Análisis de las operaciones de Fuerzas Armadas ecuatorianas en el ciberespacio y los medios necesarios para contrarrestar el ciberespionaje y el cibersabotaje desde la creación del comando de ciberdefensa hasta el 2022

Espinosa Carrera, Jaime Patricio y Espinoza Martínez, Christian Raúl

Vicerrectorado de Investigación, Innovación y Transferencia de Tecnología

Centro de Posgrados

Maestría en Defensa y Seguridad mención Logística Militar

Trabajo de titulación previo a la obtención del Título de Magister en Defensa y Seguridad mención Logística Militar

TCRN COM EM Semanate Esquivel, Ángelo

20 de febrero de 2023

COPYLEAKS

TC. ESPINOSA P. TC.ESPINOZA C.docx

Scanned on: 17:17 March 6, 2023 UTC

5.9% Overall similarity score

67 Results found

13813 Total words in text

	Word count
Identical	506
Minor Changes	136
Paraphrased	165
Omitted	226

Vicerrectorado de investigación, innovación y Transferencia de tecnología

Centro de Posgrados

Certificación

Certifico que el trabajo de titulación, **"Análisis de las operaciones de Fuerzas Armadas ecuatorianas en el ciberespacio y los medios necesarios para contrarrestar el ciberespionaje y el cibersabotaje desde la creación del comando de ciberdefensa hasta el 2022"** fue realizado por los señores **Espinosa Carrera, Jaime Patricio y Espinoza Martínez, Christian Raúl,** el mismo que cumple con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, además fue revisado y analizado en su totalidad por la herramienta de prevención y/o verificación de similitud de contenidos; razón por la cual me permito acreditar y autorizar para que se lo sustente públicamente.

Sangolquí, 20 de febrero de 2023

Firmado electrónicamente por:
ANGELO SEMANATE ESQUIVEL

TCRN COM EM Semanate Esquivel, Ángelo
Director
C.C. 0501805352

Vicerrectorado de Investigación, Innovación y Transferencia de Tecnología

Centro de Posgrados

Responsabilidad de Autoría

Nosotros, **Espinosa Carrera, Jaime Patricio** con cédula de ciudadanía N° 1711440063 y **Espinoza Martínez, Christian Raúl**, con cédula de ciudadanía N° 1710873322, declaramos que el contenido, ideas, y criterios del trabajo de titulación: **"Análisis de las operaciones de Fuerzas Armadas ecuatorianas en el ciberespacio y los medios necesarios para contrarrestar el ciberespionaje y el cibersabotaje desde la creación del comando de ciberdefensa hasta el 2022"** es de nuestra autoría y responsabilidad, cumpliendo con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, respetando los derechos intelectuales de terceros y referenciando las citas bibliográficas.

Sangolquí, 20 de febrero de 2023

firmado electrónicamente por:
JAIME PATRICIO
ESPINOSA CARRERA

Espinosa Carrera, Jaime Patricio
C.C. 1711440063

firmado electrónicamente por:
CHRISTIAN RAUL
ESPINOZA MARTINEZ

Espinoza Martínez, Christian Raúl
C.C. 1710873322

Vicerrectorado de Investigación, Innovación y Transferencia de Tecnología

Centro de Posgrados

Autorización de Publicación

Nosotros, **Espinosa Carrera, Jaime Patricio** con cédula de ciudadanía N° 1711440063 y **Espinoza Martínez, Christian Raúl**, con cédula de ciudadanía N° 1710873322, autorizamos a la Universidad de las Fuerzas Armadas ESPE publicar el trabajo de titulación: **"Análisis de las operaciones de Fuerzas Armadas ecuatorianas en el ciberespacio y los medios necesarios para contrarrestar el ciberespionaje y el cibersabotaje desde la creación del comando de ciberdefensa hasta el 2022"** en el Repositorio Institucional, cuyo contenido, ideas y criterios son de nuestra autoría y responsabilidad.

Sangolquí, 20 de febrero del 2023

Firmado electrónicamente por:
JAIME PATRICIO
ESPINOSA CARRERA

Firmado electrónicamente por:
CHRISTIAN RAUL
ESPINOZA MARTINEZ

Espinosa Carrera, Jaime Patricio
C.C. 1711440063

Espinoza Martínez, Christian Raúl
C.C. 1710873322

Dedicatoria

Dedicamos este trabajo a Dios Todopoderoso que hizo posible se cumpla una meta más para el fortalecimiento de nuestra carrera militar.

A nuestros padres, esposas e hijos que nos brindaron amor y comprensión, sin este apoyo, el camino sería difícil de seguirlo.

Gracias a todos!

Patricio y Christian

Agradecimiento

El agradecimiento a nuestra querida institución la cual nos ha permitido alcanzar cada una de las metas para ser parte de este glorioso Ejército.

Patricio y Christian

Índice

Índice de tablas

Índice de figuras

Resumen

El presente trabajo titulado “Análisis de las operaciones de Fuerzas Armadas ecuatorianas en el ciberespacio y los medios necesarios para contrarrestar el ciberespionaje y el cibersabotaje desde la creación del comando de ciberdefensa hasta el 2022”, realizó un trabajo investigativo aplicando una metodología exploratoria, descriptiva y correlacional con enfoque cuantitativo y planteó la hipótesis que afirma que a partir de la creación del Comando de Ciberdefensa hasta el 2022, el análisis de la capacidad de FF.AA. para utilizar las operaciones militares del ciberespacio permitirá enfrentar el ciberespionaje y el cibersabotaje. Se propuso como objetivo ejecutar un análisis de la capacidad de FF. AA para utilizar las operaciones militares del ciberespacio y los medios para contrarrestar el ciberespionaje y el cibersabotaje desde la creación del Comando de Ciberdefensa hasta el 2022. A través de las encuestas a 125 oficiales, se pudo concretar la falta de equipo del que carece FF. AA para el control del ciberespacio, así como la capacitación adecuada. Existe además un desconocimiento del 82% de las Amenazas Persistentes Avanzadas cuya intervención están relacionadas directamente con el ciberespacio. Para determinar las estrategias, se trabajó con el análisis FODA, concluyendo con las Matrices EFE y EFI. Al validar las matrices se definió que las estrategias ofensivas son las específicas para este propósito. De manera concluyente se recomienda establecer programas y proyectos de I+D+i propios de FF. AA para implementar sistemas de información y comunicación seguros, mejorar la interoperabilidad interna y externa bajo normas y estándares internacionales.

Palabras clave: ciberespacio, cibersabotaje, ciberespionaje, ciberseguridad, ciberdefensa

Abstract

The present work entitled "Analysis of the operations of the Ecuadorian Armed Forces in cyberspace and the necessary means to counteract cyber espionage and cyber sabotage since the creation of the cyber defense command until 2022", carried out an investigative work applying an exploratory, descriptive and correlational with a quantitative approach and raised the hypothesis that states that from the creation of the Cyber Defense Command until 2022, the analysis of the capacity of the Armed Forces. to use the military operations of cyberspace will allow to face cyber espionage and cyber sabotage. It was proposed as an objective to carry out an analysis of the capacity of FF. AA to use military cyberspace operations and the means to counter cyber espionage and cyber sabotage from the creation of the Cyber Defense Command until 2022. Through surveys of 125 officers, it was possible to specify the lack of equipment that the FF lacks. AA for the control of cyberspace, as well as adequate training. There is also an ignorance of 82% of Advanced Persistent Threats whose intervention is directly related to cyberspace. To determine the strategies, we worked with the SWOT analysis, concluding with the EFE and EFI Matrices. When validating the matrices, it was defined that the offensive strategies are the specific ones for this purpose. Conclusively, it is recommended to establish FF own R&D&I programs and projects. AA to implement secure information and communication systems, improve internal and external interoperability under international norms and standards.

Keywords: cyberspace, cyber sabotage, cyberespionage, cybersecurity, cyber defense

Capítulo I

Planteamiento del problema

Formulación del problema

El ciberespacio se ha convertido en el dominante de los Sistemas de Mando y Control y su dependencia a este es cada vez mayor en el ámbito militar, estatal y privado. Esto ha generado una nueva amenaza a la seguridad nacional si no se controla adecuadamente el ciberespacio considerado como un espacio estratégico para la seguridad y como consecuencia, se debe planear la correspondiente Defensa Nacional por lo que habrá que definir en ella los objetivos a alcanzar y las medidas de prevención, disuasión, protección y reacción de la ciberdefensa (Enriquez, 2012).

Naciones desarrolladas como Estados Unidos han sufrido múltiples ciberataques a objetivos gubernamentales y empresariales usando ransomware[1] involucrando una petición de rescate, transfórmense en un cibersabotaje, ya que su intención era dañar la reputación de las organizaciones. Se acusa a China y a una contratación de redes criminales para invadir y extorsionar al gobierno de Baiden y a instalaciones estratégicas americanas.

El ciberespionaje y el cibersabotaje son amenaza relacionada con el robo de información, tanto en empresas particulares como en instituciones gubernamentales. Los propósitos son múltiples, van desde el aspecto económico, hasta el causar daño y desprestigio a una institución, el cibercriminal se infiltra en las redes de comunicación de funcionarios para obtener datos confidenciales sensible y credenciales de acceso a ordenadores, dispositivos móviles y equipos de red. Un ejemplo de este caso es el denunciado por Julian Assange y los Wikileaks que acusaba a la CIA de ciberespionaje a través[2] de televisores y celulares.

