UNIVERSIDAD INTERNACIONAL DE LAS AMÉRICAS

FACULTAD DE RELACIONES INTERNACIONALES

TÍTULO DE LA INVESTIGACIÓN:

LA MILITARIZACIÓN DEL CIBERESPACIO Y SU IMPACTO EN LOS CONFLICTOS INTERNACIONALES: ESTRATEGIAS, RIESGOS Y DESAFÍOS PARA LA SEGURIDAD GLOBAL EN EL PERIODO 2020-2025

MÓNICA DELGADO MARÍN

San José, Julio, 2025

Planteamiento del Problema

El avance del ciberespacio se ha venido intensificando desde décadas atrás, con el ingreso de las tecnologías en cada campo de la realidad actual, ha logrado crear nuevas configuraciones a nivel social, político o económico, buscando crear nuevas conexiones, nuevos actores y mecanismos de poder, dando a conocer cómo nacen espacios diferentes de interacción.

Cada uno de estos elementos que se observan, creciendo dentro del contexto del ciberespacio, así como los actores que vienen a desempeñar funciones y atractivos dentro de este, va a ocasionar de manera paulatina la puesta en práctica de procesos defensivos por parte de cada Estado, cada actor u organismo privado.

Para contextualizar (Ramón, 2018 como se citó en Chaves y Jurado, 2019), define el ciberespacio de la siguiente manera; "realidad simulada o artificial de una persona en su entorno virtual y no físico, desarrollado a través de herramientas informáticas." Con relación al texto anterior, queda claro que se considera un ámbito de acción diferente, donde se intercambia de manera constante la información de las personas, las empresas, el sector público y privado, por ende, actores que vienen a descubrir las posibilidades de desarrollo, pero también, las vulnerabilidades que pueden afectarlos.

Al convertirse en un espacio de sumo interés y necesidades para mantenerse comunicado, realizando negocios o activar de manera dinámica el comercio, ha nacido la necesidad de mantener una mayor protección y control por parte de los diferentes actores, esto ha llevado poco a poco a que los Estados o actores privados militaricen este sitio.

A raíz, de tantas problemáticas y acciones negativas que han comenzado a existir, dentro de las situaciones de mayor riesgo que persisten actualmente, se puede mencionar la lucha contra el crimen y el terrorismo en este ámbito, robo de información y bases de datos, chantajes, desviación de fondos, ataques a infraestructuras críticas.

El accionar de los nuevos actores del ciberespacio va en aumento, debido al gran campo de acción y diversidad de actividades que presenta esta reconfiguración de la realidad,

lo que implica un riesgo constante de la seguridad nacional y de las infraestructuras críticas. Gracias a estos dinamismos se crean herramientas complejas de protección.

El ciberespacio al ser un entorno totalmente virtual, las actividades de protección se encuentran encaminadas a ser armas cibernéticas y con altos niveles estratégicos para combatir cualquier tipo de amenaza o amenaza de guerra. Creando grandes ejércitos virtuales para mantener en orden la estabilidad de sus sistemas. Sin embargo, esto ha creado ciertas tensiones entre los diferentes medios y actores que se encuentran relacionándose diariamente, ya que se ha convertido en un territorio nuevo para conquistar y establecer el dominio.

Asimismo, gracias a las relaciones instaladas dentro del ciberespacio, se establecen nuevas políticas o acciones de protección por parte de la comunidad internacional, principalmente, dirigidas a las infraestructuras críticas de las cuales dependen en gran medida la actividad diaria, así como, alianzas estratégicas para establecer conexiones puntuales dentro de los Estados.

Por otro lado, es importante recalcar que diferentes actores del sistema internacional se han actualizado, así como sus modalidades de actuar, esto ha llevado a establecer cibercrímenes, por parte de ciber terroristas, propuestas militares tecnológicas y virtuales por parte de organismos internacionales, de Estados o de empresas. Estos han implementado pautas específicas para disminuir acciones negativas o ataques directos a sus sistemas.

Sin embargo, es importante destacar, que dentro de estas modalidades que se experimentan en la actualidad, aumentan en demasía los riesgos y vulnerabilidades de diversos Estados, principalmente, a raíz del desarrollo tecnológico con el que estos puedan contar. Haciendo la diferencia entre las grandes potencias con gran fortaleza en temas tecnológicos y virtuales, quienes se encuentran con mayor preparación ante diferentes ataques o una posible guerra cibernética.

Esto crea uno de los riesgos más importantes para la agenda global, donde se pueden ver comprometidos cada uno de sus sistemas o en situaciones de mayor riesgo, un efecto en cadena debido a las falencias en distintos sectores. Dando paso a que no todos los países se encuentren capacitados para hacer frente a riesgos específicos o ataques a sus infraestructuras.

Cada uno de los actores pueden incurrir en ataques sin la necesidad de llevarlos a un campo físico como históricamente se ha experimentado, creando bloques o esferas de guerra y militarización, trayendo consigo una visión fresca en la manera de analizar el sistema internacional pero también de plantear nuevas estrategias que puedan mantener la seguridad internacional.

No obstante, al ser una experiencia tan reciente para todo el sistema internacional, se encuentra latente la falta de medidas o regulaciones a nivel internacional sobre cómo hacer frente a diferentes ataques, ya que se vuelven elementos asimétricos. De igual forma, el cómo comprender los desafíos globales y las nuevas dificultades que viven las comunidades.

Aunado a la vulnerabilidad existente en las infraestructuras críticas, ataques masivos y la creación de nuevas armas, ya sea a nivel nuclear o biológico. Se debe entender que es un nuevo espacio de acción, de interacción y de peligros, donde los sistemas se encuentran en constante adaptación a las necesidades del medio y a rendir cuentas a la protección de la integridad de las personas y de cada una de las empresas u organismos.

Gracias a esto es importante destacar el ¿cómo la militarización del ciberespacio y su impacto en los conflictos internacionales proporcionan estrategias, riesgos y desafíos para la seguridad global?

Objetivos de la Investigación

Objetivo general

Examinar el avance de la militarización del ciberespacio y el impacto en los conflictos internacionales con base en las estrategias, desafíos y riesgos a la seguridad global.

Objetivos específicos

•Analizar la evolución de la militarización del ciberespacio y su relación con los conflictos internacionales.

•Evaluar el papel de los organismos internacionales en la regulación de la guerra cibernética.

•Proponer estrategias para fortalecer la seguridad global frente a la militarización del ciberespacio.

Justificación

La digitalización ha convertido al ciberespacio en un campo nuevo de acción y de batalla por parte de los diferentes actores que se encuentran rondando en el sistema internacional y que se viene introduciendo a este nuevo espacio. Tanto como lo son los Estados, los actores públicos o privados, que han comenzado a crear y desarrollar nuevas estrategias para protegerse, pero que incrementan las tensiones de una posible guerra cibernética.

En la actualidad se ha visto y experimentado un aumento considerable de los ataques cibernéticos a diferentes áreas de actividad diaria. Desde entidades financieras y bancos, hasta hospitales o empresas importantes en temas de tecnologías o armas, las popularmente llamadas infraestructuras críticas, haciendo referencia a redes de sistemas eléctricos, toda el área de comunicaciones, cada una de las anteriormente mencionadas, ponen en peligro la estabilidad del sistema internacional y, por ende, la seguridad global.

Cada uno de estos elementos nacen con dichas particularidades a raíz de la gran dependencia que se ha generado de las tecnologías, pero también de la interconectividad que se experimenta a nivel mundial. Este proceso que se percibe todos los días, involucra procesos que se modernizaron y tienen sus bases en la digitalización.

Debido a esto, se expone gravemente y se vuelve aún más vulnerable la información que se encuentra en las redes, tanto de las empresas como de las personas, datos financieros, legales o políticos.

A pesar de que se han creado estrategias de ciberseguridad por parte de los Estados a nivel independiente, la falta de un marco regulatorio sobre ciberseguridad a nivel internacional, dificulta suministrar alternativas para Estados que cuentan con mayores vulnerabilidades y sin la capacidad económica o tecnológica de poder hacerle frente.

Es necesario fomentar una visión internacional sobre la generación de acuerdos e identificar las necesidades de cada individuo, así como, a nivel global, con el objetivo del mantener procesos claves para la solución de problemáticas.

Esto es fundamental para poder prevenir desde el primer movimiento diferentes ataques cibernéticos, identificando las clases de ataques o los dispositivos que se llegaran a usar, evitando difundir el pánico en la población, asimismo, establecer mecanismos para procurar una mayor información para y por la sociedad. Debido a, que una sociedad informada previene y disminuye en gran medida los niveles relacionados a estos ataques, comprendiendo y ejecutando medidas personales de protección.

Con relación a lo anterior, los países con mayor desarrollo en materia de tecnología han podido establecer y crear actitudes defensivas más fructíferas, esto ha incrementado las tensiones entre los actores, por la capacidad que puedan tener con relación al resto de los miembros de la comunidad internacional, cuanto poder pueden llegar a establecer y la influencia para manejar distintos sistemas, dando como resultado que se genere una nueva carrera armamentista en el área tecnológica y cibernética.

Esto viene a fomentar nuevos retos y desafíos a los que la comunidad tiene que hacerle frente, por medio de estrategias y acuerdos internacionales. Con el objetivo de disminuir tensiones y el riesgo de mayores ataques cibernéticos y en el peor de los casos, una guerra cibernética. Haciendo frente de la misma manera, a evitar que actores con intenciones de monetizar por medio de actividades ilegales puedan tomar gran control o autoridad.

Con relación a lo mencionado con anterioridad, es importante analizar el papel de la cooperación internacional en este ámbito, la creación de herramientas para disminuir los peligros y formular acuerdos fundamentales, promoviendo una visión global de unión y enseñanza sobre el ciberespacio y la ciberseguridad.

Finalmente, un punto de análisis esencial es evaluar y comprender como el proceso de militarización continua, puede afectar a la sociedad, las empresas y los gobiernos. Así como, el impacto de este proceso puede generar en la toma de decisiones de los gobiernos y el manejo de la información privada aunado al proceso de soberanía digital actual.

Esto viene a cambiar las agendas nacionales de cada gobierno, así como la búsqueda de la reestructuración de la agenda internacional, relacionado a un avance continuo de la digitalización. Promoviendo en cada caso la búsqueda de medidas para coexistir en un ambiente pacífico, reglamentado y con igualdad de accesos a las necesidades del medio tecnológico, formando una estabilidad por medio del actuar de los organismos internacionales, quienes conforman una parte esencial de la reglamentación internacionales y de las buenas relaciones entre los gobiernos del mundo.

Estado de la Cuestión

El constante aumento en la militarización del ciberespacio, la conciencia sobre la digitalización y la gran cantidad de oportunidades que ofrece este reciente campo de acción, ha impulsado la creación de escritos e investigaciones. Esto con el objetivo de comprender los nuevos fenómenos del marco internacional, así como, las capacidades que se pueden obtener de este.

Debido a esto, se presenta una recopilación de diversas investigaciones relacionadas al tema, guiando a crear una perspectiva más amplia de lo que se ha estudiado, comprendiendo las dimensiones que se han brindado al tema.

