de poder a escala global, que permitía a las grandes potencias resolver o reaccionar de manera de no escalar o acotar el conflicto a un área determinada, ante cualquier amenaza interna o externa.

Este dilema de seguridad, según el académico estadounidense de relaciones internacionales John Hertz, consiste en:

> "una noción estructural en el que los intentos de autoprotección de los estados para cuidarde sus necesidades de seguridad tienden, a dar lugar, independientemente de su intención,a la creciente inseguridad para los demás, ya que cada uno interpreta sus propias medidas como defensivas y las medidas de los demás como una amenaza potencial". (Hertz, 2009)

Al término de la Guerra Fría, el mundo se expuso a un cambio globalizado, debido al incremento de las tecnologías y de Internet, lo que generó, que la información se expandiera y llegara a niveles excepcionales. Lo anterior, ha provocado un problema mundial en cuanto a cómo se ve afectada la seguridad, ante las nuevas amenazas de la llamada ciberguerra o también llamada guerra digital, en la cual se hace referencia al desplazamiento de un conflicto, que toma el ciberespacio y las tecnologías de la información, como campo de operaciones (Vargas, 2015).

La presencia de nuevas redes sociales y tecnologías digitales provocó el incremento acelerado del acceso a la información privilegiada y clasificada, por parte de grupos de poder, que buscan mantener el control militar, político y económico a su alcance.

Realizar una investigación referente a la ciberguerra y su impacto frente al dilema de la seguridad actualmente, es relevante, debido a que esto ha repercutido a nivel global, afectando tanto a países desarrollados como en vías de desarrollo, generando una alteración en la clásica ecuación de equilibrio de poder, que gobierna la seguridad nacional de las principales potencias del orbe.

Así entonces, se ha gestado un nuevo y artificial escenario, en el cual se ejerce una innovadora influencia estratégica digital en el siglo XXI. El escenario denominado ciberespacio, proporciona herramientas para que, hasta los actores más modestos, puedan potencialmente ser una amenaza para las grandes potencias, a través de técnicas y tácticas, que se engloban bajo el concepto de las operaciones militares centradas en redes (Ramirez, 2018).

De acuerdo con lo anterior, se hace evidente que, dentro del ciberespacio, cualquier Estado en términos de una guerra convencional puede tener acceso o hacer uso del poder blando, aquel que definimos como, el que utiliza un país para alcanzar sus objetivos, a través de la vía

diplomática, sin el uso de la fuerza militar.

Sin embargo, en el actual escenario de la ciberguerra, el Estado más débil acrecienta su poder por medio del empleo de armas cibernéticas, que le proporcionan accesibilidad para amenazar en puntos vulnerables a Estados más fuertes (2015).

Es por esto, que, en el contexto del nuevo paradigma cibernético, emerge la potencialidad de que Estados con evidente menor capacidad militar y económica, puedan desestabilizar a Estados más poderosos, emergiendo una nueva forma de desequilibrio de poder, que se manifiesta como una versión actualizada del desarrollo de capacidades asimétricas.

En consecuencia, este documento tendrá como centro de gravedad principal, aceptar o rechazar la hipótesis, que tiene relación con la importancia de la ciberseguridad como una herramienta fundamental para evitar el desequilibrio de poder, como amenaza global, para ser utilizada por Estados y/ u organizaciones con el propósito de satisfacer sus propios intereses. Por ende, es necesario a través de este estudio aclarar si es que, en el actual orden internacional, ¿es factible que, mediante el empleo de tecnología contextualizada en el concepto de la ciberguerra, un Estado, organización, y/o grupo de individuos pueda amenazar, neutralizar o destruir la infraestructura crítica y de defensa de un Estado desarrollado?

Desarrollo

Durante los últimos 10 años, se puede observar cómo ha existido un gran auge de los llamados "ciberataques" a diversas empresas y entidades privadas y estatales, con el fin de producir daño o hurto de información confidencial, lo cual permite visualizar que es necesario implementar una política regional de ciberseguridad al menos en América Latina, que permita que los países tengan opciones de apoyarse mutuamente ante este tipo de agresión/atentado, que tendría la capacidad de obstaculizar procesos infraestructurales completos en los países de la región.

Es posible verificar que entre los años 2016 hasta junio de 2019, la mención a la palabra ciberseguridad en búsquedas, ha aumentado de 20 a 100 (scored points in Google Trends). Esto ha permitido dejar al descubierto, que cada vez más aumenta la utilización de este medio para generar obstrucción en el medio digital y lograr generar desequilibrios a nivel global (IDB, 2020).

Dada esta situación, muchos usuarios han considerado la relevancia de capacitaciones en el ámbito digital y de poder sumar conocimientos en la red para poder manejarla y así llegar a evitar ciertas circunstancias de peligro en la red, que podrían eventualmente destruir la infraestructura física y alterar bases de datos con información clasificada.

Debido a todo lo descrito anteriormente, es que la OEA (Organización de Estados Americanos) y el BID (Banco Interamericano de Desarrollo), han visto la importancia de implementar el Modelo de Madurez de la Capacidad de Ciberseguridad para las naciones (CMM), con la finalidad de poder

medir el crecimiento y desarrollo de los países miembros, para poder defenderse ante este tipo de ciber amenazas en la red (IDB, 2020).

Las dos instituciones mencionadas, se encuentran satisfechas en torno a la importancia que ha adquirido este tema dentro de la agenda política y económica de los Estados de la región. Es por esto, que se han creado e implementado diversos programas de capacitación en ciberseguridad por parte de la OEA para que, sobre todo, usuarios del ámbito público (gobierno, municipalidades, etc.), tengan opciones de capacitarse cada vez más en herramientas para evitar caer en ciber espionajes y en chantajes virtuales (CICTE, 2021).