[1]El Ransomware es un software malicioso que al infectar nuestro equipo le da al ciberdelincuente la capacidad de bloquear un dispositivo desde una ubicación remota y encriptar nuestros archivos quitándonos el control de toda la información y datos almacenados, El virus lanza una ventana emergente en la que nos pide el pago de un rescate, dicho pago se hace generalmente en moneda virtual (bitcoins por ejemplo) **Fuente especificada no válida.**.

[2]

Esta situación se ha agravado debido al aumento de población con acceso a internet, sobre todo en el último año debido a la pandemia de COVID-2019, la fata medidas de protección y prevención para las amenazas y peligros de su uso, ocasionado por la falta de una educación formal sobre el tema informático. La creciente de elementos disruptivos ha incrementado una variedad de amenazas y ataques dentro del contexto tecnológico y que ha sido aprovechado por la delincuencia común como la delincuencia organizada poseedora de equipos sofisticados, redes criminales y su esmero de campañas de ransomware.

En Ecuador la situación no es diferente, el país no cuenta con una estrategia de seguridad cibernética, a pesar de haber logrado algunos avances significativos en la mejora de sus capacidades a este nivel. Para mejorar el enfrentamiento a estas amenazas, se han registrado casos significativos como los casos del Banco de Pichincha y a la Corporación Nacional de Telecomunicaciones CNT, esta última sufrió un ataques de alta sofisticación obligada a declararse en emergencia institucional (El Comercio, 2021). Estos casos se tipifican dentro de la ciberdelincuencia.

Con la llegada del nuevo gobierno en mayo de 2021, se promulgó el Plan de Creación de Oportunidades 2021-2025 donde se plantea como política el “fortalecimiento del Estado para mantener la confidencialidad, integridad y disponibilidad de la información frente a amenazas provenientes de ciberespacio y proteger su infraestructura crítica” (Secretaría Nacional de Planificación, 2021), adicionalmente se propone incrementar el Índice de Ciberseguridad Global de 26.3 a 51.3 como meta para el 2025, considerando además, que Ecuador ocupa el 6to lugar entre todos los países de la región (Ministerio de Telecomunicaciones, 2020)

Con estos parámetros, este trabajo se propuso resolver la interrogante planteada en la siguiente formulación del problema:

¿Cuál es la situación de las operaciones de Fueras Armadas en el ciberespacio para enfrentar el ciberespionaje y el cibersabotaje desde la creación del Comando de Ciberdefensa hasta el 2022?

Antecedentes

En el mundo actual ha surgido una nueva dimensión donde pueden materializarse las amenazas: el ciberespacio. Anteriormente, en el ámbito de la defensa, estaba claro que se movía en las tres dimensiones de tierra, mar y aire, e incluso el espacio, ahora se cuenta con una dimensión adicional, y más intangible que las anteriores (Caro, 2021)

Debido a la incorporación de las TIC en el ámbito militar y en las Fuerzas y Cuerpos de Seguridad de los Estados, es incuestionable la gran dependencia existente del ciberespacio en funciones básicas como el apoyo logístico, el mando y control de las fuerzas, la información de inteligencia en tiempo real (Díaz del Río, 2010) o en la información de los campos de batalla, en las comunicaciones, en los sistemas armamentísticos, así como en los sistemas aéreos, marítimos y terrestres.

Es así como, el interés por mantener la seguridad nacional en un Estado es fundamental para su desarrollo constante. Estudios como el propuesto definirán parámetros alineados a la ciberseguridad y ciberdefensa implicadas directamente a la seguridad nacional.

Justificación

El avance tecnológico, ha obligado a los Estados a ampliar sus dimensiones de seguridad, y este nuevo campo de batalla llamado ciberespacio presente en este siglo XXI con nuevas amenazas de características asimetrías y sin fronteras.

Estas características hacen que las acciones ofensivas en el ciberespacio, o la simple presunción de contar con la capacidad de poder realizarlas, se están convirtiendo en métodos de disuasión cada vez más utilizados por los actores amenazantes actuales en el ciberespacio (Sánchez-Román, 2020).

Las acciones en el ciberespacio, que tienen cada vez más influencia en las operaciones militares en sus dominios tradicionales (tierra, mar y aire), han irrumpido con fuerza en el marco de la guerra híbrida y la sola presunción de tener la capacidad de realizarlas podría ser utilizada por los Estados como medida de disuasión para evitar ser atacados. Por esta razón, se reconoce al ciberespacio como el quinto dominio de las

operaciones militares actuando de manera transversal con los otros dominios o entornos operacionales tradicionales (Arreola, 2016).

El Ministerio Nacional de Defensa, en la Política de Seguridad y Defensa en el Plan Nacional de Seguridad Integral 2019-2030, considera como condición sine qua non contar con un marco jurídico que garantice el empleo efectivo de las unidades en sus diferentes niveles y dimensiones (aire, mar, tierra, ciberespacio y espacio ultraterrestre). La intervención de las amenazas sustentadas por redes delincuenciales, con carácter dimensional, no tienen limitaciones internas o externas por lo que los diferentes organismos con responsabilidad de brindar seguridad deberán redefinir sus capacidades y competencias para asistir en estos nuevos escenarios (Ministerio de Defensa Nacional, 2019).

Con este antecedente, se realizó un análisis para justificar el trabajo del Comando de Ciberdefensa, el cumplimiento de sus objetivos, lineamientos y su relación con las operaciones militares en el ciberespacio.

Esta investigación abarcó la comprobación de la presencia de las amenazas cibernéticas en el ciberespacio ecuatoriano, sus actores y la afectación a la Seguridad Nacional.

Otro punto fundamental fue determinar las limitaciones legales, y definir el impacto de la defensa nacional al desarrollar capacidades militares para su mejor desenvolvimiento en este espacio virtual donde no existen límites entre lo público y privado, donde las amenazas híbridas serán persistentes.

Importancia

En el terreno militar la tecnología supone un desafío mayor puesto que se relacionan con la seguridad y defensa nacional, tipificada en la misión del Ejército. Este trabajo aportó con análisis conceptuales acogidos en el entorno de ciberespacio y sus temas conexos, aportando una visión general de sus características en el ámbito militar.

Al concretar esta investigación, permitió evaluar la importancia del trabajo del Comando de Ciberdefensa. Al final se podrá emitir conclusiones que ayuden cumplir su

objetivo enmarcado en reforzar la seguridad y defensa de la soberanía e integridad territorial que pueda verse afectada por situaciones de espionaje desde cualquier parte del mundo.

El trabajo busca mostrar la necesidad de una estrategia de ciberseguridad a nivel nacional, pero ofreciendo también, los retos y oportunidades a los que se enfrenta el Ejército, encubiertos en las acciones de ciberataje y ciberespionaje.

Este estudio es importante en la medida que esta investigación va a aportar con información relevante, recolectada de fuentes primarias como secundarias y se nutrirá además con técnicas prospectivas que definirán los factores y actores que influirán en las capacidades de respuesta por parte de las fuerzas militares adaptándose al ritmo de a un mundo tecnológicamente cambiante.

Objetivos

Objetivo general

Ejecutar un análisis de la capacidad de FF.AA. para utilizar las operaciones militares del ciberespacio y los medios para contrarrestar el ciberespionaje, el cibersabotaje desde la creación del Comando de Ciberdefensa hasta el 2022.

Objetivos específicos

- Definir las amenazas cibernéticas que atentan el ciberespacio afectando a la Seguridad Nacional.
- Analizar la situación actual del Comando de Ciberdefensa (COCIBER) dentro de Fuerzas Armadas y las limitaciones para el cumplimiento de sus objetivos y metas desde su creación en 2014 hasta la fecha.
- Plantear estrategias para las operaciones del ciberespacio que contrarresten el ciberespionaje, cibersabotaje que atentan a la seguridad nacional.

Capítulo II

Marco teórico

Antecedentes investigativos

Hoy en día, resulta imposible concebir el planeamiento y la conducción de las operaciones militares sin contar con las capacidades que proporciona el espacio en múltiples aspectos. Es así como la ciberseguridad emerge ante el creciente uso del ciberespacio como nueva dimensión para la interacción social, resultado de la revolución de la tecnología de la información y comunicación (TIC), que ha acelerado el proceso de globalización y periódicamente sorprende con su constante innovación, dando la oportunidad para el desarrollo de nuevas amenazas.

Por las características de este espacio, las amenazas recurrentes se acoplan a este, es decir mantendrán la particularidad de “ciber”, que etimológicamente indica “redes informáticas”. De aquí parte el ciberespionaje y el cibersabotaje que específicamente será el tema de este trabajo.

Los temas asociados a este trabajo involucran a la tecnología, las nuevas amenazas con características ciber y la situación del Comando de Ciberdefensa en relación a las operaciones militares del ciberespacio. Este organismo, para el año 2021 ha demostrado un avance generalizado por la conectividad, generando el aumento los ciberataques sobre todo a la infraestructura crítica del Estado, por lo que es necesario diseñar políticas intersectoriales, directrices y lineamientos para el empleo, uso y explotación de los sistemas de tecnología e información (Minsiterio de Defensa Nacional, 2017).