Calderón, (2025) en el artículo científico titulado El ciberespacio como escenario de conflicto en el siglo XXI ¿Hacia una militarización de la ciberseguridad? Expone que la conectividad existente a nivel actual conlleva aspectos positivos y negativos, una mayor comunicación entre las comunidades se puede tomar como un avance positivo, sin embargo, estos colectivos se convierten en una parte del problema, ya que pueden ser atacados con mayor frecuencia al ser más vulnerables. Asimismo, queda claro que, gracias a estos elementos, aumentan la constancia de ciberataques, siendo un vasto espacio de actividades, motivados por diferentes acciones.

Aunado a lo anterior, dentro de ciertos marcos regulatorios a los Estados se encuentra el involucramiento de las fuerzas armadas, guiadas a la protección de la tecnología, de las infraestructuras críticas. No obstante, el autor indica la necesidad de una mayor preparación

para las fuerzas armadas en temas de ciberseguridad y la protección de datos de sectores públicos y privados.

Dentro de la investigación, Calderón (2025) concluye que la comunidad internacional se encuentra cada día más inmersa en el ciberespacio, sin embargo, no cuentan con las herramientas necesarias y adecuadas para una militarización completa de este medio, asimismo, cada Estado necesita mayor preparación con relación a dichos temas, para ejercer una mayor protección del as infraestructuras críticas, de igual forma, se ve necesario fortalecer y ampliar los tratados internacionales con relación a estos temas.

Por otro lado, Edwin Matú (2012) en su tesis de graduación basada en la militarización del ciberespacio por parte de los Estados Unidos, propone una visión desde el neorrealismo y la seguridad internacional, logrando comprender el actuar de Estados Unidos en la actualidad, con relación a su poderío, sus capacidades de superpotencia y su creciente innovación. Aunado a esto, se expone la militarización del ciberespacio como una nueva rama de la política internacional.

Asimismo, Matú (2012) expone lo siguiente relacionado al ciberespacio.

> El cual se ha convertido en una zona estratégica y competitiva, en donde se ha generado una serie de acontecimientos que han impactado de forma significativa en el mundo real y tangible, tal es así el alcance, que existe una exportación de conceptos hacia este nuevo campo de investigación, tal es el caso de elementos como armas cibernéticas, ciberguerras, ciber-terrorismo, hactivismo, ciber-comando, ciber-ejércitos, ciber-delitos, ciberseguridad, y todo un nuevo argot que busca dar nombre y explicar de forma precisa que ahí ocurre. (p. 18)

Con lo mencionado anteriormente, el autor da a entender que la migración de cada concepto da como resultado el nacimiento de estas actividades en el ciberespacio, por ende, el involucramiento de las potencias tecnológicas, llevando a cabo, la introducción de sus ejércitos, para mantener el control en este ámbito. Esto ha provocado mayor posicionamiento de dichas fuerzas, así como tensiones crecientes entre los Estados, lo que puede desembocar en conflictos directos.

El presente proceso indica la necesidad de que los Estados deban responder a las vulnerabilidades existentes, a pesar de verse como un lugar a dominar. Sin embargo, la incapacidad general de poder regular de manera adecuada el ciberespacio, indica un aumento de ataques. Dicho autor llega a la siguiente conclusión, el internet es el elemento clave actual para un mayor desarrollo económico y político, igualmente, el ciberespacio está transformando la configuración de la comunidad internacional, esto dio paso a que Estados Unidos se convirtiera en una potencia tecnológica, siendo un caso exitoso en proteger la seguridad nacional, que paulatinamente, se posiciona como un ejemplo a nivel internacional.

Por otro lado, una investigación realizada por el Centro Superior de Estudios de la Defensa Nacional del año 2012, marcan un panorama guiado a la ciberseguridad, su influencia en el ciberespacio y las evaluaciones a nuevos conflictos.

Al recapitular el documento, la investigación expone que el conflicto es parte de la naturaleza del ser humano, al conocer una variante nueva, en este caso virtual, surge la necesidad de utilizarla en su beneficio. Provoca que los conflictos evolucionen de manera paulatina, se explica que los Estados tienen diversos medios relacionados a la seguridad nacional, como medios diplomáticos o políticos, sin embargo, estos deben fortalecerse y actualizarse de acuerdo con las necesidades del medio.

Asimismo, se aclara que el ciberespacio va más allá de la conexión a internet, se compone de hardware, software, una comunidad global con sus propias directrices. Plantea de esta forma un reto para la ciberseguridad, principalmente, para la aplicación de nuevas medidas que controlen al ciberespacio y sus usuarios, ya que en él no se encuentran fronteras.

A partir de aquí implementan el término ciberseguridad, haciendo referencia a la evolución de los conflictos tradicionales en este nuevo marco, implicando aspectos políticos, económicos, sociales, esto lleva a plantear nuevas estrategias para dar solución a las inseguridades que afrontan los Estados y la comunidad internacional. Establecen la necesidad de identificar las amenazas principales, los riesgos que pueden sufrir los colectivos, además, enfocarse en el fortalecimiento de las agencias de seguridad, a la vez de involucrar a las estrategias nacionales de diferentes Estados, con el objetivo de concretar una solución a nivel internacional.

De la misma manera, crean un marco de importancia, guiado a observar un escenario crítico en la actualidad, con un campo de batalla que se extiende diariamente, con relación a esto, ven necesario establecer estrategias nacionales y planteamientos nuevos para prevenir ataques o diferentes peligros, precisando las infraestructuras críticas y la protección de información, por lo tanto, generar mayor conciencia sobre el uso de la ciberseguridad y la responsabilidad de cada miembro activo en el ciberespacio.

Continuando con esta línea exhaustiva de documentos, teniendo claro lo investigado sobre el ciberespacio, también hay que conocer qué se ha estudiado sobre las implicaciones o riesgos existentes en el ciberespacio.

Eissa et al (2012), exponen el tema del ciberespacio y sus implicaciones en la defensa nacional. Aproximaciones al caso argentino. Los autores dentro de su argumento central exponen al ciberespacio como un fenómeno apto para el involucramiento de los Estados y diferentes actores para el desarrollo de ciberguerras o guerras de información.

El peligro naciente viene a raíz de que dichos ataques se realizan mediante distintas computadoras a lo largo del planeta, los distintos sistemas de flujos de datos pueden interconectarse en el ciberespacio. Eissa et al (2012), exponen lo siguiente con relación a los ataques que pueden realizar.

> La forma más habitual o recurrente de operación cibernética es la denominada "ataque de denegación de servicio" (Denegation of service, DOS), que consiste en sobrecargar los recursos informáticos o computacionales del sistema de la víctima a partir del aumento del tráfico de información. (p.8)

Los DOS se encuentran entre los ataques más comunes, no obstante, no son los únicos tipos de ataques que existen dentro del ciberespacio, comúnmente los actores encuentran debilidades dentro de los sistemas de los Estados, esto lleva a crear nuevos tipos de ataques, gusanos informáticos, malwares o phishing. Esta variedad aumenta el peligro para cada organización o Estado.

Con lo mencionado anteriormente, el peligro en el ciberespacio aumenta, no solamente por los actores que evolucionaron a este espacio, si no los ataques entre Estados, aumentando el historial de tensiones que estos compartían. Con relación a esto, concluyen

que la comparación entre el plano físico y ciberespacial no cuenta con un punto de unión debido a la falta de fronteras geográficas. Gracias a esto, debe haber un cambio en la visión de análisis hacia el ciberespacio, con el objetivo de disminuir tensiones, crear una dirección clara a nivel internacional para regular de la mejor manera las actividades que se llevan a cabo.

Seguidamente, en la investigación creada por el Comité Internacional de la Cruz Roja (2019), a partir de ahora CICR plantea una visión más humanitaria y su relación directa con el ciberespacio, ampliando la perspectiva no solamente a un factor tecnológico, si no, implementando las necesidades sociales, asimismo, habla directamente de los ataques relacionados a la sociedad civil, los servicios públicos actuales se encuentran en su mayoría ya digitalizados, lo que da como resultado que la información de las personas se encuentren en la red. Gracias a esto, las infraestructuras críticas son cada vez más atractivas, por este motivo distintos organismos han comenzado a implementar medidas puntuales para poder hacer frente a las constantes preocupaciones.

Las ciber-operaciones deben fortalecer sus bases de datos y sus procesos de detección y protección de datos, asimismo, avanzando al resto de infraestructuras críticas, se evita tener pérdidas humanas en caso de ataques a servicios de salud, pérdidas económicas o robo de identidad, relacionadas a ataques a entes económicos y financieros. Se tiene claro el impacto de los ataques cibernéticos, ya que en la actualidad no solo abarca el impacto físico, si no la pérdida de elementos importantes para el desarrollo de empresas o de los gobiernos.

El presente autor aclarara la importancia de la sociedad civil, ampliar el conocimiento de los métodos de guerra utilizados, aumentar los diálogos entre los Estados y el establecimiento de guías para la preparación del proceso de militarización y la protección de la sociedad civil, indicándolo como un de los sectores del ciberespacio más importantes.

Siguiendo la misma línea de los ciberataques, es importante hablar sobre las ciberarmas, para crear un contexto más acertado a los peligros que pueden llegar a desarrollarse. El autor Arreola (2016), expone ampliamente sobre el armamento digital que se encuentra disponible, las ciberarmas y la capacidad de destrucción. Iniciando con el armamento digital indica que, gracias a los cambios en las estrategias, se han creado desde cero armamentos tecnológicos adaptados a las necesidades que se observan en el

ciberespacio. Con relación a lo mencionado con anterioridad, explica que una ciberarma nace como un elemento con poder destructivo y con la capacidad de poder adaptarse. Principalmente, lo indica como la forma de poder generar daño a las estructuras.

Seguidamente, son utilizadas para causar daño directo, material y físico, si se llegan a comprometer diferentes infraestructuras, pueblos, ciudades u organizaciones. Con la capacidad de paralizar los sistemas, abre las puertas hacia otra gran cantidad de oportunidades al dejar fuera de acción las defensas de los actores mencionados con anterioridad. Entre ellas menciona los virus, los malware o incluso los troyanos, donde cada uno tiene una función diferente y un método de actuar distinto para atacar diversos medios de las estructuras digitales.

De igual manera, el autor aclara la capacidad de estas ciberarmas y el aumento de ataques internacionales que se concretan como un punto de partida para protegerse de cada amenaza que existe alrededor. Cada una representa la oportunidad de analizar los sistemas y fortalecer las infraestructuras de salud y financieras principalmente, por ende, proteger de vulnerabilidades a la población.

Bajo esta misma guía, el autor da cierre al artículo donde se destaca la accesibilidad a estas armas en comparación a las que se usan en los escenarios físicos, las armas cibernéticas se caracterizan por poder obtenerse de una manera menos compleja, incrementando la posibilidad de nuevos ataques, son armas multidisciplinarias, esto ocasiona causar daños económicos y psicológicos a la sociedad, ocasionando miedo al desestabilizar al gobierno de cara a la población, la introducción del miedo termina siendo clave para generar golpes más certeros. Dando como resultado, que exponga la necesidad de reconsiderar las necesidades y el actuar de la seguridad nacional, su reacción a los riesgos y a los ataques, aclarando la necesidad de mejorar la capacidad de respuesta y la protección a las personas y gobiernos.