Evolución de Amenazas y Riesgos en el Ciberespacio

En el estudio e investigación de las Relaciones Internacionales, el término "amenaza" es reciente y escasamente utilizado para caracterizar situaciones, en donde existe un potencial peligro para el sistema internacional. Generalmente la amenaza como concepto, se emplea para referirse a una preocupación estratégica de esencia militar, y vinculada con las Fuerzas Armadas en la nueva correlación que surgió a partir del fin de la Guerra Fría (Saint-Pierre, 2002).

Usualmente, vinculamos subjetivamente el término "amenaza" con la palabra temor, dando a entender que, este concepto es utilizado por los actores internacionales como un mecanismo, que coopere a la consecución de los objetivos de una nación, en el contexto político y estratégico sin necesariamente tener que llegar a la acción bélica misma.

Desde un punto de vista etimológico "amenaza", deriva de la palabra latina Minacia, la cual puede tener 3 significados diferentes:

- Palabra o gesto intimidatorio
- Promesa de castigo o maleficio
- Preanuncio o indicio de cosa desagradable o temible, de desgracia o dolencia.

En consecuencia, en los 3 casos se puede visualizar un componente común, que tiene relación con enviar una señal de peligro o maleficio a otro actor del sistema internacional.

Dado lo anterior, se vislumbra que la amenaza provoca temor ante la posibilidad de perder el estado de Seguridad. Como señal, representa en nuestra percepción, aquello que nos preocupa o intimida. Por tanto, es precisamente ésta, la que permite al amenazado tomar decisiones y medidas preventivas, para protegerse de la agresión implícita en dicha amenaza (Saint-Pierre, 2002).

Dado el eficiente y rápido desarrollo de la globalización y la expansión de Internet y las tecnologías de la información, la red global creada a fines del siglo XX ha evolucionado generando un campo cibernético muy consolidado, que, sin embargo, requiere de ciertas regulaciones debido a sus constantes peligros y amenazas que han surgido paralelamente a ella.

En la red, podemos encontrar diversos virus, gusanos y una variedad de instrumentos utilizados para el espionaje digital, que se han desarrollado a lo largo del siglo XXI, convirtiendo al ciberespacio en un potencial escenario con diferentes inseguridades permanentes, que pueden generar grave daño, irreversible para personas, instituciones, organizaciones y Estados.

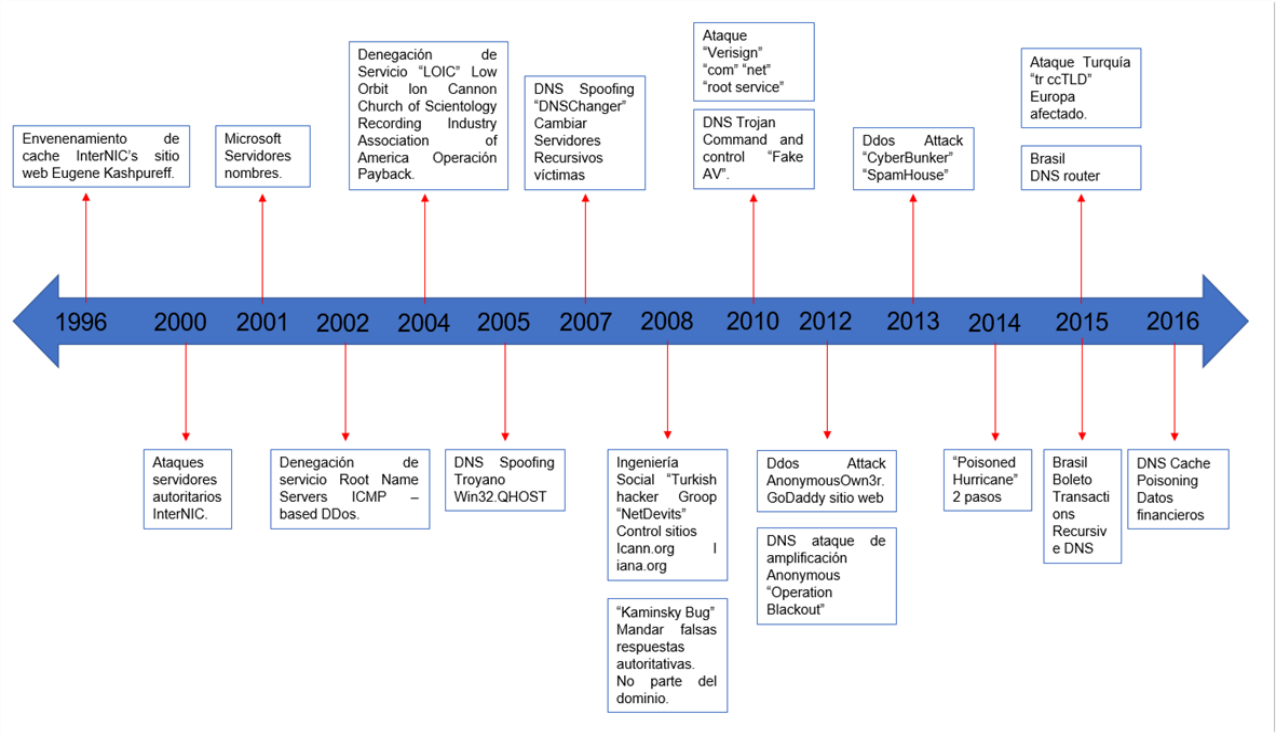
Los antecedentes, nos permiten aseverar que existe una evidente gradualidad de incremento de las amenazas no solo a privados, sino que a organizaciones, empresas e infraestructura que compromete todos los servicios de un Estado.