Por lo dicho los debates sobre defensa nacional y el diseño de las fuerzas militares para desarrollar capacidades militares que contrarresten el ciberespionaje y el cibersabotaje dentro de los objetivos de la ciberseguridad, han despertado el interés en FF.AA. ganando cuidado en todos los ámbitos sobre todo para la seguridad y defensa nacional.

Partiendo de lo anterior, el presente estudio se estructura en tres temas centrales. El primero, examinará las condiciones que hacen del ciberespacio el nuevo ámbito de guerra; donde, a pesar de su invisibilidad, se pueden realizar ataques contra los Estados, su

infraestructura y su población. En segundo término, se analizará el por qué las computadoras y sus accesorios son potencialmente tanto armas de guerra como los blancos de los ataques cibernéticos. Para posteriormente pasar a la descripción de las principales amenazas a la seguridad de los Estados y las razones que motivan a los diversos actores a realizar ciberataques que pueden escalar hasta la ciberguerra.

Fundamentación teórica

Antecedentes de la investigación

En la cumbre de la OTAN de 2016, en Varsovia, se reconoció al ciberespacio como un nuevo dominio de operaciones, al lado del espacio terrestre, del espacio marítimo, el espacio aéreo y el espacio exterior, proponiéndose la Organización a mejorar la ciberdefensa de sus redes e infraestructuras como un asunto prioritario (Argumosa, 2020).

Con estas circunstancias, es importante “analizar las reglas, principios, actores, estrategias, amenazas y oportunidades que dan forma a la geopolítica del espacio incluyendo la Luna actualmente, con especial atención al proceso de configuración de las dinámicas y normas que caracterizarán la nueva era espacial” (Santa-Bárbara, 2021, pág. 1).

Todos estos espacios, en los que conviven actores estatales y no estatales, ofrecen sin duda grandes oportunidades y riesgos, desde el punto de vista civil como militar, con una escasa regulación normativa y legalizaciones nacionales como internacionales.

Revisando la bibliografía que sustente esta investigación se analizó el trabajo de Torres (2019) titulado “El futuro de la competición estratégica a través del ciberespacio”. Se planteó el objetivo de analizar las principales incertidumbres sobre cómo evolucionará la rivalidad estratégica entre Estados a través del ciberespacio durante los próximos cinco años, resolviendo su planteamiento con una metodología analítica-descriptiva, llegó a la conclusión que el futuro de la competencia estratégica en el ciberespacio no está condicionado únicamente por la tecnología. Los atributos de los diferentes actores políticos y naturales son los influyentes en este espacio (Torres, 2019) , en estos se incluye a las fuerzas armadas de cada nación como entres protectores de la seguridad nacional.

Los Global Commons como el ciberespacio y el espacio ultraterrestre enfrentan amenazas globales y sus consecuencias. Así lo presenta Molina (2021) en su investigación “Geopolítica espacial y búsqueda de recursos” cuyo objetivo es señalar cuáles son las amenazas globales y las iniciativas para paliar las consecuencias y a su vez describir los recursos espaciales que poseen un mayor atractivo para afrontar los nuevos retos derivados del crecimiento de la población mundial. Usando el método descriptivo, al concluir enumera los recursos encontrados en el espacio como el agua, minería espacial y explotación de tierras raras como el platino, hierro, cobalto, hidrógeno, oro, calcio, etc. Las amenazas siempre estarán relacionadas con la explotación de estos recursos. Sin embargo, la autora considera que la lucha por el espacio ultraterrestre no se ve llegar en corto tiempo, las grandes naciones primero sobreexplotarán la tierra y la industria privada aprovechara el espacio de manera turística antes que intervenir sobre sus recursos.

De aquí parte otro estudio importante. Kutt (2021) donde enuncia “La importancia de dominar los Global Commons en el siglo XXI”. Su objetivo es describir y conceptualizar de manera concreta los beneficios de un espacio común cuyo uso compartido resulte beneficioso para todos los actores participantes, que lógicamente tendrían su interés legítimo en su conservación y libre disfrute. Identificando en primer lugar la obligación de protección de los global Commons del siglo XXI, en particular el espacio ultraterrestre y el ciberespacio. La conclusión a su trabajo está dirigida al compromiso de la “Comunidad Internacional de controlar la tendencia a la militarización de los espacios comunes, antes que un dilema de seguridad nos lleve a un enfrentamiento armado por el control de los global Commons, de consecuencias imprevisibles” (Kutt, 2021, pág. 19) .

Feliu (2021) escribe “La ciberseguridad y la ciberdefensa”, cuyo objetivo es realizar una reseña histórico de los conflictos armadas, para justificar la necesidad de implementar ciberseguridad y ciberdefensa en el ciber espacio de cada nación y mantener la seguridad nacional. Aplicando el método analítico-descriptivo tipifica su conclusión encamina a afirmar que estamos frente a un nuevo escenario estratégico con la presencia de un nuevo Global Common, un nuevo campo de batalla, donde se producen los comportamientos o

fenómenos conocidos en todos los conflictos pero que aquí emplean técnica nuevas de las propias características del ciberespacio.

La normativa jurídica en cuando al ciberespacio también no es clara Castellón y López (2016) realizan un estudio titulado “Crisis y ciberespacio: hacia un modelo integral de respuesta en el Sistema de Seguridad Nacional”, enuncia la Estrategia de Seguridad Nacional del 2015 de los Estados Unidos promulgada por el presidente Barack Obama, y explica que el control de los Global Commons se ha convertido en un objetivo estratégico de primer orden y entre ellos el ciberespacio ocupa el primer lugar. Concluye al decir que el mundo está en un juego geopolítico y geoeconómico con inmensas consecuencias sobre el poder, la prosperidad y la seguridad de los Estados y las sociedades, Un juego que carece todavía de reglas claras que lo ordenen y hasta que las tengamos habrá margen para malentendidos fatales.

Otra investigación que contribuye con información relevante es la escrita por Gil (2017). “La integración del ciberespacio en el ámbito interno”, propone la necesidad de cambios a la seguridad y defensa así como planteamientos estratégicos. El ciberespacio supone la desaparición de las fronteras tal y como las concebíamos, lo que supone nuevos desafíos para poder distinguir entre seguridad interior y exterior, viéndose acentuada esta situación por la falta de una normativa internacional al respecto. El trabajo concluye explicando que estas novedades suponen cambios en las doctrinas militares, plantea nuevas cuestiones estratégicas, como la disuasión en el ciberespacio, o genera nuevos conceptos, como el de ciberguerra o ciberarma.

En el marco del ciberespacio Aguilar (2021) presenta un trabajo regional titulado “Retos y oportunidades en materia de ciberseguridad de América Latina frente al contexto global de ciberamenazas a la seguridad nacional y política exterior”, su objetivo es analizar de manera individual, los esfuerzos de los países latinoamericanos en el desarrollo de una política nacional para el control del ciberespacio, encaminados a la ciberseguridad y la construcción de cibercapacidades por parte de las Fuerzas Armadas.

La metodología analítica, documental y bibliográfica con base en los informes sobre la materia presentados por la Organización de los Estados americanos (OEA) y el Banco Interamericano de Desarrollo (BID), así como los indicadores del National Ciber Security Index (NSCI) y el Global Cybersecurity Index (GCI) consiguió hacer comparaciones entre los países objetivos y otras naciones del mundo. La conclusión fundamental describe que en las últimas décadas las amenazas y riesgos provenientes del ciberespacio se han incrementado a un ritmo acelerado, transformando a la ciberseguridad en un tema central de la policía de seguridad nacional, así como factores de trascendencia de la política exterior de los Estados-Nación. Se demostró además que:

En América Latina detenta carencias en el desarrollo de cibercapacidades en el ámbito militar y una política nacional de ciberseguridad que edifique una Estrategia Nacional de Ciberseguridad apta para encarar los retos y amenazas provenientes del ciberespacio, con el fin de salvaguardar su seguridad nacional y política exterior (Aguilar, 2021, pág. 193).

Haciendo una relación entre los estudios presentados, el escenario prospectivo para la siguiente década no es muy halagador. Domínguez (2017) en su estudio “La ciberguerra como realidad posible contemplada desde la prospectiva”, en su objetivo general plantea la posibilidad de una gran confrontación entre grandes potencias, Estados Unidos y China son las naciones con mayor ponencia para demostrar su hegemonía, sin dejar a un lado a Rusia. Aplicando un método descriptivo-analítico, su trabajo llega a la conclusión que la ciberguerra es presente y es futuro.

Los países desarrollados serán los más capacitados para repeler las agresiones del ciberespacio, al contrario que los llamados del tercer mundo, serán los que contribuyan a la desestabilización de sistemas políticos y económicos por no contar con una normativa, reglamentos o siga el Derecho Internacional para el cuidado del Ciberespacio.

Se complementa el estudio investigativo con el trabajo realizado por Castro (2015) orientado en el Estudio prospectivo de la ciberdefensa en las Fuerzas Armadas del Ecuador”. Enfoca el objetivo en determinar las variables de cambio, hechos portadores del

futuro y actores más trascendentales que configurarían los escenarios alternativos que el ámbito de la Ciberdefensa enfrentaría las Fuerzas Armadas ecuatorianas en el año 2017.