Finalmente, con relación a las investigaciones estudiadas en el presente apartado, se puede observar que la connotación del ciberespacio, a pesar de no ser relativamente nueva, si cuenta con gran desconocimiento por parte de los Estados y diferentes organismos e instituciones, de igual forma, se observa un gran aumento de armas adaptadas al

comportamiento del ciberespacio y amplios peligros para el desarrollo de enfrentamientos o ataques cibernéticos hacia la sociedad o los gobiernos.

Marco Teórico

Dentro de la presente investigación, se debe establecer un marco teórico esencial, para brindar aportes específicos por parte de diversas teorías dando así respaldo a los elementos claves que se lleguen a investigar, así como conceptos esenciales para brindar profundidad al tema estudiado. Asimismo, por la naturaleza de la investigación, se establecieron tres teorías.

Se inicia por el realismo, para brindar una visión más puntual de la actualidad, enfocado principalmente en temas de seguridad nacional y la conflictividad. Por otro lado, el constructivismo se enfoca en la construcción social del ciberespacio y la percepción que existe sobre él, por otro lado, cerrando con el liberalismo, basándose en el desarrollo de la cooperación entre organismos internacionales o instituciones.

La teoría realista es una de las más antiguas de Relaciones Internacionales, desarrollada por diferentes autores que tratan de explicar el actuar del sistema internacional. Dentro de su visión general expone un sistema internacional anárquico sin una autoridad clara. Lo que se puede extrapolar a la actualidad con el ciberespacio.

De acuerdo a Morgenthau, uno de los impulsores de dicha teoría, expone las características de un estatocentrismo, la conflictividad y la centralidad del poder. Menciona lo siguiente; “El Estado es el único actor digno de consideración en un medio, como el sistema internacional, de carácter político (es decir, basado en el poder).” (Barbé, 1987).

Desde dicha visión, en la actualidad se puede observar al ciberespacio como este medio de carácter político, que se encuentra regido únicamente por temas de poder, donde los Estados buscan ser el ente único, con mayor control, mayor posicionamiento y lograr ampliar su proceso de militarización dentro del ciberespacio. Cada uno de estos elementos con el objetivo de crear una guía para el resto de Estados y así, demostrar a la comunidad internacional su capacidad y fortaleza.

De igual forma, la configuración actual del sistema internacional se eleva al ciberespacio, debido a esto, se mantiene el equilibrio del poder, las tensiones y luchas por el

mismo y el esfuerzo constante por la conquista, aún más intensificadas al conocer un nuevo espacio. Gracias a estas acciones se ven involucrados diferentes actores como lo es la sociedad, organismos o entidades internacionales y los peligros o afectaciones que esta puede tener.

Bajo la misma línea, se debe entender que el interés nacional en la política exterior de los Estados sigue presidido por estos, aún en lugares que hay por descubrir. Con relación a esto, se concentran las motivaciones de seguridad y defensa contra amenazas, en este caso, nuevas intimidaciones cibernéticas. De igual importante a este punto anterior, entra la visión de conflictividad establecida por Morgenthau, el conflicto se posiciona como una naturalidad dentro de las Relaciones Internacionales.

No es de extrañar el aumento de tensiones que se viven en el ciberespacio, el desarrollo de ataques cibernéticos a infraestructuras críticas, el riesgo constante de hackeos a elementos de seguridad o información delicada de los Estados o incluso la información de las personas, aquí recae uno de los pensamientos más claros del autor, el hecho de que no pueda existir paz u orden total de manera perpetua.

Con relación a lo mencionado con anterioridad, la necesidad que se observa en la actualidad e históricamente, sobre la imposición de los Estados, es un elemento que clave, donde se demuestra la lucha constante de conquistar nuevos territorios, así como la preparación por parte de los gobiernos para tomar medidas en defensa y conquista. Desde la perspectiva del autor, se observa claramente, la capacidad de que cada uno de estos fenómenos se pueda transformar. En este factor recae la importancia de lograr observar con mayor atención al ciberespacio y lo que este tiene para ofrecer.

Recapitulando los puntos importantes del realismo, se tiene la lucha constante por el poder, los conflictos permanentes en diferentes niveles y el conocimiento sobre un nuevo espacio donde se busca mantener el equilibrio que se encuentra establecido directamente en el sistema internacional. Bajo esta misma línea, al tener en claro la visión realista, es necesario exponer la visión del constructivismo, desde un punto más social.

Según Tah Ayala (2018) el constructivismo expone que el medio va a influir en la manera en la cual los actores se van a comportar dentro del sistema internacional, la

interacción que estos pueden compartir y la transformación del entorno. Dando a entender que la sociedad no es estática, sino que se encuentra en constante cambio, donde evoluciona el sistema y las sociedades al interior de estas.

El constructivismo al tener una base social, logra exponer una nueva perspectiva del análisis del sistema internacional, como dicho autor menciona, estas interacciones entre los elementos sociales, abarca una organización nueva del sistema internacional, esto se ha observado mediante una metamorfosis desde los últimos años.

Asimismo, se ve crecer las distintas necesidades por parte de las sociedades que deben ser cumplidas bajo la responsabilidad de los gobiernos y los Estados. El aumento de la comunicación internacional debido a la globalización, impulsó un proceso creciente de interconexiones en ámbitos sociales, políticos, económicos, logísticos o comerciales, entre muchos más. Esto creo necesidades puntuales que aunado al impacto de la pandemia, impulsó un mayor uso del ciberespacio y, por ende, la demanda de adaptarse para solucionar problemas.

Con relación a lo mencionado con anterioridad, tanto las exigencias como las amenazas que se presentan a día de hoy dentro del ciberespacio, están condicionadas y cimentadas por medio de las interacciones que se ejecutan diariamente. Ya que dentro del constructo social el ciberespacio se ha convertido en el lugar más reciente para ser un dominio de guerra y poder.

Mediante esta teoría se logra explicar cómo los actores que están dentro del sistema internacional de carácter económico, político o militar por medio de nuevas identidades y políticas avanzan a una configuración adaptada a los peligros del medio. La conclusión y relación directa con dicha teoría se observa mediante el proceso de socialización de los últimos años y el nacimiento de la militarización del ciberespacio, con la creación de estrategias y políticas claves para llegar a su dominio, finalmente se puede ver el creciente impacto de la visión social en el mundo.

De igual forma, para finalizar el apartado teórico, se debe mencionar la teoría del liberalismo, enfoque clásico de la disciplina, la misma ha brindado amplitud de análisis y medios para comprender el acontecer internacional.

Abad (2019) realiza una breve explicación del liberalismo, de acuerdo al pensamiento de distintos autores.

> Si ya desde principios del siglo XX se había hablado de su importancia, para los años setenta de dicho siglo, se insiste en la intensificación de dicha dinámica y se profundiza en su estudio de la mano del concepto de "interdependencia compleja" de la también creciente importancia de la globalización, de los actores no territoriales y de la diversificación de la agenda internacional, integrada por un abanico cada vez más amplio de cuestiones entre las que no resulta fácil establecer una jerarquía clara. (p. 2)

Con relación al apartado anterior, es importante destacar diversos puntos mencionados, en primera instancia, las dinámicas del sistema internacional se volvieron más convulsas conforme el avance de los años, el aumento de las tensiones, tratados o procesos estratégicos, mantiene en constante movimiento y cambio el sistema. Dicha situación ha llevado a crear cambios en la agenda internacional, de acuerdo a los intereses que tiene la sociedad y los Estados, así como cada miembro del sistema internacional.

Entre estas situaciones se encuentra los peligros latentes en el desarrollo del ciberespacio, a pesar de existir tensiones, también se ha planteado la idea principal de poder establecer canales de comunicación, interacciones y lo más importante, acuerdos para hallar un ordenamiento y equilibrio del poder claros. De aquí nace los procesos de interdependencia, cada Estado necesita del otro y de los organismos internacionales y cualquier otro actor del sistema para poder llevar a cabo sus planes.

La cooperación internacional en el ámbito moderno toma mayor importancia, al comprender que los Estados, por gran cuota de poder que conserven, dependen de las acciones, medios y en muchas ocasiones recursos de sus contrapartes. Esto impulsa la cooperación internacional, en busca de la creación de tratados internacionales para mediar el ciberespacio.

Es un elemento clave dentro de la realidad actual, se puede observar mediante la creación de organismos especializados en temas del ciberespacio, la búsqueda de tratados

para la protección de datos, la regulación de armas cibernéticas, asimismo, cierto control o pautas a seguir para mantener la paz entre los Estados o la búsqueda al disminuir tensiones.

La caracterización de esta teoría dentro del análisis actual experimenta gran peso, paulatinamente gracias al conocimiento existente se regula los comportamientos de los Estados, aumenta la cooperación en procesos económicos, políticos, sociales, comerciales que se vuelven fundamentales para el quehacer diario. De igual forma, se plantea una hoja de ruta clara para poder intervenir en el nacimiento de los conflictos, donde se entiende que los gobiernos buscan beneficios mutuos.

Por otro lado, un componente importante del marco teórico es el apartado conceptual, para esclarecer conceptos importantes y generar mayor aclaración con relación a los aspectos que se van a abarcar en el documento.

Ciberespacio: el cyberspace (ciberespacio) por William Gibson en su novela Neuromancer (1984), texto en el cual se describe el ciberespacio como un espacio emergente no material en el que se dan interacciones entre sujetos que se conectan a una red de ordenadores para realizar distintas actividades de orden social, incluyendo actividades delictivas. (Santana & Báez, 2022)

Ciberseguridad: La ciberseguridad, también conocida como seguridad digital, es la práctica de proteger su información digital, dispositivos y activos. Esto incluye información personal, cuentas, archivos, fotos e incluso el dinero. (Microsoft, s.f).

Cooperación internacional: La cooperación internacional comprende todas las modalidades concesionales de ayuda y colaboración entre los países, que contribuyen a procesos de desarrollo mediante la transferencia de recursos técnicos y financieros entre diversos actores del sistema internacional. (Ministerio de Relaciones Exteriores Colombia, s.f).

Infraestructuras críticas: En otras palabras, las infraestructuras críticas son todos aquellos sistemas físicos o digitales que facilitan funciones y servicios esenciales para apoyar a los sistemas más básicos a nivel social, económico, medioambiental y político. (LISA institute, s.f).

Organismos internacionales: Los organismos internacionales son asociaciones que se encuentran en todo el mundo con un propósito en particular: ayudar a la población económica, socialmente y en la salud. La primera organización mundial que existió fue "Versalles". Para que una organización sea reconocida mundialmente necesita de la participación del Estado, en primera instancia, y conocer sus recursos disponibles, territorio (fronteras), espacio geográfico y población. (Universidad Intercontinental, 2020).

Los conceptos mencionados anteriormente, brindan un contexto más amplio de los elementos utilizados dentro del documento, ya que se posicionan como un factor importante para ampliar el conocimiento sobre el tema.