Probablemente, es la amenaza a la infraestructura crítica, el mayor efecto que puede producir un ataque cibernético a los servicios esenciales en una sociedad. Una definición combinada del tema nos permite aseverar que: La infraestructura Crítica son todos aquellos sistemas físicos o virtuales que facilitan funciones y servicios esenciales para apoyar a los sistemas más básicos a nivel social, económicos, medioambientales y políticos. Una alteración o interrupción en su funcionamiento debido a causas naturales (por ejemplo: una inundación que afecta al suministro eléctrico) o provocada por el hombre (por ejemplo: un atentado terrorista o un ataque cibernético a una central nuclear o a una entidad financiera) podría llevar graves consecuencias. (ISBL, 2020)

Las amenazas también se pueden producir sobre los datos de carácter privado de las personas. En consecuencia, la información que mantienen instituciones financieras, salud, impuestos internos, entre otras, constituye un activo esencial para las organizaciones; debiendo desarrollar mecanismos de protección ante amenazas que alteren o dañen la privacidad de la información.

Un claro ejemplo de lo anterior es el masivo robo de contraseñas que sufrió el proveedor de servicios de Internet Yahoo. El hecho aconteció cuando un conjunto de hackers llamados D33Ds Company, vulneraron los sistemas computacionales, a través de consultas SQL, logrando robar 450.000 claves (CSO computer world, 2012).

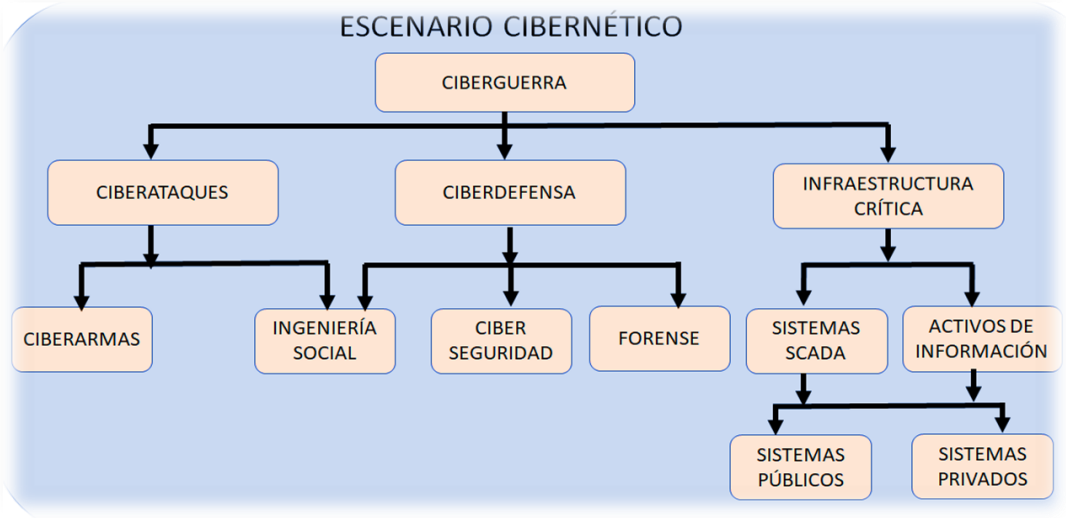
La figura 1.1 Evolución que han tenido las amenazas por Internet los últimos años.



Fuente: Adaptado de Corletti (2005)

La evolución de las amenazas, han generado una estructura sistémica de la ciberguerra, que para propósitos de esta investigación se estructura conforme a la figura 1.2

Figura 1.2. Estructura Sistémica de las amenazas.



Fuente. Elaboración propia

Respecto a los instrumentos de los ciberataques, se han clasificado en diversas categorías como ciberincidentes, ciberdelitos, ciberterrorismo, ciberespionaje.

Finalmente, la sistematización que se propone en esta investigación considera a la ciberseguridad en su contexto de la estrategia a desarrollar por los Estados y organizaciones para defenderse de acciones agresivas en el espectro digital. Así mismo, se ha incorporado como parte de la ciberseguridad el concepto de forense, que implica los procesos tecnológicos que permiten entregar una trazabilidad respecto a la identidad de intrusos, usuarios afectados, software empleado, bases de datos corrompidas o usurpadas, entre otros, que tiene validez legal al momento de iniciar una controversia internacional respecto a quién causó grave daño en los sistemas computacionales de un Estado u organización determinada.

A su vez, existe el término de "Riesgo" que para la academia es considerado como la probabilidad de que se produzca un evento y sus respectivas consecuencias negativas.

En términos de concepto, "es el entorno complejo resultante de la interacción entre las personas, el software y los servicios de Internet por medio de dispositivos tecnológicos conectados a redes, las cuales no existen en ningún tipo de forma física" (LDGRUPO, 2019).

En cuanto a riesgo en la seguridad de la información, se puede visualizar una clasificación relevante para poder determinar el grado de impacto (LDGRUPO, 2019).