Realiza una metodología que correlaciona entre sus variables para analizar su mutua asociación y el método prospectivo FAR[3] para identificar los escenarios prospectivos al 2017. En sus conclusiones Castro explica la necesidad de implementar un marco legal en el campo de la seguridad de la información, al igual que las políticas del Estado en el campo de la Ciberseguridad y la Ciberdefensa, la capacitación del talento humano para la Ciberdefensa para mejorar sus habilidades, destrezas, aptitudes en el campo informático.

Fundamentación conceptual

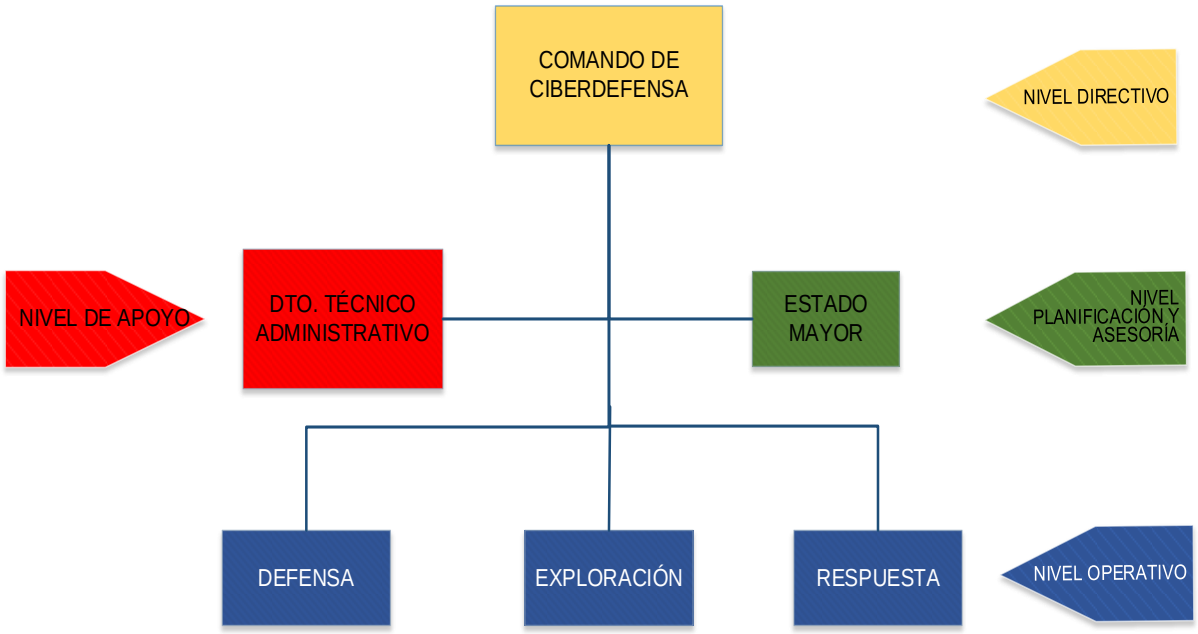
Bases teóricas

Comando de ciberdefensa.- El 12 de septiembre de 2014, por el Acuerdo Ministerial No. 281 se crea el Comando de Ciberdefensa dentro de las Fuerzas Armadas, con la misión de "proteger y defender la infraestructura crítica e información estratégica del Estado mediante operaciones de protección del espacio cibernético, acciones de prevención, disuasión, explotación y respuesta ante eventuales amenazas, riesgos e incidentes.

[3] Para realizar este análisis se aplica el método de Relación de Anomalías de Campo (FAR) por su siglas en inglés de Field Anomaly Relaxation

Figura 1

Organización del COCIBER – 2014



Una tarea fundamental que se vuelve más importante es la protección de la información estratégica y la infraestructura crítica del país y de los ciudadanos y ciudadanas, así como las redes y la información electrónica, para lo cual se requiere fortalecer estrategias de ciberdefensa (Ministerio de Defensa Nacional del Ecuador, 2014).

En este contexto el Ministerio de Defensa, determina que las acciones cibernéticas deben tener las siguientes denominaciones según el nivel de decisión

1. Nivel político - Seguridad de la información y las comunicaciones (SIC) y Seguridad cibernética - coordinado por la Presidencia de la República y que abarca la administración pública federal directa e indirecta (FPA), así como las infraestructuras de información crítica inherentes a las infraestructuras críticas nacionales.

2. Nivel estratégico - Defensa cibernética: a cargo del MD, Jefes de Estado Mayor Conjunto de las Fuerzas Armadas (EMCFA) y los Comandos de la FA, que interactúan con la Presidencia de la República y la APF; y

3. Niveles operativos y tácticos - Guerra cibernética: nombre restringido al alcance interno de las FF.AA. (Vergara & Trama, 2017)

El 5 de marzo de 2021 se inauguró un nuevo Comando de Ciberdefensa a través del cual implementará las estrategias para contrarrestar los ciberataques y la ciberguerra en contra de sus entidades críticas (Infodefensa.com, 2021).

Su objetivo será reforzar la seguridad y defensa de la soberanía e integridad territorial que pueda verse afectada por situaciones de espionaje desde cualquier parte del mundo, modernizando además las capacidades operativas de las fuerzas.

“Se plantea alcanzar desde el nuevo Comando tratar la ciberdefensa como un bien público de carácter no solo nacional sino regional, buscando que el continente sea una zona blindada en contra de posibles ataques cibernéticos” (Infodefensa.com, 2021).

Operaciones Militares. - Son el conjunto de actividades realizadas por unidades del Ejército, en forma independiente o como parte de una fuerza mayor, con tropas y medios orgánicos o bajo cualquiera de las relaciones demando, coordinadas en tiempo y en espacio, de acuerdo con lo establecido en una directiva, plan u orden para el cumplimiento de una misión o tarea (Comando de Educación y Doctrina del Ejército, 2015, pág. 11)

Operaciones cibernéticas. - En relación a las oraciones militares en el ciberespacio son todas aquellas en las que se emplean capacidades “ciber” con el objetivo principal de alcanzar objetivos militares en el ciberespacio o a través de este. Estas operaciones se planean igual que en el resto de los dominios, es decir en niveles tácticos, operacionales y estratégicos (García, 2018). “Son complementarias a las tradicionales, y por lo tanto tenidas en cuenta después que se formula el Plan de Maniobra” (Vergara & Trama, 2017, pág. 48)

Para el Reino Unido, las operaciones cibernéticas son la planificación y sincronización de actividades en y a través del espacio cibernético para permitir la libertad de maniobra y, de esa manera, alcanzar los objetivos militares. Pueden categorizarse en cuatro funciones distintas: las operaciones cibernéticas defensivas (DCO); las operaciones cibernéticas ofensivas (OCO); las operaciones de ciber inteligencia, vigilancia y reconocimiento (IVR); y las operaciones cibernéticas de preparación operacional del ambiente.

En el área ciber, se definen cuatro tipos de operaciones:

Defensivas: Su objetivo es mantener la libertad de acción, evitando que se vea afectada la confidencialidad, integridad o disponibilidad de la información. “Son medidas activas y pasivas tomadas para preservar la habilidad de usar el espacio cibernético” (Vergara & Trama, 2017, pág. 49)

Su lineamiento es comprender acciones para proteger, monitorizar, analizar, detectar y responder a actividades no autorizadas en sistemas de información propios.

Las operaciones defensivas están clasificadas en dos tipos:

- Las realizadas permanentemente en los sistemas del Ministerio de
- Defensa (medidas de protección).
- Las realizadas con misión de proteger un sistema específico contra una amenaza definida.

Explotación: Su objetivo es la obtención de información de los sistemas adversarios designados como objetivo susceptibles a ser atacados. Es primordial la obtención de información del origen de ataques a sistemas propios.

Se identifican tres tipos de operaciones de explotación:

- Inteligencia de fuentes abiertas (OSINT): información DNS, Google hacking, sitios web y metadatos de archivos.
- Reconocimiento pasivo: enumeración de dispositivos, escaneo de puertos activos (protocolos y servicios), identificación de SO,s y evaluación de vulnerabilidades.
- Amenaza Persistente Avanzada (APT): exfiltración constante de información del objetivo mediante la penetración en sus sistemas (García, 2018).

Ofensivas: Son las acciones realizadas en el ciberespacio para degradar, interrumpir, denegar o destruir sistemas de información o la propia información que estos almacenan**.** Son actividades que proyectan el poder para lograr objetivos militares en o a través del espacio cibernético (Vergara & Trama, 2017, pág. 49).

Deben estar sincronizadas con acciones de los otros dominios para alcanzar los objetivos militares asignados; y requieren previamente de operaciones de explotación para la obtención de información.

Vigilancia y reconocimiento: “Las operaciones de ciberinteligencia, vigilancia y reconocimiento (cyber IVR) comprenden actividades en el espacio cibernético para reunir inteligencia activa de los sistemas del blanco y del adversario requeridos para apoyar las operaciones militares” (Vergara & Trama, 2017, pág. 50).. Conjunto de acciones orientadas a la obtención, análisis y aprovechamiento de información sobre las capacidades ciber del adversario (Santos, 2016)

“La “Dotrina Militar de Defesa Cibernética” de Brasil, al igual que la de España y Francia clasifican a las operaciones cibernéticas solamente en ofensivas, de protección y de exploración” (Vergara & Trama, 2017, pág. 51).