Metodología

Enfoque de investigación

Con relación al tema estudiado, este cuenta con un enfoque cualitativo, orientado en comprender la ciberseguridad y la militarización del ciberespacio como los ejes centrales que lo componen.

Según Hernández (2014)

> El enfoque cualitativo también se guía por áreas o temas significativos de investigación. Sin embargo, en lugar de que la claridad sobre las preguntas de investigación e hipótesis preceda a la recolección y el análisis de los datos (como en la mayoría de los estudios cuantitativos), los estudios cualitativos pueden desarrollar preguntas e hipótesis antes, durante o después de la recolección y el análisis de los datos. Con frecuencia, estas actividades sirven, primero, para descubrir cuáles son las preguntas de investigación más importantes; y después, para perfeccionarlas y responderlas. (p.7)

Debido al texto mencionado con anterioridad, es importante introducir el enfoque cualitativo para aclarar las incógnitas nacidas con relación al tema, al ser la ciberseguridad un tema relativamente reciente, planteando estudios en áreas significativas, de igual forma, es sustancial recalcar que la investigación es de tipo documental, ya que es importante recabar

información de los medios posibles, documentos estratégicos, para que el análisis bibliográfico se sustente en dichas bases y lograr entender las doctrinas militares y así ahondar en el ciberespacio, por otro lado, ampliar el escenario de poder y conflicto que se viene configurando en la actualidad, por medio de las narrativas de los gobiernos u organismos que se encuentran en constante relación.

Asimismo, la investigación tiene sus bases en tipo explicativas, con el motivo de poder exponer y desarrollar este fenómeno, su crecimiento en la actualidad, el proceso de militarización, así como, la introducción de diversos actores, las acciones y actividades que llevan a cabo. Igualmente, se explora las actividades e influencia por parte de los organismos internacionales.

Hernández (2014) expone sobre el tipo explicativo.

> Los estudios explicativos van más allá de la descripción de conceptos o fenómenos o del establecimiento de relaciones entre conceptos; es decir, están dirigidos a responder por las causas de los eventos y fenómenos físicos o sociales. Como su nombre lo indica, su interés se centra en explicar por qué ocurre un fenómeno y en qué condiciones se manifiesta o por qué se relacionan dos o más variables. (p.95)

Al ser de características explicativas, se guía a poder entender de manera correcta y más a profundidad cada una de las acciones y el impacto que estas pueden tener dentro del Sistema Internacional, así como el crecimiento de tensiones por la búsqueda de poder y cómo este puede afectar a cada Estado o miembros del sector social, incluyendo factores políticos, económicos o comerciales. Importante también destacar el proceso de seguridad internacional que se ha podido construir, los alcances, las limitaciones y debilidades de los actores involucrados y el Sistema en general.

De igual forma, relacionar las variables para lograr que se pueda analizar el conjunto de acciones desarrolladas, el crecimiento del ciberespacio y la transformación y aumento de poder con relación al dominio militar de los actores.

Fuentes de Información

Por otro lado, con relación al tema del muestreo, será realizado por medio de conveniencia, con relación a los textos a los cuales se tenga acceso con relación a organismos internacionales, instituciones universitarias, entre otras, asimismo, los tipos de fuentes se encuentran relacionas a la información que será extraída por medio de diversos documentos como libros, artículos científicos y académicos, diferentes estudios de caso o textos de importancia por parte de organismos internacionales o entidades que brinden un respaldo seguro y confiable para el análisis. De igual forma, la muestra va a estar guiada por elementos de importancia para la investigación, regidos por los puntos centrales de cada uno de los objetivos.

Finalmente, para la recolección de datos se ubica en el análisis de los datos, por medio de fuentes bibliográficas, siendo uno de los instrumentos principales. El proceso de recolección de datos se va a encontrar guiado por medio de la revisión y estudio de documentos y bibliografía especializada en el tema. Cuando se analice la información se va a encontrar condicionada bajo criterios como el ciberespacio, militarización, seguridad e impacto social. Puntos clave y centrales para comprender la investigación.

De igual forma, con relación a los medios de exclusión e inclusión los principales documentos como artículos científicos o revistas científicas, académicas, tesis se encuentran delimitados a una temporalidad de 5 años, del periodo 2020-2025 a nivel latinoamericanas y europeas, con relación a ciencias sociales.

Por otro lado, la unidad de análisis va dirigida al estudio de elementos claves para aclarar el proceso investigativo.

- Organismos internacionales como la Organización de Naciones Unidas, Foro de Gobernanza de Internet.
- Estados como; Estados Unidos, República Popular de China.
- Personajes: terroristas, hackers.

Diseño de investigación

Por otro lado, el diseño de la investigación cualitativa se plantea como hermenéutica, en el sentido de poder investigar a mayor profundidad las operaciones que ha cometido los

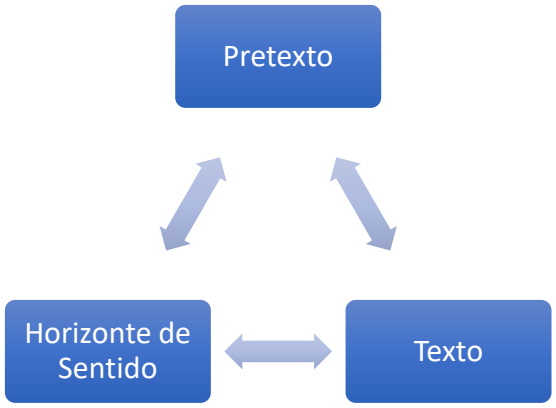
Estados y el impacto en la sociedad civil por medio de los ciberataques. (Quintana, 2019). habla un poco sobre el diseño de hermenéutica.

> La hermenéutica provee una alternativa propia para la interpretación de los textos. La hermenéutica es, en sentido general, el estudio de la comprensión y de la interpretación, y en sentido particular, la tarea de la interpretación de textos (Palmer, 1969).

En este sentido se escoge el diseño para profundizar en temas del ciberespacio y su militarización, ya que es un hecho latente, pero reciente y que no se encuentra investigado a grandes magnitudes, debido a esto, es necesario interpretar y comprender los textos existentes, para obtener la información puntual en el desarrollo de la investigación. Dando respuesta principalmente a las problemáticas, entre ellas, a la inseguridad en temas de ciberataques y protección de información, así como protección para las infraestructuras críticas, tres elementos esenciales en el proceso de militarización y poder.

Dentro de las fases del proceso es necesario exponer que se van a interpretar textos bibliográficos como revistas, artículos científicos o académicos, para poder dar respuesta a la pregunta de investigación que indica cuál es el proceso de militarización del ciberespacio y su impacto en la seguridad internacional. Se comprende el factor histórico, social y tecnológico que rodea este nuevo proceso, igualmente, se delimita el estudio del periodo 2020 al 2025, haciendo un enfoque en la influencia a raíz de Estados Unidos y la República Popular de China.

Asimismo, este método cuenta con pasos a seguir puntuales como lo son los siguientes:



Fuente: Información extraída de (Londoño et al, 2016).

Para el caso de la presente investigación el elemento central es el ciberespacio, su desarrollo y evolución, aunado a su relación directa con el proceso de militarización y cómo este puede afectarlo directamente junto con la seguridad internacional.

El texto corresponde al impacto que se recibe dentro del ciberespacio y hacia la comunidad internacional por el gran proceso de militarización a raíz de los ataques cibernéticos, inseguridad y lucha por el poder y control.

El horizonte del sentido viene de la mano con el uso y lectura de diferentes medios bibliográficos que puedan dar respuesta a la pregunta de investigación, asimismo, que brinden la pauta para establecer un escenario de análisis interpretativo a través de distintos textos estudiados.

Desarrollo

Con el motivo de poder dar respuesta al problema de investigación y comprender más a fondo el desarrollo del ciberespacio, el crecimiento de la militarización y la mejora en la seguridad internacional, se busca desarrollar cada uno de los objetivos planteados. Iniciando por la evolución del ciberespacio y su proceso de militarización con relación a los conflictos internacionales.

Analizar la evolución de la militarización del ciberespacio y su relación con los conflictos internacionales.

Desde el nacimiento del internet en la época de los sesenta, la interconexión a nivel mundial se vio más avanzada, el poder comunicarse desde diferentes puntos de un país o entre países, facilitó cada vez más las relaciones entre los Estados o diferentes instituciones, de igual forma, se logra ampliar el comercio, las relaciones sociales, políticas o económicas.

El internet alcanzó un nuevo nivel de crecimiento y desarrollo, en la década de los noventa se implementaron nuevos elementos como las páginas web, los buscadores, entre otros elementos, aquí se puede observar como el factor tecnológico se encuentra en constante innovación.

Cada uno de estos avances condujo a la creación del ciberespacio. A lo largo de los años este ha tenido diferentes concepciones y realidades de acuerdo a las necesidades de las distintas poblaciones. Santana & Baez (2022), mencionan lo siguiente con relación al ciberespacio.

> El ciberespacio como concepto nace en la literatura, con la novela Neuromancer de Gibson (1984), y es acogido por la informática, dado el parecido de la obra con lo que sucede en el mundo actual y las redes de ordenadores de distintos tipos sustentadas en la internet. (párr. 1)

Esta es la primera vez que se escucha y conoce el concepto de ciberespacio, donde comienza a experimentar esta visión, de un campo de comunicación global sin control de ningún gobierno, elemento que llama la atención a los distintos actores del sistema internacional. Como se puede observar, la base del ciberespacio recae en la interconexión de computadoras y el uso directo del internet, esto ha llevado a que se cree un amplio uso de la digitalización. Han nacido intereses de por medio, nuevas necesidades y un proceso puntual del uso de seguridad a nivel internacional.

El ciberespacio tomó mayor posicionamiento y poder durante la época de los noventa y continuó reforzándose a lo largo de los últimos años. Esto ha moldeado la acción de los actores de este nuevo espacio, creando tensiones e inseguridad, dando como resultado que se comience a dar un proceso de militarización, para disminuir las tensiones y asegurar el poder dentro de este medio no tangible. Sin embargo, a raíz de estas tensiones dadas nacen diferentes enfrentamientos y por ende un nuevo concepto por conocer, el de ciberguerra o guerra cibernética. Guamba et al (2025) mencionan lo siguiente.

> Los ciberconflictos han estado presentes desde la década de 1960, con los primeros actos de vandalismo informático. En los años 80, con la creación de redes informáticas privadas, estos conflictos evolucionaron exponencialmente, desde acciones cibercriminales menores hasta los conflictos cibernéticos. (p. 141)

Cuando se habla de ciberguerra o ciberconflictos, es necesario ampliar el termino y comprender que no es solo el enfrentamiento entre Estados, como tradicionalmente se

conoce. Al ciberespacio ser tan profundo y ofrecer tantas posibilidades, los actores han evolucionado sus acciones y medios hacia este nuevo lugar.

En este caso, en la actualidad se encuentran con operaciones cibernéticas, los Estados, los organismos internacionales, actores independientes como grupos de hackers o actuando de manera autónoma, ciberterroristas, así como distintas instituciones. En este caso, se puede observar el constante movimiento de información o actividades digitales y cibernéticas que pueden ser tanto positivas como negativas.