1. *Riesgo Residual*: Aquel remanente que existe después de que se hayan tomado las medidas adecuadas de seguridad.
2. *Riesgo de Aceptación*: Es la decisión informada para tomar un riesgo específico.
3. *Análisis de Riesgos*: Proceso que se toma para poder comprender la naturaleza y el nivel del riesgo.
4. *Evaluación de Riesgos*: Proceso donde se identifica, se analiza y evalúa.
5. *Estimación de Riesgos*: Proceso de comparación de resultados para determinar magnitud.
6. *Gestión de Riesgos*: Actividades coordinadas que dirigen y controlan a una organización en un determinado riesgo.
7. *Tratamiento de Riesgo*: Proceso que se requiere para modificar el riesgo.

La clasificación propuesta, permite poder realizar un análisis preliminar respecto a cómo los conceptos de Poder, Asimetría y su consecuencia de Desequilibrio, son afectados derivado de la alteración de la Infraestructura Crítica de un Estado.

En efecto, si se considera que existe una correlación positiva entre el poder asociado a un Estado y la envergadura de su Infraestructura Crítica; ¿Cómo podría un Estado de menor tamaño tener la capacidad de alterar los equilibrios de poder, a pesar de la manifiesta debilidad de uno con respecto a otro que produce la asimetría?

Amenazas Futuras

En el contexto de evolución de las amenazas y sus proyecciones futuras, esta investigación ha procedido a realizar un análisis prospectivo en función de la evidencia, que es posible de detectar en las tendencias de las tecnologías de la información, computación e inteligencia artificial. Con estos antecedentes, se ha procedido a describir las principales futuras amenazas.

Internet de las Cosas: Al propagarse la cantidad de número IP que existen en los potenciales artefactos electrónicos, que existen en los hogares, oficinas, fábricas, edificios públicos, etcétera, se acrecentará la posibilidad que los hackers naveguen a través de dichos artefactos, llegando mediante ellos a vulnerar datos, bases de datos, software, entre otros (Alcaraz.M, 2014).

Computación Cuántica: Derivado del potencial cambio de tecnología en los procesadores, la capacidad de cómputo se aumentará en niveles insospechados, proporcionando a los hackers, nuevas herramientas para vulnerar los sistemas privados (Vélez. M & Sicard, 2000).

Exceso de automatización y control a través de software: En los próximos años se debe asumir que gran parte de las tareas de manufactura y aquellas repetitivas serán realizadas por robot y software controlados desde sistemas computacionales centralizados. Lo anterior, implicará mayores vulnerabilidades, en donde hackers podrían alterar los sistemas productivos y financieros. En consecuencia, a medida que se incremente la automatización se incrementarán las vulnerabilidades si no se realizan medidas de ciberdefensa acorde a las nuevas tecnologías (Boasson, 1993).

Centralización de datos y almacenamiento en la nube: El incremento del almacenamiento en la "nube", por parte de proveedores de este servicio como Google y Microsoft, desarrollará intentos de Estados emergentes y hackers independientes por penetrar y alterar, modificar o hurtar datos de la nube, en consecuencia, se deberá esperar para los próximos años intentos reiterados por vulnerar estos nuevos sistemas de almacenamiento de datos (Aguilar, 2009).

Sistemas SCADA: La dependencia de la infraestructura crítica de los sistemas de control centralizados, generará un esfuerzo permanente de los hackers perteneciente a Estados u organizaciones, para alcanzar y vulnerar dichos sistemas, lo que podría producir un efecto estructural, por efecto "dominó", en la continuidad de los servicios de un país (Pérez-López, 2015).

Inteligencia artificial: Las nuevas técnicas de algoritmos y heurísticas, desarrolladas con computadores cada vez más poderosos podrán amenazar con mayor eficiencia a los sistemas de países y organizaciones privadas, por tanto, estas técnicas de inteligencia artificial maliciosas deberán ser contrarrestadas con desarrollos similares que protejan con procedimientos digitales inteligentes a los datos públicos y privados (Trillas, 1998).

Construyendo capacidades de Ciberseguridad

Con fecha 1 de octubre del 2021, Joe Biden, el presidente de los Estados Unidos, en una declaración compartida por CNN, convocó a 30 países a una reunión, con la intención de intensificar los esfuerzos globales para hacer frente a la amenaza del ramsomware dentro de la seguridad económica y nacional.

Según el asesor de seguridad nacional, Jake Sullivan, "Las amenazas cibernéticas afectan a las vidas y sustentos de las familias y las empresas de Estados Unidos", y aseguró: la administración "continuará construyendo sobre el esfuerzo en conjunto del gobierno para disuadir e impedir los ciberataques". El objetivo de la alianza será "acelerar nuestra cooperación en la lucha contra la ciberdelincuencia, mejorar la colaboración de las fuerzas de seguridad, frenar el uso ilícito de las criptomonedas y comprometerse en estas cuestiones de forma diplomática", según anunció Biden.

En un comienzo, la primera reunión será de manera virtual, permitiendo que todos los países realicen un esfuerzo continuo para cortar el ingreso de los grupos de ramsomware y buscar las formas más eficientes de perseguirlos.

Esta situación permite dilucidar que es necesario generar conocimiento y diversas capacitaciones a distintos niveles de educación por parte de los estados hacia sus ciudadanos, con el fin de que exista una mayor preparación ante una posible amenaza o ataque dentro del área cibernética. Para enfrentar este escenario complejo, lleno de riesgos, se hace necesario resguardar y proteger los derechos de las personas naturales y jurídicas.

Modelo de Madurez de la Capacidad de Ciberseguridad para las naciones.

El Modelo de Madurez de la Capacidad de Ciberseguridad para las Naciones (CMM) fue desarrollado por el Centro Global de Capacidad en Seguridad Cibernética (GCSCC) de la Universidad de Oxford.