Amenazas cibernética.- Una amenaza cibernética es cualquier cosa que tenga el potencial de dañar cualquier parte de un sistema informático o red: todo, desde archivos individuales hasta entornos completos. Los ejemplos de amenazas cibernéticas incluyen malware, ransomware, ataques DoS y ataques de phishing (Acronic, 2020).

La naturaleza de las amenazas está determinada por sus motivaciones e intenciones. Por ello, de acuerdo con el “Global Internet Security Threat Report” publicado en abril de 2009 por Sysmantec, se pueden mencionar al ciberespionaje, las ciberoperaciones militares, el ciberterrorismo, y al cibercrimen como las principales amenazas a la seguridad de los Estados, perpetradas por la ciberdelincuencia (Santos, 2016).

Más del 80 por ciento de los actos de ciberdelincuencia se estima que tienen su origen en alguna forma de organización criminal, como el cibercrimen originado en el mercado negro que han establecido ciclos de creación de malware, equipo infección, gestión de botnets, información datos financieros personales, venta de datos y recuperación de información financiera. Otras amenazas que se desembocan en el tipo ciber son:

- Ciberespionaje

- Cibersabotaje de servicios e infraestructuras críticas,
- Ciberterrorismo,
- Ciberoperaciones de información y propaganda,
- Ciberdelincuencia
- Ciberguerra,
- Hacktivismo,
- Cibercrimen.

Estas amenazas pueden ser aprovechadas por múltiples actores, no fácilmente identificables, y generarse diversos tipos de ataques, entre los cuales se enumera:

1. Colección de información clasificada.
2. Vandalismo cibernético (por ejemplo, denegación de servicio, hacking, entre otros).
3. Guerra sicológica en el ciberespacio.
4. Ataques distribuidos para la denegación de servicio (“redes zombis”).
5. Ataques contra equipos electrónicos.
6. Ataques contra infraestructuras críticas (redes SCADA): energía, agua, comunicaciones, entre otros.
7. Amenaza persistente avanzada (“Advance Persistent Threat”-APT), es un tipo de ataque que permite el ciberespionaje (Alvarez, 2021).

Estas amenazas están apoyadas por organizaciones formales o informales no legales ni ligadas a fronteras nacionales, están supuestas a ejercer hacktivismo o acciones terroristas haciendo uso del ciberespacio, su objetivo es: ganancias económicas y la prestación de servicios a estados o actores transnacionales con el propósito de desestabilizar gobiernos (Vergara & Trama, 2017).

Si bien se aplican varias teorías criminológicas diferentes, el hecho de que el delito cibernético representa un nuevo y distintivo formato de crimen, crea desafíos para predecir desarrollos y para su prevención, mediante la aplicación de las teorías generales del delito.

Ciberespacio. - “El termino ciberespacio desde la década de los años 1990 inicio con su conversión a sinónimo de internet y posteriormente de la WWW, en específico entre los círculos académicos y grupos de activistas” (Arreola, 2016, pág. 117)

Data de la segunda mitad del siglo XX, y fue presentado por Alvin Toffler en su libro Future Shock (1973) popularizado por Gibson (2007) en su obra Neuromancer de 1984 y dice que:

> El ciberespacio. Una alucinación consensual experimentada diariamente por billones de legítimos operadores, en todas las naciones, por niños a quienes se enseña altos conceptos matemáticos... Una representación gráfica de la información abstraída de los bancos de todos los ordenadores del sistema humano. Una complejidad inimaginable. Líneas de luz dispuestas en el no-espacio de la mente, agrupaciones y constelaciones de datos [...] el propio terreno delo virtual, donde todos los medios se juntan (fluyen) y nos rodean (Citado en Arreola, 2016, pág.117)

Esta definición abarca dos puntos importantes: la conexión global en la red y la representación gráfica de los bancos de información, que llevan a la conformación de una realidad virtual que todo conecta. En definitiva es un mundo paralelo creado y sostenido por las computadoras y las líneas de comunicación, es invisible, con alta dependencia de la vida en la sociedad (Arreola, 2016).

Para Feliú Ortega

> El espacio cibernético es mucho más que Internet, más que los mismos sistemas y equipos, el hardware y el software e incluso que los propios usuarios, es un nuevo espacio, con sus propias leyes físicas que, a diferencia de los demás espacios, ha sido creado por el hombre para su servicio (Feliú, 2012, págs. 42-43).

Para la República Federativa del Brasil:

> El Ciberespacio es una de las cinco áreas operacionales que penetra todas las demás las cuales son: la tierra, el mar, aire y espacio, que son interdependientes. Las actividades en el ciberespacio pueden crear libertad de acción para las actividades en otras áreas, así como actividades en otros dominios y también crean

> efectos dentro y a través del ciberespacio. El objetivo central de la integración de dominios es la capacidad de aprovechar las capacidades de múltiples dominios para crear efectos únicos y a menudo decisivos (Ministerio da Defensa, pág. 18)

Este concepto se relaciona a lo dicho en epígrafes anteriores que, antes de la aparición de las computadoras y el internet, los ámbitos de la guerra se dividían en cuatro: terrestre, marítimo, aéreo y espacial. Sin embargo, “el uso de los satélites llevó a la llamada “Guerra de las Galaxias” con las tecnologías de la información apareció el fenómeno de la ciberguerra. Esta situación permite considerar ahora un quinto dominio de la guerra, el ciberespacio” (Arreola, 2016, pág. 113).

Con el tiempo, el ciberespacio ha crecido en importancia dentro de las estratégicas de seguridad nacional de los Estados que cada vez más dependen de la interacción con la red para sus actividades no sólo comerciales, académicas, financieras sino también de defensa y ataque.

Como puntos vulnerables están las infraestructura más crítica (IC) que depende de Tecnologías de la información (TI) y tecnología utilizado para controlar y monitorear la infraestructura, dispositivos y procesos conocidos como Operacionales Tecnología (OT). Hay una clara dependencia sobre Información y Comunicación Tecnologías (TIC), por lo tanto los ciberataques son comunes.

La IC puede ser definida como el conjunto de activos, sistemas y redes (tanto físicas como virtuales) tan esenciales que su incapacitación o destrucción puede tener un efecto debilitante en la seguridad nacional del Estado, estabilidad económica, salud pública y seguridad.

El Plan Nacional de Protección de Infraestructuras Críticas las define como: “Aquellas instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya interrupción o destrucción tendría un impacto mayor en la salud, la seguridad o el bienestar económico de los ciudadanos o en el eficaz funcionamiento de las instituciones del Estado y de las Administraciones Públicas”.

Para alcanzar un Ecuador Digital Ciberseguro que garantice el Estado de Derecho, proteja los servicios e infraestructuras críticas del Estado y de seguridad a la población en el ciberespacio, el Gobierno trazó su línea de acción asentada en 7 pilares:

> I) Gobernanza de ciberseguridad; 2) Sistemas de información y gestión de incidentes; 3) Protección de servicios e infraestructuras críticas digitales; 4) Soberanía y defensa; 5) Seguridad pública y ciudadana; 6) Diplomacia en el ciberespacio y cooperación internacional; 7) Cultura y educación de ciberseguridad (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2021, pág. 2).

Los efectos de un ciberataque pueden variar de un interrupción temporal del servicio a acciones que tendría el mismo efecto disruptivo que un ataque cinético. Ataques en y a través ciberespacio son escalables y pueden ser el medio de ataque preferido tanto por el estado como por actores no estatales que deseen interferir movilidad militar en tiempos de paz o de guerra (Beckvard & Zotz, 2021).

Todos los conflictos políticos y militares tienen ahora una dimensión cibernética, cuyo tamaño e impacto son difícil de predecir. Los expertos en seguridad nacional deben reconocer ahora que los verdaderos políticos y los objetivos militares se pueden ganar o perder en el ciberespacio. La globalización e internet han ayudado a los servicios de inteligencia extranjeros y a los terroristas como a cualquier otra parte de la sociedad a involucrarse en el ciberespacio a través de las comunicaciones, recaudación de fondos, relaciones públicas y la recopilación de información, todos apoyados por las tecnologías de red.

Ciberespionaje y cibersabotaje. - Ciberespionaje es el entorno complejo resultante de la interacción entre las personas, el software y los servicios de Internet por medio de dispositivos tecnológicos conectados a redes, las cuales no existen en ningún tipo de forma física (Asamblea Nacional, 2021). Mientras que cibersabotaje busca dañar la reputación de una organización y por ende su funcionamiento (Abc tecnología, 2013)..

El objetivo de estos ataques es que los Estados tratan de sustraer información para mejorar su posición estratégica, económica y política o innovadora, lo que se llama

“espionaje”**.** Al mismo tiempo los ciberdelincuentes tratan de influir en la opinión pública de los países atacados o interrumpir el normal funcionamiento de los servicios esenciales.