En los sesenta se comienzan a proporcionar un control en las redes para quienes tenían acceso y así proteger la información que se manejaba, de igual forma, se separaban las actividades que se llevaban a cabo. Posteriormente, en los setenta se crea el primer tipo de programa de carácter libre dentro de la red, que se podía colar bajo la información de ciertos medios, a raíz de esta actividad, el desarrollador Ray Tomlinson crea el primer antivirus para protegerse de estos programas, que podían interceptar la información.

> Un ejemplo histórico relevante en este contexto sería el ataque virtual de 1982, que consistió en la producción masiva de citas ficticias en un sistema de información informatizado (Drouilly del Río, 2022; Gil, 2023 citado por Guamba et al, 2025, p.142)

Como se puede observar los mismos tipos de ataques incluso han ido en evolución, desde ser ataques sencillos sin afectar directamente a infraestructuras críticas o información personal de las empresas o individuos a llegar a comprometer estos elementos anteriormente mencionados. Eventualmente, se convierten en procesos más preparados, estratégicos y dañinos para obtener los beneficios deseados.

Esto llevó a que los Estados comenzaran un proceso de militarización dentro del ciberespacio para proteger sus sistemas y la información delicada, así como, sus infraestructuras, debido a esto, se presentan la evolución de las capacidades ofensivas para comprender más a fondo el proceso de militarización. Naturalmente, por la inmensidad del ciberespacio, se cumple la visión de un espacio anárquico, donde no hay capacidad para presentar funciones a cada Estado o guiar las acciones de cada uno de los actores presentes.

Al inicio del desarrollo del ciberespacio, los Estados y los pocos actores independientes que se encontraban en el medio, no habían desarrollado las capacidades necesarias para hacer frente a como las amenazas se iban desarrollando. Apenas se posicionaban como un actor para promover la comunicación, interconexión, paulatinamente, comenzaron a realizar procesos de militarización al observar las amenazas.

Al conocer el potencial que se podía encontrar dentro del ciberespacio, se dio la búsqueda por tratar de generar un control o ciertos reglamentos para asegurar una estabilidad dentro del presente sitio. Asimismo, donde se demuestre las posibilidades, alcances y limites que pueden tener los actores involucrados.

Con relación a cada uno de estos elementos, se dio un aumento de inseguridad, ataques y crímenes por medio del ciberespacio, que afectan a la sociedad civil, los gobiernos y distintas entidades que puedan conectarse por medio del ciberespacio.

Las características de los ciberataques van relacionadas a amenazas con márgenes de acción más grandes e inmediatos, donde se dificulta detectar con agilidad y rapidez de donde provienen los ataques, estos pueden generar mayor caos a nivel interno con relación a los sistemas de comunicación e información, dependiendo del tipo de ataque resultan ser menos costosos y utilizar menor cantidad de insumos, de igual manera, generan gran impacto.

Cabe destacar que sus medios están dirigidos a generar extorsión a los usuarios por medio del robo de identidad, el robo de información personal o en infraestructuras críticas como bancos y hospitales, se procede a hackear los sistemas y restringir el acceso. El motivo de estas acciones se encuentra guiado a pedir una suma de dinero sumamente alta para devolver la información de los usuarios en caso contrario se elimina toda la información de la empresa.

Han existido distintos casos, principalmente, a inicios de los dos mil que provocaron inseguridad y nuevas medidas de seguridad para los Estados, estos se mencionan como precedente del nuevo accionar de los gobiernos a nivel mundial.

El primer caso a mencionar es el de Estonia en el año 2007, se expone que desde el Estado ruso se produjo el ataque, donde se demostraba el poderío que tenía Rusia en este sector y como países vulnerables se podían ver afectados por la baja capacidad de seguridad

en temas tecnológicos. Los ataques se basaron en la utilización de robots informáticos que paralizaron los servicios públicos como los bancos, lo que provocó pánico en la población, al no poder acceder a su dinero o realizar trámites, como el pago de cuentas, transacciones nacionales o internacionales.

Este evento representó un antes y un después para la seguridad cibernética de Estonia como del resto del mundo, al poder observar como un movimiento en las redes interconectadas podría afectar el desarrollo y el diario vivir de todo un país.

Por este medio, los ataques comenzaron a evolucionar a pasos agigantados. El siguiente caso de ejemplo se hace mención a la primera arma encontrada dentro del ciberespacio Stuxnet, que llegó a causar un caos altamente grande aunado de pánico y sorpresa al conocer lo que se podía llegar a generar.

> El año 2010 el mundo conoció la existencia de un programa informático malicioso que por primera vez fue mucho más allá de denegar servicios, robar información u obtener dinero, provocando daños materiales en instalaciones físicas, equivalente a un bombardeo de precisión, es decir, se conoció la primera ciberarma. (Rivadeneira, 2016).

Los protagonistas de este ataque son Irán y sus reservas de uranio. Durante meses las reservas de uranio se encontraban afectadas y la empresa no encontraba la razón de dicho fallo. Las centrífugas se encontraban en constante fallo, la maquinaria fallaba constantemente y se realizaban cambios, sin embargo, la situación se repetía.

Luego de diversas investigaciones se llegó a la conclusión de ser afectados por un gusano informático dentro de sus sistemas, se controló los softwares de las maquinas haciendo que estas fallaran, pero también se perdiera la producción. El ataque fue dirigido a Irán por el gran poderío nuclear con el que contaba, la idea fue desestabilizar y disminuir la capacidad nuclear.

Aunado a esto, se convierte en el primer ataque cibernético que afectó a infraestructuras críticas y delicadas como lo son las plantas nucleares. Paulatinamente, se transforma en un punto de inflexión al dimensionar que el ciberespacio podía extenderse a medios físicos. El peligro se hacía latente y cada uno de los Estados o actores independientes

podían correr peligro por cada posible acción, impulsados por estos peligros los gobiernos comienzan a mejorar y ampliar sus fuerzas dentro del ciberespacio.

A pesar de ser un medio anárquico, como lo establece la teoría realista, los actores involucrados en este nuevo medio buscan construir poder dentro de un espacio sin fronteras. La falta de control a nivel general obliga a que estos participantes se armen y creen elementos de seguridad para protegerse.

Con relación a lo anterior, estas actividades se vuelven realidad cuando aumenta el peligro de ataques y consecuencias a nivel social, económico y comercial principalmente, así como todas las actividades que conlleven al impacto directo de las infraestructuras críticas. La coordinación de los ataques de la mano con la desinformación muestra una guerra no convencional y elemento clave para comenzar a desestabilizar gobiernos desde un ámbito económico, pero también social.

La base de los Estados y su buena organización recae en gran medida de su población, al tener una interconexión infinita y creciente día con día, aumenta el radio de inseguridad y peligro en el ciberespacio.

Esto ha llevado a que países como Estados Unidos o la República Popular de China, actores centrales dentro del sistema internacional que cuentan con las mayores cuotas de poder establezcan un punto y aparte en la organización del ciberespacio. La militarización y la seguridad internacional se volvieron puntos centrales en sus agendas internacionales.

En el caso de Estados Unidos, al ver un escenario armado, diversidad de actores, aumento de peligros y constantes amenazas, plantean la Estrategia Nacional de Ciberseguridad, el país cuenta con un plan estratégico impulsado para el periodo 2024-2026, basado en la experiencia que han tenido y el constante proceso de investigación.

El objetivo principal de la estrategia abarcar la capacidad de abordar las amenazas cibernéticas, disminuyendo y combatiendo las campañas maliciosas relacionadas a que la población logre identificar los diferentes medios por los cuales pueden ser afectados, creando lazos estratégicos con entidades público y privadas. Guiados por medio de la detección o divulgación de las vulnerabilidades, ya sea a nivel del individuo o de las instituciones que conformen parte de la red central de comunicación.

Asimismo, dentro del proceso de militarización se guían a la cooperación entre las organizaciones, así como infraestructuras críticas para poder hacer frente en caso de que se presente alguna amenaza, teniendo claro que como Estado deben mantenerse protegidos en cada aspecto. Asimismo, el impulso de herramientas digitales para detectar ataques y dar una respuesta coordinada.

La coordinación y cooperación dentro del proceso de militarización se ha vuelto clave, para priorizar las amenazas, mejorar las defensas y brindar a apoyo a las instituciones o infraestructuras críticas que no tienen el conocimiento y las herramientas para fortalecer sus sistemas. El gobierno estadounidense se ha convertido en un ejemplo en temas de seguridad y militarización.

Con un proceso de reforma tecnológica e innovación, así como educación fortalecen su ciberespacio. Mayores capacitaciones y conocimientos en ciberseguridad lo vuelven un gobierno con una población informada, con conocimientos básicos para detectar las amenazas más básicas y evitar efectos en cadena que puedan estar en constante crecimiento.

Enfocándose en la defensa colectiva y por ende tener una respuesta de carácter coordinada permite guiarlos bajo los principios militares de ciberseguridad y proteger las infraestructuras críticas. El proceso de militarización en este nuevo espacio incluye inteligencia artificial capacitada para detectar ataques, proteger y bloquear los sistemas cuando sea necesario y mantener una constante monitorización de los sistemas, demostrando a nivel internacional como han robustecido sus sistemas para protegerse pero también para poder dar respuesta en caso de un ataque, con diversidad de personal capacitado en el caso de acceder a sistemas, identificar la procedencia del ataque y la capacidad de involucrarse en una guerra cibernética con las armas digitales y tecnológicas más estructuradas y desarrolladas, desde gusanos informáticos, bonets, virus, entre otros, como métodos de defensa y ataque.

Por otro lado, tras analizar el contexto de la militarización estadounidense, es necesario observar su contraparte, ahondando en el caso chino. Tras tomar un poderío político, militar, territorial y estratégico durante los últimos años, China es un gran modelo de desarrollo tecnológico y digital, por ende, es necesario prestar atención a una de las sobresalientes fuerzas de la comunidad internacional.

China en el año 2016 expuso su Estrategia Nacional de Ciberseguridad, entre las pautas principales impulsan el fortalecimiento de la cooperación internacional dentro del ciberespacio, con el objetivo de reformar el sistema que existe dentro de internet, los niveles de poder o control existentes, de esta forma se promueve un liderazgo por parte de la Organización de Naciones Unidas (ONU), como mecanismo de control, gestión y revisión de las actividades de cada miembro del ciberespacio. Aunado a fortalecer las infraestructuras críticas y desarrollar normativas para proteger la seguridad en estas. (Markovski y Trekyhalin, 2022).

Estas estrategias y políticas impulsadas por la República Popular China se encuentran guiada también a la protección de las infraestructuras críticas, todo el sector de comunicación, salud, finanzas. El país ha logrado mejorar su seguridad por medio de políticas independientes para queda sector, es decir, leyes y reglamentos dedicados a infraestructuras críticas, información personal, seguridad de datos, entre otros, para ampliar la cobertura en cada sector.

> A nivel internacional, el Partido y sus agentes, el Ministerio de Seguridad del Estado (MSS) y el Ministerio de Seguridad Pública (MPS), se han convertido en los principales piratas cibernéticos de tecnología y secretos comerciales.