Este modelo ha permitido generar estudios donde se puede comprobar el nivel de desarrollo tecnológico que tienen los países que lo integran, y su nivel de protección frente a amenazas y ataques cibernéticos. Con ello, es factible determinar el nivel de madurez de los países en materia de educación, formación y desarrollo de capacidades en el ámbito de las tecnologías de información (IDB, 2020).

El actual informe permite corroborar la dispar desigualdad económica, social y cultural que existe en la región de América Latina y el Caribe.

En una primera instancia, tenemos un grupo de países que representa un tercio del total analizado, los cuales en los últimos dos años han incrementado sus índices en áreas como educación y capacitación, alcanzado niveles intermedios. Uno de los casos más relevantes ha sido Uruguay, logrando un nivel estratégico de capacitación profesional. También se encuentran en este nivel México, Argentina, Chile, Costa Rica Colombia, Paraguay, República Dominicana, Trinidad y Tobago (IDB, 2020).

Estos son países que cuentan en general con una política o estrategia nacional de ciberseguridad y que la han ido desarrollando en base a criterios educativos, tanto públicos como privados, considerando tanto el punto de vista técnico como jurídico.

A su vez, el informe de Madurez da cuenta de aquellos países que tienen escaso o nulo avance en el nivel de desarrollo en temas cibernéticos, dentro de la región de América Latina y el Caribe.

Es por lo descrito anteriormente, que se hace necesario y de suma relevancia generar una política regional dedicada a capacitar en área de ciberseguridad, permitiendo crear estrategias y mecanismos de cooperación internacional, con el fin de que aquellos que han tenido avances significativos, tengan la opción de poder ayudar y colaborar con aquellos que están en gran desventaja (IDB, 2020).

Asimismo, se hace relevante destacar que se requiere un avance en el desarrollo de programas multidisciplinarios, los cuales permitan la formación y capacitación de profesionales integrales, que tengan la habilidad de reacción frente a diversas situaciones de riesgo y con distintas perspectivas. Esto implica, la incorporación no solo de profesionales y técnicos especialistas del área de las TI y ciberseguridad, sino que también contar con profesionales del área de las ciencias sociales, tales como derecho, ciencia política, ingeniería comercial, comunicación social, entre otros (IDB, 2020).

Mediante el intercambio de información y la constante colaboración entre países, permite generar un círculo virtuoso, que convoque a crear diversas medidas de confidencialidad, seguridades técnicas y jurídicas, otorgándole a los países menos desarrollados, alcanzar de manera más rápida y eficiente niveles tecnológicos y de protección digital más audaces, consiguiendo mejores niveles de madurez estratégicos y dinámicos, que tengan la habilidad de adaptarse a diversos escenarios, pudiendo identificar correctamente los tipos de riesgos y vulnerabilidades que deban enfrentar.

Etapas del Modelo de Madurez

1. *Inicial*: No existe nivel de madurez en ciberseguridad, es posible que existan discusiones iniciales acerca del tema, pero sin tomar medidas específicas.
2. *Formativa*: Ciertos aspectos comenzaron a formularse y desarrollarse, pero podrían estar mal organizados o esquematizados.
3. *Consolidada*: Los indicadores están listos y funcionando. Pero, no se han destinado mayores recursos a la implementación.
4. *Estratégica*: Etapa en la que se toman las decisiones de qué indicadores utilizar y cuales son poco relevantes para la organización.
5. *Dinámica*: Ya hay mecanismos claros para poder llevar a cabo investigaciones profundas en materia de ciberseguridad. Existe sofisticación tecnológica y las estrategias están consolidadas para enfrentar cambios.

La evaluación para avanzar de un nivel a otro está dividida en cinco dimensiones, las cuales corresponden a ámbitos esenciales y específicos de la ciberseguridad (IDB, 2020).

Figura 2. Dimensiones de Ciberseguridad

Dimensión 1 Política y Estrategia de Ciberseguridad (Diseño de estrategia y resiliencia de ciberseguridad)	**D1.1** Estrategia Nacional de Ciberseguridad **D1.2** Respuesta a Incidentes **D1.3** Protección de Infraestructura Crítica (IC) **D1.4** Gestión de Crisis **D1.5** Defensa Cibernética **D1.6** Redundancia de Comunicaciones
Dimensión 2 Cultura Cibernética y Sociedad (Fomentar una cultura de ciberseguridad responsable en la sociedad)	**D2.1** Mentalidad de Ciberseguridad **D2.2** Confianza y Seguridad en Internet **D2.3** Comprensión del Usuario de la Protección de Información Personal en Línea **D2.4** Mecanismos de Presentación de Informes **D2.5** Medios y Redes Sociales

Dimensión 3 Educación, Capacitación y Habilidades en Ciberseguridad (Desarrollo del conocimiento de ciberseguridad)	**D3.1** Sensibilización **D3.2** Marco para la Educación **D3.3** Marco para la Formación Profesional
Dimensión 4 Marcos Legales y Regulatorios (Creación de marcos legales y regulatorios efectivos)	**D4.1** Marcos Legales **D4.2** Sistema de Justicia Penal **D4.3** Marcos de Cooperación Formal e Informal para Combatir el Delito Cibernético
Dimensión 5 Estándares, Organizaciones y Tecnologías (Control de riesgos a través de estándares, organizaciones y tecnologías)	**D5.1** Adhesión a los Estándares **D5.2** Resiliencia de Infraestructura de Internet **D5.3** Calidad del Software **D5.4** Controles Técnicos de Seguridad **D5.5** Controles Criptográficos **D5.6** Mercado de Ciberseguridad **D5.7** Divulgación Responsable

Fuente: IDB, 2020.