El asombroso logro del delito cibernético y el espionaje cibernético o ciberespionaje, a los que las fuerzas del orden y la contrainteligencia ha encontrado poca respuesta, en primera instancia, insinúa que los ataques cibernéticos más serios en las infraestructuras críticas son sólo cuestión de tiempo. Aun así, los planificadores de la seguridad nacional deberían abordar todas las amenazas con método y objetividad. A medida que crecer la dependencia de las TI, los gobiernos deben hacer inversiones proporcionales en seguridad de red, incidente respuesta, capacitación técnica y colaboración internacional (Geers, 2019).

La amenaza más utilizada para el ciberespionaje es el Phishing, la que ha aumentado en un 85% desde el año 2011. Corea del Norte es quien más la ha utilizado seguido de China e Irán, también Rusia.

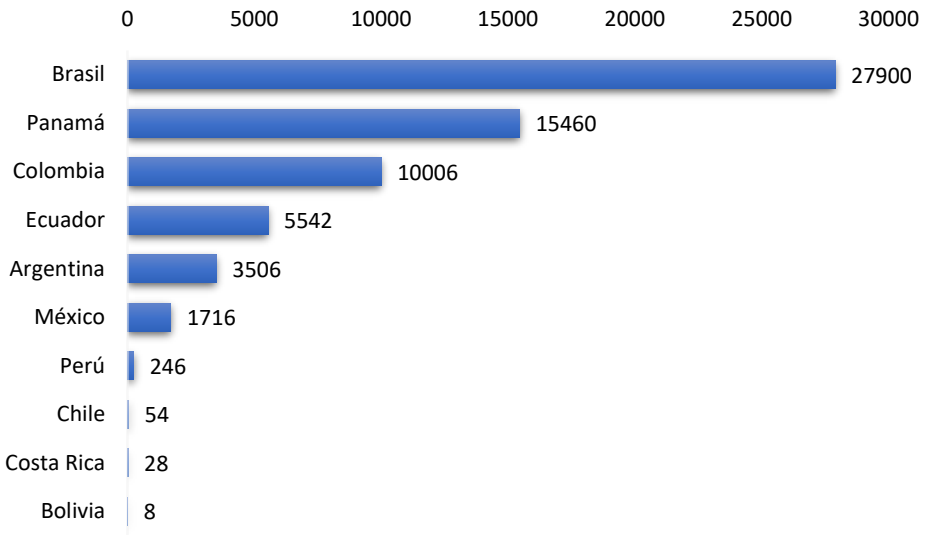
El 96% de estos ataques se utilizan para funciones de Inteligencia y la más frecuente es la técnica de “spear phishing”, por correo electrónico. Donde obtienen información personal y sobre todo bancaria. Sin embargo, el protagonista principal sigue siendo el Ransomware, cuyo objetivo es secuestrar la información a cambio de recompensas en bitcoin.

Latinoamérica es la región más expuesta a ciberespionaje, afectando a entidades militares, diplomáticas y gubernamentales. Los países más afectados son: Brasil, Colombia, Venezuela y Ecuador desde 2010. La empresa Kaspersky Lab descubrió el virus troyano que lo llamó “Machete” cuyos ataques han seguido hasta la fecha, influyendo en su ciberdelincuencia: embajadas, fuerzas militares, gobiernos, fuerzas del orden etc.

Según Akamai Thechnologies (2019) se demuestra los ciberataques en Latinoamérica durante el año 2018 (figura 2)

Figura 2

Ciberataques a web gubernamentales en Latinoamérica



Fundamentación Legal

Constitución de la República del Ecuador

Art. 158.- Las Fuerzas Armadas y la Policía Nacional son instituciones de protección de los derechos, libertades y garantías de los ciudadanos.

Las Fuerzas Armadas tienen como misión fundamental la defensa de la soberanía y la integridad territorial (Asamble Nacional Constituyente, 2008).

La obligatoriedad de la Policía Nacional y de las Fuerzas Armadas por la seguridad y soberanía territorial, se convierte en su misión y deber, incluyendo todos las dimensiones; aire, tierra, mar, ciberespacio y espacio ultraterrestre.

Política de Defensa Nacional Libro Blanco 2018

Las Fuerzas Armadas ejecutan operaciones militares en cumplimiento de su misión fundamental establecida en la Constitución, como es la defensa de la soberanía e integridad territorial en el espacio continental, insular, aéreo, marítimo, ulterior y ciberespacio, acciones que se llevan a cabo con los medios y capacidades existentes; complementariamente, contribuyen a la seguridad integral y al desarrollo nacional (Ministerio de Defensa, 2018).

Política de Ciberseguridad

Publicada el 23 de junio de 2021 según Acuerdo Ministerial 006-2021 expone:

Art. 2.- El objetivo de la presente política es construir y fortalecer las capacidades nacionales que permitan garantizar el ejercicio de los derechos y libertades de la población y la protección de los bienes jurídicos del Estado en el ciberespacio. La política establece directrices que buscan afianzar un ciberespacio seguro para contribuir al desarrollo social, económico y humano del país, así como a la creación de una confianza digital que favorece el intercambio de información y, en consecuencia, de bienes y servicios en línea (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2021, pág. 4).

Para asegurar la eficacia de la Política de Ciberseguridad promueve trabajar en siete pilares:

1. Gobernanza de la ciberseguridad
2. Sistemas de información y gestión de incidentes
3. Protección de la infraestructura crítica digital y servicios esenciales
4. Soberanía y defensa
5. Seguridad pública y ciudadana
6. Diplomacia en el ciberespacio y cooperación internacional
7. Cultura y educación de la ciberseguridad

Código Orgánico Integral Penal (COIP)

A partir del 2014 el COIP se incluyen artículos relacionados con la seguridad de los activos de los sistemas de información y comunicación. Específicamente en los artículos:

- Artículo 229.- Revelación ilegal de base de datos
- Artículo 230.- Interpretación ilegal de datos.
- Artículo 231.- Transferencia electrónica de activos patrimoniales.
- Artículo 232.- ataque a la integridad de sistemas informáticos.
- Artículo 233.- Delitos contra la información pública reservada legalmente.

- Artículo 234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones (Asamblea Nacional Constituyente, 2014).

Ley Orgánica de la Identidad y datos civiles

La presente Ley tiene por objeto garantizar el derecho a la identidad de las personas y normar y regular la gestión y el registro de los hechos y actos relativos al estado civil de las personas y su identificación.

Se referencia básicamente los Art. 1 y 3 (Núm. 4 y 6)

Ley Orgánica de Telecomunicaciones

Esta Ley tiene por objeto desarrollar, el régimen general de telecomunicaciones y del espectro radioeléctrico como sectores estratégicos del Estado que comprende las potestades de administración, regulación, control y gestión en todo el territorio nacional, bajo los principios y derechos constitucionalmente establecidos.

En primera instancia se enuncia los Art. 76, 77, 78, 79, 80, 81, 82, 83, 84, 85 y 140.

Otras normativas y planes vinculadas a la ciberseguridad se nombran a:

- Plan Nacional de Seguridad Integral 2019-2030
- Plan Específico d Defensa Nacional 2019-2030
- Plan Específico de Seguridad Pública y Ciudadana 2019-2030
- Plan Específico de Inteligencia 2019-2030
- Política Ecuador Digital

Sistemas de variables

Definición nominal

Independiente. - Situación actual del Comando de Ciberdefensa desde 2014 hasta 2022

Dependiente. - Amenazas cibernéticas y Ciberespionaje, cibersabotaje

Definición conceptual

Tabla 1

Definición conceptual

Variable		Conceptos
Independiente.	Comando de Ciberdefensa	El 12 de septiembre de 2014, por el Acuerdo Ministerial No. 281 se crea el Comando de Ciberdefensa dentro de las Fuerzas Armadas, con la misión de "proteger y defender la infraestructura crítica e información estratégica del Estado mediante operaciones de protección del espacio cibernético, acciones de prevención, disuasión, explotación y respuesta ante eventuales amenazas, riesgos e incidentes (Freire 2016).
	Operaciones militares	Son el conjunto de actividades realizadas por unidades del Ejército, en forma independiente o como parte de una fuerza mayor, con tropas y medios orgánicos o bajo cualquiera de las relaciones demando, coordinadas en tiempo y en espacio, de acuerdo con lo establecido en una directiva, plan u orden para el cumplimiento de una misión o tarea (Comando de Educación y Doctrina del Ejército, 2015)
Dependiente.	Amenazas cibernética	Una amenaza cibernética es cualquier cosa que tenga el potencial de dañar cualquier parte de un sistema informático o red: todo, desde archivos individuales hasta entornos completos. Los ejemplos de amenazas cibernéticas incluyen malware, ransomware, ataques DoS y ataques de phishing (Acronic, 2020).

Variable	Conceptos
Ciberespionaje Cibersabotaje	**Ciberespionaje:** Robo de información a empresas o instituciones e infraestructuras críticas con el fin de acceder a su información más valiosa (propiedad intelectual, desarrollos tecnológicos, estrategias de actuación, bases de datos de clientes, etc.) **Cibersabotaje:** Busca dañar la reputación de una organización y por ende su funcionamiento (Abc tecnología, 2013)..