En este sentido, parte del proceso de militarización se encuentra guiado bajo las fuerzas del gobierno chino, quienes realizan los principales movimientos dentro del ciberespacio, para proteger sus sistemas, pero también tener controlados por medio de información el resto de sistemas internacionales. Asimismo, que dichos agentes recolectan toda la información de la población y cada miembro, con el objetivo de alcanzar mejores beneficios y controles para evitar traiciones.

Aunado a esto, la creación de un Centro Nacional de Ciberseguridad constituido en China, se encarga directamente de realizar una escuela de ciberseguridad para la preparación de sus habitantes y técnicos superiores. Asimismo, a raíz de la preparación de tantos individuos, el país ha impulsado diversas herramientas para proteger su ciberespacio, desde simuladores y pruebas continuas por parte del estrato militar.

Asimismo, el desarrollo de inteligencia artificial brinda a China una gran ventaja para establecer una vigilancia continua de sus sistemas y de las entradas y salidas de información registrada en su sector del ciberespacio. De igual forma, cuentan con equipos de hackers preparados y especializados en conocer y resolver las vulnerabilidades de sus sistemas digitales.

Esto brinda la oportunidad de que China militarice el ciberespacio de manera paulatina para establecer un control directo y ventaja sobre el resto de actores del sistema internacional. Por medio del espionaje o actividades puntuales dirigidas a sus contrapartes. La capacidad en ciberseguridad de China se ha convertido en una de las más grandes, estructuradas y fortalecidas del mundo.

La visión de Estados Unidos como de China representa en la actualidad para la comunidad internacional un aumento de tensiones, pero también una mayor preparación y engrosamiento del ciberespacio. El proceso de militarización compromete la seguridad internacional, con relación a esto, nace la necesidad de establecer mecanismos globales para proteger los datos, pero también mantener la estabilidad en el mundo.

De igual forma, la militarización evoluciona, es decir, las tácticas utilizadas a nivel territorial, las estrategias son las mismas, los gobiernos se adaptan a las necesidades y movimientos del ciberespacio. Aprenden a utilizar los medios que tienen al alcance.

La evolución del ciberespacio ha dado la oportunidad del desarrollo de guerras cibernéticas y la coordinación de ataques relacionados al uso de la desinformación, sabotaje o espionaje. Dirigidos a la desestabilización de los gobiernos, sus herramientas y sus sistemas de primera mano.

Como se mencionó con anterioridad, los primeros pasos del ciberespacio y la guerra cibernética al inicio de los dos mil, más la preparación de las mayores potencias en la actualidad crea una relación directa a los nuevos conflictos internacionales en materia tecnológica. Esto debido a que, se convierten en gobiernos y actores más preparados, con mayores conocimientos y actividades para beneficio propio, también en búsqueda del poder.

Por un lado, el impacto dentro de los conflictos internacionales también se relaciona a nuevas herramientas ofensivas, entre ellas se pueden encontrar los malware, rasonware que

son herramientas guiadas a generar caos, interferir en los sistemas y estructuras militares para obtener información delicada de los gobiernos, información económica, entre otras.

Estas ciberarmas son numerosas, existen de diferentes tipos, fuerza y capacidades que afectan las redes de las empresas e infraestructuras críticas, donde tienen la capacidad de introducirse en la información de los hospitales, detener las máquinas que mantienen a los pacientes, interferir en las máquinas para los exámenes que necesitan realizarse, todo a cambio de dinero o información valiosa. Es uno de los principales impulsos y motivaciones por parte de estos grupos de hackers, que pueden ser contratados por los gobiernos o ser actores de carácter independiente.

Por otro lado, estos mismos ataques ven afectados a los bancos o instituciones financieras, tienen la capacidad de bloquear todas las transacciones de dinero a nivel nacional o internacional de un banco, robar el dinero de las cuentas o bloquear el uso de los cajeros automáticos. Esto provoca un pánico en la población, la paralización del comercio a nivel interno, ya que los negocios no tienen la capacidad de hacer frente a estos ataques o se va perdiendo el uso de dinero en efectivo, dando como resultado que no pueda hacerse el intercambio de bienes o servicios.

Entre las infraestructuras críticas también se encuentran las bases nucleares o militares, estas desencadenan mayor peligro desde el material que las mismas manejan, la cantidad de armas o elementos químicos que pueden manipular, en un ataque pueden afectar a la industria, los trabajadores o incluso más.

Es debido a todos los blancos que existen, que la militarización se ha establecido con mayor fuerza dentro del ciberespacio, con grandes sistemas de seguridad, contratación de expertos en el tema capaces de combatir los ataques, mitigarlos y contraatacar. Gracias a esto, es necesario que se creen proyectos, leyes comunes y programas de cooperación para disminuir las amenazas a nivel mundial, con relación a esto, es necesario conocer el papel que los organismos internacionales están cumpliendo con relación al ciberespacio.

Evaluar el papel de los organismos internacionales en la regulación de la guerra cibernética.

A nivel global, los organismos internacionales cumplen un papel importante para la puesta en práctica de conversaciones, negociaciones y acuerdos en común, para disminuir tensiones, peligros o guerras. En el caso del ciberespacio y las guerras cibernéticas no es la excepción, a pesar de no ser un campo que en la actualidad se encuentre estudiado a profundidad.

Cuando se habla de ciberdefensa y organismos internacionales, uno de los protagonistas por excelencia es la Organización del Tratado de Atlántico Norte (OTAN)

Proponer estrategias para fortalecer la seguridad global frente a la militarización del ciberespacio.

Debido al ataque del año 2010, se le solicitó ayuda a la OTAN como organismo internacional, para brindar ayuda y poder combatir los ataques que se desde meses atrás estaban impactando. La organización se puso a trabajar en un plan para poder establecer regulaciones e ir aclarando el espacio de acción existente, así poder conocer las capacidades que tienen y cómo pueden hacer frente a las problemáticas. Galizia (s.f) hace mención del proceso de la OTAN.

> A raíz de distintas reuniones llevadas a cabo por los Ministros de Defensa de la OTAN realizadas en el marco del Nuevo Concepto de Ciberdefensa de la Alianza, la OTAN ha aprobado en 2011 una Política de Ciberdefensa y un plan de acción para su implementación. El principal objetivo consiste en la protección de las redes informáticas de los Estados Miembros. Uno de los principios fundamentales de este Concepto es el de la cooperación como pilar fundamental para poder integrar las capacidades de otros Estados y organismos internacionales en el planeamiento de la Defensa de la OTAN frente a las ciberamenazas.

La OTAN comienza a establecer pautas generales para controlar el ciberespacio, una medida sustancial se guía a la capacidad de integrar capacidades y conocimientos de todos los Estados miembros para que en conjunto puedan hacer frente a las diversas problemáticas. La característica común y la base de estos procesos se trata de establecer plataformas solidas de cooperación, con el objetivo de tener una respuesta rápida y efectiva.

La regulación por parte de la OTAN ha logrado crear una planificación más coordinada con los gobiernos, implementar medidas de ciberdefensa y preparar las capacidades de cada uno, procurando la ayuda entre Estados y obtener información necesaria en respuesta a ataques. Dentro de los mismos procesos para evaluar y asegurar un mejor manejo del ciberespacio, se han creado organismos con características especiales en ciberdefensa.

En este caso el Centro de Ciberseguridad de la OTAN, cuenta con un control diario sobre las redes de comunicación y actividades del ciberespacio, procurando la creación de alianzas y comunicación en la red. Asimismo, cuentan con la capacidad de ofrecer servicios y protección a los usuarios, donde se atiende todas las emergencias reportadas.

El papel de la OTAN es fundamental para la atención de problemas, por medio de políticas de riesgo y confianza mutua, logran establecer lazos cooperativos con miembros regionales e internacionales. Así como redes de apoyo a nivel regional o internacional, para el fomento de investigación, mejora en los sistemas tecnológicos y digitales.

Como parte del creciente desarrollo en temas de ciberseguridad por parte de la OTAN, se creó el Manual de Tallin, este desarrolla las principales ideas y pasos a seguir en caso de un ataque cibernético a gran escala. Galizia (s.f) menciona lo siguiente.

> En el Manual se indica por primera vez el procedimiento a seguir por parte de los estados y las alianzas militares en caso de ciberataques masivos. En cierta medida, el objetivo de la publicación es apreciar que las actuales normas legales internacionales (sobre todo en derecho internacional humanitario) son aplicables también en el ciberespacio. Para el Manual, los (ciber) ataques desarrollados en ausencia de acciones militares pertenecen a la categoría de las “acciones en contra de la ley” por lo que la reacción a los mismos puede llevar al agresor ante ámbitos penales o tomar “contramedidas proporcionales” (pág. 137)

El manual demuestra ser un avance sustancial para llevar a otro plano el derecho internacional y demostrar que el mismo puede ser aplicable en el sentido del ciberespacio. Asimismo, la capacidad de poder clasificar y entender más a fondo los ataques cibernéticos que pueden realizarse y las armas a utilizar. El mismo no conforma una ley establecida dentro

de la organización, sin embargo, logra un mayor entendimiento de los movimientos que se realizan y como interpretarlos.

Aunado a contener normas que identifican las funciones de los Estados, la responsabilidad de cada individuo dentro del ciberespacio y la cuota de soberanía que estos o los Estados pueden tener. Bajo esta misma línea, existe el Convenio de Budapest sobre la ciberdelincuencia, de acuerdo a lo establecido en el convenio se abarca una política para proteger a la sociedad principalmente, no a los gobiernos y las herramientas necesarias para proteger los datos. Protege los derechos humanos, guiados a temas de privacidad y libertad.

De igual forma, como todos los elementos a nivel internacional, la cooperación se vuelve un factor indispensable, por medio de diferentes procedimientos y comunicación entre los gobiernos que ratifiquen el convenio, dicho documento se encuentra en constante evolución, un aspecto fundamental cuando se relaciona al ciberespacio, aunado a un marco institucional que es más flexible, con relación a las capacidades de cada Estado. Por otro lado, es importante destacar el proceso de ciberseguridad en la Organización de Naciones Unidas (ONU).

Muchas organizaciones y gobiernos componen la ONU, no todos le han brindado el mismo nivel de cuidado a las cuestiones relacionadas a la ciberseguridad. Debido a esto, el nivel de madurez de los sistemas en ciberseguridad varía en gran medida, aunado a la disponibilidad de los recursos, las herramientas y estructuras.

La ONU se guía por medio de acuerdos internacionales, con el objetivo de que los Estados puedan unirse por voluntad propia con relación al interés que vean reflejados. A día de hoy se ha firmado una convención sobre el ciberdelito, con el objetivo de fortalecer la cooperación internacional.

> El acuerdo sobre el tratado jurídicamente vinculante marcó la culminación de un esfuerzo de cinco años por parte de los Estados miembros de las Naciones Unidas, con aportes de la sociedad civil, expertos en seguridad de la información, el mundo académico y el sector privado. (Mishra, 2024, párr. 2)

La declaración se marca como un gran paso para crear conexiones, cooperación y respeto para los derechos humanos. Brinda a los gobiernos las herramientas necesarias para

prever ciberdelitos, proteger los datos de las instituciones y las personas, este se amplía incluso a delitos no solo a infraestructuras críticas, si no a la protección de los menores de edad, se incluye la trata de personas, tráfico de drogas, ataques económicos y comerciales.