Ciberseguridad en Chile

La Política Nacional de Ciberseguridad de Chile (PNC), recoge de forma detallada el desarrollo de tareas a corto y largo plazo, así como las instituciones que intervienen en asuntos de ciberseguridad.

El cumplimiento de los objetivos recogidos en la PNC chilena tiene como horizonte el año 2022. Además, incluye un apartado con 41 medidas de política pública a llevar a cabo en el periodo 2017 – 2018, así como el órgano responsable de la implementación de cada una de ellas (IDB, 2020).

Los objetivos para el año 2022 son seis, cada uno de los cuales contiene una serie de objetivos específicos, sumando estos un total de 22. A continuación, se exponen los objetivos generales:

1. *Desarrollar una infraestructura de las TIC que, bajo una óptica de gestión de riesgos, sea capaz*

de resistir y recuperarse de incidentes de ciberseguridad (BCN, 2019).

2. *Garantizar los derechos de los ciudadanos en el ciberespacio* (BCN, 2019).
3. *Desarrollar una cultura de ciberseguridad en torno a la responsabilidad en el uso de lasTIC, a las buenas prácticas y a la educación* (BCN, 2019).
4. *Establecer relaciones de cooperación con otros actores en materia de ciberseguridad y participar de forma activa en foros internacionales* (BCN, 2019).
5. *Desarrollar una industria de la ciberseguridad chilena, que sea útil a los objetivos estratégicos del país* (BCN, 2019).

Procediendo posteriormente a revisar la estructura institucional, la PNC prevé que una ley contemple tanto dicha estructura como un modelo de gobernanza de ciberseguridad. Además, también se plantea evaluar la creación de un consejo consultivo asesor (PNCS-gob.chile, 2015).

De forma transitoria, a nivel técnico, el CSIRT del Gobierno, es la instancia encargada de gestionar los incidentes generados en la Red de Conectividad del Estado, mientras que a nivel político se prorroga el mandato del Comité Interministerial sobre Ciberseguridad, cuyas funciones se circunscriben a los ámbitos de la comunicación, coordinación y seguimiento de las medidas contenidas en la PNC (CSIRT.gob, 2019).

Finalmente, se debe destacar que se creó una Alianza Chilena de Ciberseguridad, integrada por nueve instituciones que representan zonas relevantes a lo largo del país; mediante reconocidos organismos estatales, privados y de la academia, quienes tienen como objetivo cooperar con las autoridades en esta materia, generar y crear nuevas redes de contacto y alianzas internacionales. Promoviendo y desarrollando el fortalecimiento de la ciberseguridad en Chile (IDB, 2020).

En conclusión, podemos identificar que el aporte del Programa de Chile se sintetiza en la matriz que se describe en la Tabla 1.1, donde se identifican tres atributos por cada tema expuesto en dicho programa.

Tabla 1. Atributos del Programa de Chile

Chile	Atributo 1	Atributo 2	Atributo 3
Respecto a la Política Nacional.	Política Nacional de Ciberseguridad, detallada de tareas de corto y largo plazo.	41 medidas de política pública (período 2017-2018).	Para el año 2022, existen seis objetivos que se desean concretizar.
Respecto a lasmedidas de políticaspúblicas.	-Desarrollar un a infraestructura de las TIC, que, bajo una mirada de gestión de riesgos, permite recuperarse de incidentes cibernéticos.	-Garantizar los derechos de losciudadanos en elciberespacio.	- Desarrollar una cultura de ciberseguridad en torno a la responsabilidad en el uso de las TIC, a las buenas prácticasy a la educación.
Respecto a políticas públicas y medidas internacionales.	-Establecer relaciones de cooperación con otros actores en materia de ciberseguridad y participar de forma activa en foros internacionales.	-Desarrollar una industria de la ciberseguridad chilena, que sea útil a los objetivos estratégicos del país.	-Se crea ley que contempletanto dicha estructura como un modelo de gobernanza de ciberseguridad. -Creación de Alianza Chilena de Ciberseguridad compuesta por 9 instituciones.

Fuente: Elaboración Propia.

Dada la información expuesta, se puede contemplar que, en Chile, se visualiza una Política Nacional de Ciberseguridad, detallada de tareas de corto y largo plazo, que abarcarían desde el período 2017 al 2022.

Se busca desarrollar una infraestructura crítica de las TIC, que permita recuperarse de incidentes cibernéticos.

A su vez, busca garantizar los derechos de los ciudadanos en el ciberespacio y desarrollar una cultura de éste, en torno a la responsabilidad en el uso de la TIC, a las buenas prácticas.

Permite establecer relaciones de cooperación con otros actores en materia de ciberseguridad y desarrollar una industria de ésta en Chile, que sea útil a los objetivos estratégicos del país.

Para finalizar, cabe destacar que se crea una ley que contemple dicha estructura y a la vez un modelo de gobernanza de Ciberseguridad; junto con la creación de la Alianza Chilena de la Ciberseguridad, compuesta por nueve instituciones.

Reflexiones Finales

Dentro de líneas de investigaciones futuras, se puede observar que esta temática es de gran relevancia y trascendencia para el estudio de la seguridad física y digital que rodea el entorno del planeta.

Es fundamental considerar toda estrategia de ciberdefensa y programas de ciberseguridad para poder combatir y prevenir diversos posibles ataques en el espacio cibernético, los cuales podrían generar daños irreparables en distintos ámbitos de la sociedad creando pánico y caos incontrolable.