Definición operacional

Tabla 2

Definición operacional

Variable	**Dimensión**	**Indicadores**	**Instrumento**
Variable independiente. Comando de Ciberdefensa Operaciones Militares	Político Institucional Militar	• Constitución de la República • Libro blanco de la Defensa. • Marco legal • Plan Nacional de Seguridad Integral 2019-2030 • Plan estratégico institucional	• Bibliografía. • Bibliografía. • Encuestas. • Entrevistas. • Bibliografía. • Encuestas. • Entrevistas.
Variable dependiente. Amenazas cibernéticas	Institucional	• Índice de ciberseguridad global • Equipamiento militar para el ciberespacio	• Entrevistas • Encuestas • Bibliografía • Documentos estadísticos publicados

Variable	**Dimensión**	**Indicadores**	**Instrumento**
Ciberespionaje Cibersabotaje	Tecnológico	• Índices de ciberdefensa • Índices de ciberseguridad • Índices de cibersabotaje • Índices de ciberespionaje	• Entrevistas • Encuestas • Bibliografía • Documentos estadísticos publicados

Hipótesis

H_0 A partir de la creación del Comando de Ciberdefensa hasta el 2022, el análisis de la capacidad de FF.AA. para utilizar las operaciones militares del ciberespacio no permitirá enfrentar el ciberespionaje y el cibersabotaje.

H_1 A partir de la creación del Comando de Ciberdefensa hasta el 2022, el análisis de la capacidad de FF.AA. para utilizar las operaciones militares del ciberespacio permitirá enfrentar el ciberespionaje y el cibersabotaje.

Cuadro de operacionalización de variables

Tabla 3

Operacionalización de variables

DEFINICIÓN NOMINAL	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL		
		Dimensión	**Indicadores**	**Instrumento**
INDEPENDIENTE Comando de Ciberdefensa	El 12 de septiembre de 2014, por el Acuerdo Ministerial No. 281 se crea el Comando de Ciberdefensa dentro de las Fuerzas Armadas, con la misión de "proteger y defender la infraestructura crítica e información estratégica del Estado mediante operaciones de protección del espacio cibernético, acciones de prevención, disuasión, explotación y respuesta ante eventuales amenazas, riesgos e incidentes (Freire 2016).	Político	• Constitución de la República • Libro blanco de la Defensa. • Marco legal	• Bibliografía.
		Institucional	• Plan Nacional de Seguridad Integral 2019-2030	• Bibliografía. • Encuestas. • Entrevistas.

DEFINICIÓN NOMINAL	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL		
		Dimensión	**Indicadores**	**Instrumento**
Operaciones militares	Son el conjunto de actividades realizadas por unidades del Ejército, en forma independiente o como parte de una fuerza mayor, con tropas y medios orgánicos o bajo cualquiera de las relaciones demando, coordinadas en tiempo y en espacio, de acuerdo con lo establecido en una directiva, plan u orden para el cumplimiento de una misión o tarea (Comando de Educación y Doctrina del Ejército, 2015)	Militar	• Plan estratégico institucional	• Bibliografía. • Encuestas. • Entrevistas.

DEFINICIÓN NOMINAL	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL		
		Dimensión	**Indicadores**	**Instrumento**
DEPENDIENTE Amenazas cibernéticas	Una amenaza cibernética es cualquier cosa que tenga el potencial de dañar cualquier parte de un sistema informático o red: todo, desde archivos individuales hasta entornos completos. Los ejemplos de amenazas cibernéticas incluyen malware, ransomware, ataques DoS y ataques de phishing (Acronic, 2020).	Institucional	• Índice de ciberseguridad global • Equipamiento militar para el ciberespacio	• Entrevistas • Encuestas • Bibliografía • Documentos estadísticos publicados
Ciberespionaje Cibersabotaje	**Ciberespionaje:** Robo de información a empresas o instituciones e infraestructuras críticas con el fin de acceder a su información más valiosa (propiedad intelectual, desarrollos tecnológicos, estrategias de actuación, bases de datos de clientes, etc.) **Cibersabotaje:** Busca dañar la reputación de una organización y por ende su funcionamiento (Abc tecnología, 2013)..	Tecnológico	• Índices de ciberdefensa • Índices de ciberseguridad • Índices de cibersabotaje • Índices de ciberespionaje	• Entrevistas • Encuestas • Bibliografía • Documentos estadísticos publicados

Capítulo III

Metodología

Modalidad de la investigación

Para realizar el análisis de las operaciones de Fuerzas Armadas ecuatorianas en el ciberespacio y los medios necesarios para contrarrestar el ciberespionaje y el cibersabotaje desde la creación del Comando de Ciberdefensa hasta 2022, se aplicó una modalidad de investigación documental, con enfoque cuantitativo.

Esta modalidad, se concreta en la recopilación de información de diversas fuentes: primarias y secundarias. Las primeras se relación a datos existentes que sustentan el problema, y las segundas contienen información organizada, elaborada, productos de análisis en referencia a documentos primarios (Suarez, 2018).

La información documental se define como una serie de “métodos y técnicas de búsqueda, procesamiento y almacenamiento de la información contenida en los documentos y la presentación sistemática, coherente y suficientemente argumentada” (Tancara, 210, pág. 92)

Tipos de investigación

Exploratoria

“Es la más apropiada para realizar una primera aproximación al problema porque facilita los primeros reconocimientos del problema planteado y de las posibles acciones a desarrollar” (Férnandez, 2014, pág. 31). La investigación para este trabajo se valida de los resultados exhaustivos de estudios cualitativos utilizados y la observación del caso tratado.

Descriptiva

Este tipo de investigación permite definir, clasificar y caracterizar el objeto de estudio, explica perfectamente conceptos basados en las fuentes primarias y secundarias utilizadas como soporte fidedigno de la investigación. La investigación descriptiva se efectúa cuando se desea describir, en todos sus componentes principales, una realidad. Los métodos descriptivos que se conjugan en ese trabajo son: la observación y el enfoque cuantitativo.

En el presente trabajo, la información recopilada determinó de manera documental la situación de FF.AA. en el ciberespacio, además se conceptualizó los términos involucrados, ampliando el conocimiento y relación en el tema investigativo.

Correlacional

“Tiene como propósito examinar la relación entre variables y la relación de los resultados por variable, sin llegar a confirmar la causalidad de la una sobre la otra. En otras palabras, la correlación examina asociaciones pero no relaciones causales” (Bernal, 2016, pág. 113). Las variables planteadas en esta investigación se correlacionaron con un enfoque cuantitativo lo que definió la justificación del trabajo.

Diseño de la investigación

El diseño aplicado es no experimental, realizado de manera transversal del tipo exploratorio descriptivo, realizado en un mismo tiempo. “Los objetivos del diseño transversal consisten en determinar las diferentes características y el desarrollo del diseño de estudio observacional, en un momento dado, en una sola medición retrospectiva” (Naghi, 2015, pág. 67) .

Para este caso la investigación se realizó con enfoque cuantitativo, usando como herramienta la encuesta descriptiva.

Población y muestra

Población

Población. Es el conjunto de personas u objetos de los que se desea conocer algo en una investigación. "El universo o población puede estar constituido por personas, animales, registros médicos, los nacimientos, las muestras de laboratorio, los accidentes viales entre otros” (López, 2004, pág. 69).

La población en referencia estuvo conformada de la siguiente manera:

Oficiales del curso de Estado Mayor de Arma	73
Oficiales del curso de Estado Mayor de Servicios	40
Oficiales del curso Avanzado de Arma y Servicios	39

TOTAL	152

Muestra

Es un subconjunto o parte del universo o población en que se llevará a cabo la investigación. Hay procedimientos para obtener la cantidad de los componentes de la muestra como fórmulas (López, 2004, pág. 69). En este trabajo se aplicó la siguiente fórmula:

$$\frac{z^2 * p * q * N}{e^2 * (N-1) + z^2 * p * q}$$

N = Universo = 152

Z= Nivel de confianza = 95%

p = Probabilidad a favor= 50%

q = Probabilidad en contra, q=(1-p) = 50%

e= Error de estimación = 1.95%

n= Tamaño de la muestra = 125

Técnicas de recolección de datos

Instrumentos

Enfoque cuantitativo. - Bajo la perspectiva cuantitativa se utilizó como instrumento confiable la encuesta descriptiva, aplicada a 125 oficiales de la Academia de Guerra del Ejército. Se aplicaron los siguientes instrumentos:

- **Encuesta. -** La técnica de la encuesta es utilizada en el método analítico, observacional y descriptivo, por lo tanto esta herramienta mantiene estas características. Este método también es denominado correlacional lo que permite establecer un control sobre la variable independiente para comprobar qué efectos producen sobre la dependiente definiendo la relación causal que existe entre ellas (Casas, Repullo, & Donado, 2003, pág. 528) .

  Utilizando una encuesta de tipo descriptivo, donde se busca crear un registro sobre las actitudes o condiciones presentes dentro de una población en un momento determinado, es decir en el momento en el que se realiza la encuesta.