Estos esfuerzos visibilizan el interés por parte de los Estados de proteger sus bienes digitales, su información y a la sociedad civil, se demuestra la importancia y el peso que el ciberespacio está tomando en la actualidad, vinculado a las necesidades de seguir con el desarrollo de la cooperación internacional. La convención demuestra interés en el uso consciente de las Tecnologías de la Información y comunicación (TIC), así como la protección de los grupos en vulnerabilidad.

Por otro lado, como parte de la ONU se encuentra la Organización Internacional de Telecomunicaciones, es un organismo especializado en temas digitales y de tecnologías, la idea principal de su creación se basa en poder conectar a la comunidad internacional de manera segura y mejorar el acceso a la tecnología. Cuenta con más de 150 Estados miembros, así como instituciones de educación superior y empresas, interesadas en temas de comunicación en la red e interconectividad.

Entre sus metas se destaca "Mejora de la preparación de los países en materia de ciberseguridad (con capacidades clave: presencia de una estrategia, equipos nacionales de respuesta a incidentes/emergencias informáticas y legislación)" (ITU, s.f). Con relación a la necesidad de preparar a los países miembros en caso de un ataque cibernético, en principio brindar el conocimiento sobre qué son los ataques, los diferentes actores del sistema y a raíz de esto, otorgarles las herramientas para que puedan prever ataques y poder desarrollar de manera paulatina sus sistemas de defensa.

La presente organización busca en primera instancia la conectividad y la transformación de los sistemas, no obstante, muestra una cuota de protección en temas de seguridad cibernética, a pesar de no ser el objetivo central, sin embargo, es necesario de cara a los peligros que habitan dentro del ciberespacio. Es parte de los intereses de la ONU, en temas de la protección de la información de cada uno de sus Estados miembros.

Por otro lado, bajo la misma línea de organismos internacionales, es importante mencionar a la Organización de Estados Americanos (OEA), dicho organismo es regional con la unión de Estados americanos, dispuestos a establecer temas de cooperación y ayuda mutua. Dentro de sus funciones y órganos, conformaron uno relacionado directamente a temas tecnológicos y de ciberseguridad.

La organización tiene bajo su mandato un programa basado en ciberseguridad, el mismo cuenta con diferentes objetivos mencionados a continuación.

- Apoyar a los Estados Miembros de la OEA en el desarrollo de capacidades técnicas y políticas para prevenir, identificar, responder y recuperarse exitosamente de incidentes cibernéticos.
- Mejorar el intercambio de información, la cooperación y la coordinación sólidas, efectivas y oportunas entre las partes interesadas en seguridad cibernética a nivel nacional, regional e internacional.
- Aumentar el acceso al conocimiento e información sobre amenazas y riesgos cibernéticos por parte de los interesados públicos, privados y de la sociedad civil, así como los usuarios de Internet. (OEA, s.f).

A nivel de América impulsaron dichas funciones, su centro va dirigido a la cooperación e intercambio de información. Cada miembro de la OEA a nivel interno tiene sus medidas y preparaciones para poder responder a delitos informáticos o ataques cibernéticos. La asistencia técnica es su principal función para el resto de miembros, aunado a las capacitaciones, entre las motivaciones se encuentra la promoción de políticas públicas y diferentes estrategias a nivel nacional.

Sin embargo, no existe una acción en conjunto para hacer frente a un ataque a nivel global o regional, elemento que debe fortalecerse dentro de esta y el resto de organizaciones.

A nivel de los organismos internacionales presentados se puede observar que cada uno cuenta con su estructura sobre ciberseguridad y ataques informáticos, con la idea principal de poder capacitar y brindar las herramientas necesarias para sus actores miembros. Sin embargo, se puede comprender que no existe una acción conjunta global para combatir un ataque masivo a nivel internacional.

Propuestas de estrategias para la seguridad global.

La cooperación es la base fundamental para establecer políticas internacionales para el bien común, un mejor uso del ciberespacio, proclamar ciertas limitaciones y fronteras para un buen funcionamiento de los mismos.

Los Estados tienen sus herramientas y políticas internas, hace falta la capacidad de enfrentar situaciones de peligro y mejorar los procesos de cooperación en tecnología, aumento de capacitaciones y una red global de ayuda mutua. Para la protección de infraestructura crítica y el aumento de investigación, para tener bases claras en el desarme y el desmantelar los grupos terroristas o de hackers que se encuentren realizando ataques a diferentes medios.

Debido a esto, es necesario proponer estrategias para fortalecer la seguridad global frente a la militarización del ciberespacio. En el apartado final de la presente investigación, se tiene claridad sobre el desarrollo del ciberespacio y la militarización, así como el papel que cumplen los organismos internacionales, bajo la misma línea de pensamiento es importante destacar algunas propuestas para fortalecer la seguridad global en temas de ciberespacio.

Con relación a este objetivo número tres, debido a que ya se conoce el contexto del manejo de ciberespacio a nivel internacional, es muy importante destacar elementos o propuestas para manejar la situación a nivel internacional.

Como ya se ha observado, se debe ampliar directamente la investigación y el trabajo en conjunto para la ciberseguridad y el ciberespacio. Con el motivo de ejercer un control directo y más controlado, con acceso multiple y las mismas oportunidades para las empresas e individuos.

Entre los primeros puntos a destacar es importante establecer normas de carácter vinculante, dirigidas a las acciones producidas dentro del ciberespacio. Es importante elevar los tratados, normas y leyes que se tienen y adaptarlas a las necesidades del ciberespacio, donde se regulen las actividades de los Estados, instituciones y actores independientes, con el objetivo central de evitar conflictos o aumento de tensiones.

A raíz de lo anterior es necesario establecer protocolos de acción en caso de ataques a infraestructuras críticas, con la capacitación y preparación de los gobiernos y sus instituciones para poder cubrir las emergencias. Principalmente, brindar conocimientos para el desarrollo de los sistemas, en primera instancia, de países en vías de desarrollo, con bajo nivel en tecnología, mediante formaciones y el fortalecimiento de sus capacidades digitales.

A nivel empresarial e institucional, es necesario constituir estándares globales en los sistemas de seguridad, para asegurar un manejo correcto de los sistemas y por ende la protección de la infprmación de la empresa, los empleados y los clientes, genera una cadena de control sobre las bases de datos que cada uno maneje.

Aunado a esto, un elemento importante del ciberespacio es la sociedad civil, su participación es una base esencial del crecimiento del ciberespacio, sin embargo, por el constante cambio e innovación, se debe preparar a la población desde edades muy tempranas. Una población estudiada, consciente de su medio, ayuda a evitar diferentes tipos de ataques a distintas escalas, incluso les brinda la capacidad de dar solución, conocer su información y proteger sus datos, de igual forma, con la visión de disminuir los casos de trata de personas por medio de internet, delitos económicos y sociales más graves.

Uno de los ejes centrales y más importantes que se pueden plantear es el poder de la cooperación internacional, la unión de gobiernos e instituciones por medio de tratados, multilaterales o bilaterales, otorga la oportunidad de crear una estrategia global en temas de ciberseguridad, ciberespacio y delitos informáticos. Aunado a esto, se deben establecer lazos estratégicos y de confianza, para concer las amenazas del medio digital.

Identificar los ataques, los atacantes y los medios o su lugar de origen, es indispensable para poder descubrir a los actores detrás del ataque, de los diferentes virus o software que controlen los sistemas. Los Estados bajo un trabajo en conjunto pueden desarticular las células de los cibercriminales y rastrear dichas direcciones.

Es importante destacar que dentro del ciberespacio no existen froteras, dando paso a que los ataques puedan tener grandes magnitudes, aquí entra la cooperación internacional, la capacidad de colaborar de manera activa y genuina para alertar o dar a concoer sobre las amenazas que se estén produciendo. Debido a esto, debe existir la participación de los

gobiernos, así como del organismo internacional, que cuentan con bases sobre ciberseguridad y un conocimiento más amplio de la situación global.

Bajo la línea de la cooperación internacional, debe haber unión de medios sociales, políticos, económicos y legales. Dentro de las necesidades de la comunidad internacional, se debe crear marcos jurídicos y legales para los delitos cibernéticos, desde el impacto social hasta el financiero, donde se cubran las áreas más vulnerables y de interés de los actores del medio, sin dejar de lado el incluir los marcos legales o intereses de cada gobierno.

Por otro lado, con el desarrollo de la inteliencia artificial como se observa hoy en día, por medio de esta pueden establecerse controles y regulaciones sobre los movimientos ocurridos en el ciberespacio. Como una herramienta de uso publico, se debe desarrollar para la defensa desde los elementos más básicos como las contraseñas de redes sociales, para facilitar la ayuda a la población, así como detección de amenazas.

Cada una de estas propuestas deben ser evaluadas y llevadas a cabo por medio de la diplomacia y la diplomacia colaborativa, con la representación de cada Estado y ente de importancia. Para mantener la paz por medio de operaciones coordinadas, para proteger a la sociedad civil y sus derechos,

Resultados

A lo largo de la investigación se pueden observar cada uno de los elementos claves para comprender el ciberespacio, se puede entender que este tiene un nacimiento y desarrollo gracias al proceso de conexión y comunicación entre los sistemas, asimismo, el crecimiento de la tecnología ha fomentado el ingreso de los Estados, empresas, organismos internacionales hasta individuos a interactuar dentro de este.

Aunado a esto, es importante recalcar que dichas interacciones se dan por medio del uso de la información personal, para el intercambio de dinero, de bienes y servicios, esto crea nuevas líneas de debilidad dentro de los sistemas, pero también atracción para actores de

reciente nacimiento, como pueden ser actores individuales en este caso hackers o terroristas cibernéticos.

El manejo de información por parte de los sistemas ha fomentado el desarrollo de la ciberseguridad, donde su objetivo recae en proteger los datos sensibles de las personas y las instituciones, logrando de esta manera un ciberespacio seguro, a pesar de ser un sector sin fronteras delimitadas.

Dentro del análisis, es importante recalcar que el ciberespacio se encuentra en constante expansión y por ende, se observa una creciente amenaza con relación a los ataques cibernéticos, desde los más básicos como el uso de páginas falsas para obtener datos personales, hasta poder robar información por medio de la clonación de los datos biométricos o aún a mayor escala, ataques a infraestructuras críticas, que ponen en peligro a las personas y genera presión y tensión a los gobiernos por poder dar respuesta a los casos.

Debido a esto, es necesario establecer estrategias puntuales que actualmente no se observan con claridad, la ciberseguridad y el ciberespacio forman parte de la vida diaria de todos los individuos y la acción de los gobiernos e instituciones, a raíz de esto, es necesario crear organismos centralizados en instaurar metas, delimitaciones y observar el actuar de los miembros del ciberespacio.