La revolución tecnológica ha alcanzado un nivel de desarrollo y expansión, lo suficientemente poderoso y profundo, que las tecnologías de información y el Internet, junto con el espacio digital, se han convertido en blancos de ataque ante cualquier amenaza existente por parte de terroristas, delincuentes, hackers y grupos revolucionarios.

Esta situación, ha generado que se haya vuelto primordial investigar y ejecutar diversos programas de ciberseguridad, basados en leyes y normativas acorde y adecuada con el avance tecnológico y la masiva expansión de la redes comunicacionales y sociales. Lo que ha dado cabida, a diversos hechos en que el individuo o usuario se ha visto protegido frente a amenazas o ataques de carácter digital, que le coartarían la libertad y le provocarían daños o perjuicio a su vida diaria.

Finalmente, se debe profundizar en el estudio y avance que han tenido los distintos países en materia de ciberseguridad, frente al progreso y crecimiento de la globalización y su entorno tecnológico. Esto resulta ser muy determinante al momento de legislar sobre ciertos hechos o condiciones que han suscitado a raíz de este cambio de paradigma, lo que ha dado curso a distintas acciones en cuanto a políticas públicas referidas a ciberseguridad y el cómo detener la llamada ciberguerra; el cual se convierte en el nuevo escenario de conflicto bélico del siglo XXI.

Para lograr alcanzar una superioridad tecnológica, se deberá disponer de una industria nacional de defensa impulsada y protegida por un conjunto de políticas que sean inclusivas. Aquellos países que no cuenten con el desarrollo e infraestructura técnica necesaria para disponer de una industria nacional de defensa tendrán que depender crónicamente de un tercero.

Consecuentemente, en los párrafos precedentes podemos encontrar la respuesta a la pregunta planteada en la introducción de este artículo, donde la amenaza de orden cibernética está presente y puede ser usada por diferentes organizaciones o estados.

Para finalizar, esta investigación permitió esclarecer, cuáles podrían ser los efectos de la ciberguerra como factor de poder entre estados de tamaño disímil, permitiendo aceptar que es necesario por sobre manera, generar capacitaciones y desarrollo multidisciplinar en distintas áreas educativas, con la finalidad de poder prevenir y contrarrestar de manera eficiente y eficaz, la nueva amenaza inminente de la cibernética.

Referencias:

ACC. (2018). Alianza Chilena de Ciberseguridad. Obtenido de: https://www.alianzaciberseguridad.cl/#somos

Aguilar, L. J. (2009). La Computadora en nube (Cloud Computing): El nuevo paradigma tecnológico para empresas y organizaciones. Revista Icade, 76.

Alcaraz.M. (2014). Internet de las Cosas. Obtenido de Universidad Católica: http://digibuo.uniovi.es/dspace/handle/10651/13140

BCN. (2019). Ley Chile. Obtenido de https://www.bcn.cl/leychile/navegar?idNorma=1138479

Boasson, M. (1993). Control systems software, IEEE Transaction on automatic control.

Buzan, B. (1983). People, States, and Fear. The National Security Problem in International Relations. Brighton : Wheatsheaf Books.

Centro de estudios avanzados en niñez y juventud. (2013). Desarrollo teórico de la Resiliencia y su aplicación en situaciones adversas: Una revisión analítica. Revista latinoamericana de ciencias, niñez y juventud, 67-68.

CICTE. (2021). OEA. Obtenido de: https://www.oas.org/es/centro_noticias/comunicado_prensa.asp?sCodigo=AVI- 094/21

Comité Interministerial sobre ciberseguridad. (2017). Política Nacional de Ciberseguridad: 2017-2022.

Constitución Política de Chile. (2005).

Corletti, A. (2005). Especialización en Estrategia Operacional y Planteamiento. Obtenido de http://www.cefadigital.edu.ar/bitstream/1847939/1171/1/TFI%2019- 017%20GOMEZ.pdf

CSIRT.gob. (2019). Comité de Ciberseguridad Nacional. Obtenido de: https://www.csirt.gob.cl/sistemas-y-herramientas/

CSO computer world. (2012). Obtenido de https://cso.computerworld.es/alertas/yahoo- resuelve-la-vulnerabilidad-que-permitio-el-robo-de-contrasenas

De Carlos, Javier. (2017). Tendencias Globales, Seguridad y Resiliencia. Obtenido de Instituto Español de Estudios Estratégicos: http://www.ieee.es

Dirección del Personal del Ejército. (2019). Programa de Resiliencia y Bienestar del Ejército. Programa. Santiago, Chile: Estado Mayor General del Ejército.

Ejército de Chile. (2012). RDI-20001 Reglamento "Inteligencia". Santiago: División Doctrina.

Ejército de Chile. (2012a). RDI-20001 Reglamento "Inteligencia". Santiago: División Doctrina.

Ejército de Chile. (2012b). RDI-20002 Reglamento "Inteligencia Función Secundaria". Santiago: División Doctrina.

Ejército de Chile. (2015). RDI-20005 Proceso de Integración del Campo de Batalla. Santiago: División Doctrina.

Ejército de Chile. (2016). MOLD 02005 Manual Ethos del Ejército de Chile. (CEDOC, Ed.) Santiago, Chile: CEDOC.

Ejército de Chile. (2016). RDPL-20001 Proceso de las Operaciones. Santiago: División Doctrina.

Ejército de Chile. (2021). RDP 20001 "Reglamento de Apoyo Administrativo". Santiago: Comando de Educación y Doctrina.