Bajo esta misma línea, es importante recalcar la preparación y capacitación para las personas e instituciones, con el objetivo de poder observar y conocer sus debilidades y oportunidades, para poder respaldar la información y evitar ciertos ataques cibernéticos, así como bridar apoyo y capacitación a gobiernos en vías de desarrollo que necesiten potenciar su material digital y su apertura dentro del ciberespacio.

Una comunidad conectada y bajo un mismo objetivo, de la mano de leyes o estructuras para un desarrollo protegido, sería lo ideal para disminuir las tensiones existentes entre los Estados y ciertos actores de carácter independiente que se manejan dentro de este nuevo ámbito.

Con relación al primer objetivo específico, la evolución del ciberespacio ha sido puntual para establecer conexiones entre los Estados y actores claves, para mantener una comunidad informada, a pesar del aumento de tensiones y la diversidad de conflictos

surgidos, nacen herramientas y claves para la búsqueda de la disminución de tensiones en el ciberespacio, su militarización representa el poderío actual de cada actor, así como el hecho de ir ganando territorio en un sector que no cuenta con fronteras.

Por otro lado, con relación al objetivo específico número dos, los organismos internacionales han venido creciendo y desarrollándose junto con el ciberespacio, conforme este se ha desenvuelto dentro de la comunidad internacional, las funciones de los organismos, sus capacidades y objetivos también se han transformado, para hacer frente a los nuevos peligros que amenazan a la comunidad internacional y el ciberespacio, con un objetivo claro y es prevenir que este nuevo espacio se convierta en un medio peligroso y controlado por pequeños sectores, si no, que brinde acceso general y seguro a todos los actores públicos, privados, políticos, sociales, económicos, entre otros.

Con relación al tercer objetivo de la investigación, el alcance que ha tenido la militarización es exponencial, los Estados buscan presencia dentro del mismo, debido a esto, las estrategias propuestas son clave para hallar un lugar seguro en temas de manejo de información, capacitaciones y concientización de la población en temas tecnológicos y de redes, conociendo las bases y comprendiendo su alcance, para un debido proceso en la protección de sus datos personales como los de la empresa o sectores donde se desarrollen, desde las redes locales a externas, tendiendo un cuidado importante de la información delicada.

En conclusión, se rescatan tres puntos importantes, el ciberespacio forma y formará parte de la vida diaria, desde establecer relaciones diplomáticas, comerciales y financieras, ya que, a raíz de la pandemia, se afianzó la facilidad de comunicación e interconexión entre los ámbitos sociales y políticos.

Debido a este punto, surge con mayor fuerza la necesidad de crear en conjunto, por medio de las actividades de los organismos y gobiernos, leyes o estructuras en común para mantener un orden claro y disminuir o eliminar en su mayoría los peligros constantes que nacen por medio de los intereses o manejo de la información. Porque se tiene claro que a pesar de que existen organismos especializados en temas de ciberseguridad o elementos por parte de organismos internacionales, no se encuentra un tratado internacional o un organismo

que pueda regular estas acciones y se presente como una de las necesidades principales para la comunidad internacional.

Por último, se encuentra la importancia de mantener a los gobiernos, las instituciones y las personas informados sobre las situaciones del ciberespacio, en este caso, brindar capacitaciones y comprensión desde los ámbitos más básicos, como lo es el internet y la tecnología, para contar con las bases y posteriormente, herramientas para manejarse de manera segura por medio del ciberespacio, evitando ataques, virus, entre otras acciones que pueden poner el riesgo su situación, así como a los sistemas a los que se encuentre conectados, finalmente, tener la capacidad de fortalecer las infraestructuras críticas de los países, para evitar riesgos a gran escala que pueda afectar a los colaboradores o a la sociedad civil.

Es claro que el ciberespacio es un avance enorme para la conexión y comunicación internacional, conlleva nuevas tensiones y peligros a los que la comunidad internacional debe estar atenta, pero se posiciona como un cambio extremo para la sociedad, facilitando las actividades diarias y la capacidad de crear nuevas oportunidades de desarrollo y crecimiento para la sociedad y el sistema internacional.

Además, se comprende que el ciberespacio paulatinamente se va a convertir en un nuevo dominio militar, debido a los elementos estratégicos que este representa, cada uno va a buscar proteger sus intereses, asimismo, una consecuencia clave es la seguridad internacional, por el aumento de herramientas cibernéticas se crean peligros latentes, debido a esto, se tienen que buscar estrategias claves para hacer frente a dichas situaciones así como la búsqueda para desarticular células cibernéticas que se ponen en peligro.

Por lo tanto, es importante invertir en tecnologías avanzadas para promover grupos de protección, proteger los sectores de información de infraestructuras críticas y de los gobiernos centrales, para limitar el nacimiento de la guerra y conflictos entre actores del ciberespacio.

Bibliografía

Adab, G. (2019). El liberalismo en la teoría de relaciones internacionales: su presencia en la escuela española. Comillas Journal of International Relations. Volumen (16) 056-064.

Arreola, A. (31 de octubre de 2016). Ciberespacio, el campo de batalla de la era tecnológica. Estudios en Seguridad y Defensa, 11 (22): 109-138. Universidad Anáhuac Norte, México. https://esdegrevistas.edu.co/index.php/resd/article/view/212/330

Barbé, E. (1987). El papel del realismo en las Relaciones Internacionales. Revista de Estudios Políticos (Nueva Época). Núm 57.

Calderón, N. (2025). El ciberespacio como escenario de conflicto en el siglo XXI. ¿hacia la militarización de la ciberseguridad? Razón Crítica, 18, 1- 21. https://doi.org/10.21789/25007807.2110

Centro Superior de Estudios de la Defensa Nacional. (febrero, 2012). El ciberespacio. Nuevo escenario de confrontación. Ministerio de Defensa, Monografías del CESEDEN. https://publicaciones.defensa.gob.es/media/downloadable/files/links/m/o/monografia_126.pdf

Chaves, L y Guerrero, H. (2019). El ciberespacio, fuente de control y vigilancia para los ciudadanos. Perspectivas en inteligencia. 11 (20): 347-357. https://revistascedoc.com/index.php/pei/article/view/39/36

CICR. (noviembre de 2019). Derecho internacional humanitario y ciberoperaciones durante los conflictos armados. Comité International Geneve. https://www.icrc.org/sites/default/files/document/file_list/icrc_ihl_and_cyber_operations_during_armed_conflict_sp.pdf

Eissa, S, Gastaldi, S, Poczynok, I, Zacarías, M. (2012). El ciberespacio y sus implicaciones en la defensa nacional. Aproximaciones al caso argentino. Universidad Nacional de La Plata. https://sedici.unlp.edu.ar/bitstream/handle/10915/40210/Documento_completo.pdf?sequence=1

Galizia, R. (s.f). El manual de Tallin y la aplicabilidad del derecho internacional a la ciberguerra. (126-147). https://cefadigital.edu.ar/bitstream/1847939/993/1/Revista%20ESG%20no.588-2014_Fonseca_172.pdf

Gumba, C, Cando, K, Recalde, P. (2025). El impacto de la ciberseguridad en las relaciones internacionales. Volumen (4). 139-152 https://doi.org/10.62465/rri.v4n1.2025.138

Hernández, A. (s.f.). Investigación-Acción. Utilidad y modestia de las Ciencias Sociales. Centro de Investigaciones Psicológicas y sociológicas. Habana, Cuba. https://biblioteca-repositorio.clacso.edu.ar/bitstream/CLACSO/5646/1/cips3.pdf

Hernández, R et al. (2014). Metodología de la investigación. McGraw-Hill. https://www.esup.edu.pe/wp-content/uploads/2020/12/2.%20Hernandez,%20Fernandez%20y%20Baptista-metodolog%C3%ADa%20Investigacion%20Cientifica%206ta%20ed.pdf

LISA Institute. Infraestructuras críticas: definición, planes, riesgos, amenazas y legislación. https://www.lisainstitute.com/blogs/blog/infraestructuras-criticas#:~:text=En%20otras%20palabras%2C%20las%20infraestructuras,%2C%20econ%C3%B3mico%2C%20medioambiental%20y%20pol%C3%ADtico

Lodoño, O, Maldonado, L, Calderón, C. (2016). Guía para construir estados del arte.

Markovski, V y Trepykhalin, A. (31 de enero 2022).Informe de enfoque por países: leyes e iniciativas de políticas relacionadas con internet en China. https://itp.cdn.icann.org/es/files/government-engagement-ge/ge-010-31jan22-en.pdf

Matú, D. (2022). La militarización del Ciberespacio por parte de los Estados Unidos, 2008-2015. Universidad Autónoma del Estado de Quintana Roo. https://risisbi.uqroo.mx/bitstream/handle/20.500.12249/2945/UB21.2.2022-2945.pdf?sequence=1&isAllowed=y

Mendoza, M. (2020). ¿Qué son los organismos internacionales y cuál es su origen? Universidad Intercontinental. https://www.uic.mx/importancia-de-los-organismos-internacionales-en-el-comercio-

exterior/#:~:text=%C2%BFQu%C3%A9%20son%20los%20organismos%20internacionales,que%20existi%C3%B3%20fue%20%E2%80%9CVersalles%E2%80%9D.

Microsoft. (s.f). ¿Qué es la ciberseguridad? https://support.microsoft.com/es-es/topic/-qu%C3%A9-es-la-ciberseguridad-8b6efd59-41ff-4743-87c8-0850a352a390#:~:text=La%20ciberseguridad%2C%20tambi%C3%A9n%20conocida%20como,fotos%20e%20incluso%20el%20dinero.

Ministerio de Relaciones Exteriores Colombia. (s.f). Cooperación internacional. https://www.cancilleria.gov.co/cooperacion-internacional

Mishra, V. (2024). La Asamblea Generals de las Naciones Unidas adopta un tratado histórico sobre la ciberdelincuencia. https://news.un.org/en/story/2024/12/1158521

Organización de Estados Americanos OEA. (s.f). Programa de Ciberseguridad. https://www.oas.org/ext/es/seguridad/prog-ciber

Quintana, L, Hermina, J. (2019). La hermenéutica como método de interpretación de textos en la investigación psicoanalítica. Perspectivas en psicología: Revista de psicología y ciencias afines. Volumen (16). 73-80 https://www.redalyc.org/journal/4835/483568603007/html/

Rivadeneira, E. (2016). Stuxnet, la primera ciberama. Revista ciencia y tecnología. (76-81). https://revistamarina.cl/revistas/2016/2/efrederickr.pdf

Santana, E & Báez, K. (2022). Ciberespacio y Cibermundo: delimitaciones conceptuales desde el materialismo sistémico. Ciencia y Sociedad, 47(1), 45–57. https://doi.org/10.22206/cys.2022.v47i1.pp45-57

Tah, E. (2018). Las Relaciones Internacionales desde la perspectiva social. La visión del constructivismo para explicar la identidad nacional. Revista mexicana de ciencias políticas y sociales. Volumen (63). 389-404. https://www.scielo.org.mx/pdf/rmcps/v63n233/0185-1918-rmcps-63-233-389.pdf

The International Telecomunication UNIO (UTI). (s.f). Acerca de la Unión Internacional de Telecomunicaciones. https://www.itu.int/en/about/Pages/default.aspx#/es