Ferrada, E. (2020). La Seguridad Nacional: ¿es necesaria su definición positiva en el derecho nacional? Escenarios Actuales, 25(2), 29-48.

Gaete Moreno, A. (Septiembre de 2020). La importancia de la resiliencia militar en un ambiente híbrido. EL CONFLICTO HÍBRIDO Y SUS EFECTOS EN LA CONDUCCIÓN OPERACIONAL Y TÁCTICA, 120-125.

García Silgo, M. &. (Marzo de 2013). Universidad Complutense de Madrid. Obtenido de ucm: http://www.ecm.es

Garcia-Vesga, M. C., & Domínguez-de la Ossa, E. (2013). Desarrollo teórico de la Resiliencia y su aplicación en situaciones adversas: Una revisión analítica*. Revista Latinoamericana de Ciencias Sociales, Niñez y Juventud, 11(1), 66-67.

Guzmán, J. (1985). Seguridad Nacional en la Constitución de 1980. Revista de Derecho Público, 45-65.

Hertz. (2009). El dilema de la seguridad.

IDB. (2020). Observatorio ciberseguridad. Obtenido de Ciberseguridad: https://publications.iadb.org/publications/spanish/document/Reporte- Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y- el-Caribe.pdf

ISBL. (2020). Instituto de Seguridad y Bienestar Laboral. Obtenido de https://isbl.eu/2020/03/que-son-las-infraestructuras-criticas/

Juanes-Cuartero, A. P. (22 de Mayo de 2012). Instituto Español de Estudios Estratégicos. Recuperado el 2021, de ieee.es: http://www.ieee.es

Koch, S., & Gallardo, M. (2015). Evolución y condicionantes de las nociones de Seguridad y Defensa. En ACAGUE, La Seguridad de Chile: Los desafíos para el sector Defensa en el Siglo XXI (págs. 25-44).

LDGRUPO. (2019). Obtenido de https://www.ldgrupo.com.pe/que-es-el-riesgo-de-seguridad-de-información/

Ministerio de Defensa de España. (Julio de 2016). Guía para mandos sobre apoyo psicológico en operaciones. Grupo de trabajo de la OTAN RTO/HFM 081/RTG 020 sobre estrés y apoyo psicológico en las operaciones militares actuales. Madrid, España: Ministerio de Defensa de España.

Ministerio de Defensa Nacional. (2018). DNC 2-0 Doctrina de Inteligencia Conjunta de las Fuerzas Armadas. Santiago: Ministerio de Defensa Nacional de Chile.

Ministerio de Defensa Nacional. (2021a). DNC 2-01 Manual de Inteligencia Conjunta. Santiago: Ministerio de Defensa Nacional de Chile.

Ministerio de Defensa Nacional. (2021b). DNC 2-05 Preparación de Inteligencia del Ambiente Operacional Conjunto. Santiago: Ministerio de Defensa Nacional de Chile.

Ministerio de Defensa Nacional. (2021c). DNC 5-0 Doctrina para la Planificación Conjunta. Santiago: Ministerio de Defensa Nacional de Chile.

Ministerio de Defensa Nacional de Chile. (4 de Diciembre de 2020). Política de Defensa Nacional de Chile 2020. Santiago, Chile: Ministerio de Defensa Nacional.

Ministerio de la Defensa Nacional. (2017). Libro de la Defensa Nacional de Chile. Ministerio de la Defensa Nacional. (2020).

Política de Defensa Nacional de Chile. Ministerio del Interior y Seguridad Pública. (2018). Acuerdo Nacional por la Seguridad Pública.

Norma Ivonne González-Arratia López Fuentes, J. L. (Enero de 2013). Resiliencia y factores protectores en menores infractores y en situación de calle. Psicología y Salud, 22(1), 50.

Organización del Tratado del Atántico Norte. (20 de Mayo de 2021). Página web de las OTAN.Recuperado el 2021, de OTAN: https://www.nato.int/docu/review/articles/2021/05/20/countering-cognitive-warfare-awareness-and-resilience/index.html

Pérez-López, E. (2015). Los sistemas SCADA en la automatización industrial. Revista Tecnología en Marcha, 28(4), pág.3.

PNCS-gob.chile. (2015). Política Nacional de Ciberseguridad. Obtenido de

https://www.ciberseguridad.gob.cl/media/2017/05/PNCS-CHILE-FEA.pdf

Ramirez, P. J. (2018). Los nuevos campos de batalla.

Real Academia Española. (30 de Noviembre de 2021). Diccionario de la Lengua Española. Obtenido de https://dle.rae.es/

Rosental, M. M., & Lidin, P. F. (1965). Diccionario Filosófico. Montevieo: Ediciones Pueblos Unidos.

Saint-Pierre, H. L. (2002). Las nuevas amenazas como subjetividad perceptiva.

Subsecretaría para las Fuerzas Armadas. (9 de Julio de 2019). Decreto Nº 265. Autoriza colaboración y delega en el Ministro de Defensa Nacional las facultades en las materias que indica. Santiago, Metropolitana, Chile.

Trillas, E. (1998). La inteligencia artificial: máquinas y personas. Temas de Debate, S.A.

Vargas.R. (2015). Ciberseguridad: ¿Estamos preparados en América Latina y el Caribe?

Vélez. M & Sicard, A. (2000). Computación cuántica: Una perspectiva de lo contínuo. Revista Universidad EAFIT, 25, 41-46.

Zegart, A. (1999). Flawed by design, the evolution of the CIA, JCS and NSC. Standford University Press.