- **Cuestionario:** Para este tipo de encuesta se aplica la escala de Likert como procedimientos escalares se utilizan los rangos sumativos que define de manera menos polarizada o dicotómica la respuesta a una pregunta, obteniendo además un valor ponderativo, obteniendo de forma concreta el concepto cuantitativo. En este cuestionario se adoptará algunas escalas del tipo Likert y que serán denominadas de manera ordinal. Adicionalmente se utilizará preguntas dicotómicas y de selección. (Anexo 1)

Validez y confianza

El nivel de confianza del muestro es del 95%, por lo tanto, las encuestas miden realmente las variables investigadas El cuestionario es único, utilizado exclusivamente para este trabajo investigativo, por tanto la confianza del instrumento se pudo comprobar con la sustentación teoría y documental presentada, así como de estudios previos similares.

Técnicas de análisis de datos

Para el análisis de datos se formaron tablas de frecuencias con los resultados obtenidos en las encuestas. A través del programa Excel se crearon tablas dinámicas para realizar tablas dinámicas que nos permita correlacionar las diferentes dimensiones e indicadores y obtener un resultado preciso de cada variable, justificando de esta manera el trabajo realizado y la hipótesis planteada.

Técnicas de comprobación de la hipótesis

La lógica de la hipótesis conceptual salta a la vista porque sigue el más puro sentido común. No obstante, no es posible verificar una hipótesis así formulada; para esto es preciso traducir la hipótesis conceptual a términos cuantificables, medibles y en definitiva analizables. Se trata de cuantificar, para poder comparar y comprobar la relación enunciada, de modo objetivo (Soler, 2001).

Al utilizar el enfoque cuantitativo las variables dependiente e independiente se cuantificó para utilizar el método estadístico de t student, donde se acepta la hipótesis alterna, o se rechaza la hipótesis nula, a través del valor de p.

Valor p

El valor p es una probabilidad que mide la evidencia en contra de la hipótesis nula. Un valor p más pequeño proporciona una evidencia más fuerte en contra de la hipótesis nula.

Capítulo IV

Resultados de la investigación

Análisis de resultados

Las encuestas tuvieron dos direccionamientos, medir las variables dependiente e independiente en cada una de las dimensiones.

Variable independiente:

Situación actual del Comando de Ciberdefensa desde 2014 hasta 2022

Dimensión institucional

Pregunta 1

¿Cómo calificaría usted el trabajo realizado hasta el momento por el Comando de Ciberdefensa de FF. AA

Tabla 4

Trabajo realizado por el Comando de Ciberdefensa de FF. AA – Dimensión institucional

OPCIÓN	FRECUENCIA	PORCENTAJE
Nada óptimas	25	20%
Medianamente óptimas	85	68%
Óptimas	15	12%
TOTAL	125	100%

Pregunta 2

Se cuenta con un marco legal para el pleno funcionamiento del COCIBER de FF.AA.

Tabla 5

Marco legal – Dimensión institucional

OPCIÓN	FRECUENCIA	PORCENTAJE
Nada óptimo	24	19%
Medianamente óptimo	89	71%
Óptimo	12	10%
TOTAL	125	100%

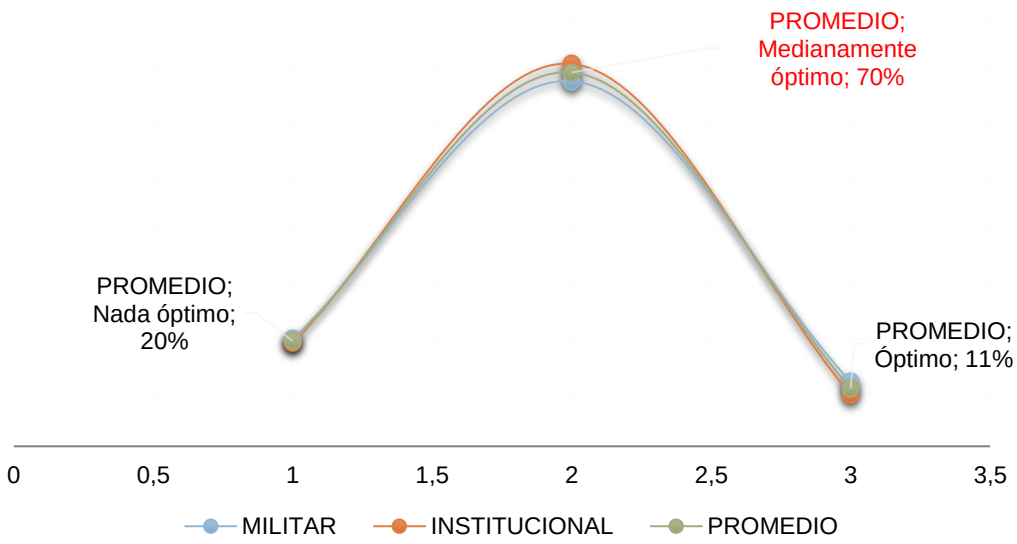
Tabla 6

Correlación dimensiones variable independiente

OPCIÓN	MILITAR	INSTITUCIONAL	PROMEDIO
Nada óptimo	20%	19%	20%
Medianamente óptimo	68%	71%	70%
Óptimo	12%	10%	11%
TOTAL	100%	100%	100%

Figura 3

Gráfico de correlación de variable independiente



El valor de la variable independiente es del 70% en la opción MEDIANAMENTE ÓTIMA. A pesar de ser un porcentaje aceptable, el nivel no se podría considerar apto, considerando que se trata de dos aspectos fundamentales para una institución, el marco legal que permita su buen funcionamiento. En este caso lo segundo es consecuencia del primero, por lo tanto, queda demostrado que el trabajo del COCIBER está limitado por un marco legal insuficiente.

Variable dependiente:

- Amenazas cibernéticas;
- Ciberespionaje y cibersabotaje

Amenazas cibernéticas - Dimensión institucional –

Pregunta 3

¿Considera usted que las FF.AA. están preparadas para hacer frente a las amenazas híbridas generadas en el espacio?

Tabla 7

Amenazas híbridas generadas en el espacio

OPCIÓN	FRECUENCIA	PORCENTAJE
Nada preparados	54	43%
Medianamente preparados	58	46%
Totalmente preparados	13	10%
TOTAL	125	100%

Pregunta 4

¿Qué tan importante es la capacitación de profesionales especializados para el control y vigilancia del ciberespacio?

Tabla 8

Capacitación de profesionales especializados

OPCIÓN	FRECUENCIA	PORCENTAJE
Poco Importante	4	3%
Importante	19	15%
Muy importante	102	82%
TOTAL	125	100%

Pregunta 5

Las amenazas híbridas alcanzan también el ciberespacio afectando las infraestructuras críticas que son responsabilidad de FF.AA.

Tabla 9

Ciberamenazas

OPCIÓN	FRECUENCIA	PORCENTAJE
Desacuerdo	5	4%
Indeciso	36	29%
Totalmente de acuerdo	84	67%
TOTAL	**125**	**100%**

Pregunta 6

En las últimas décadas las nuevas amenazas han cambiado sus lineamientos, generándose nuevos conceptos que hacen necesario revisar sus alcances para una total comprensión de estos.

Tabla 10

Nuevo conceptos

OPCIÓN	FRECUENCIA	PORCENTAJE
Nada	22%	22%
Medianamente	8%	8%
Totalmente	70%	70%
TOTAL	125	100%

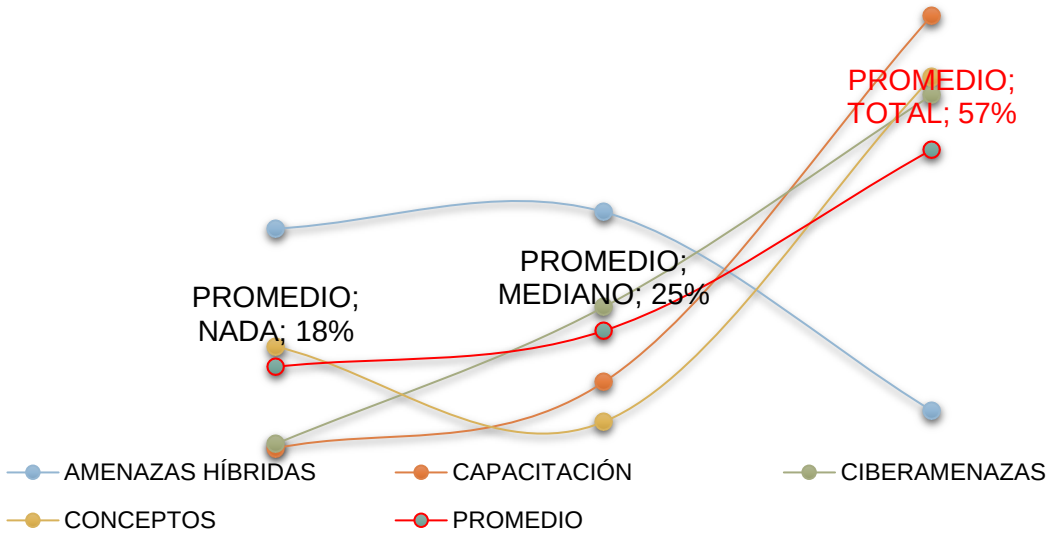
Tabla 11

Análisis amenazas cibernéticas - Dimensión institucional –

	AMENAZAS HÍBRIDAS	CAPACITACIÓN	CIBERAMENAZAS	CONCEPTOS	PROMEDIO
Nada	43%	3%	4%	22%	18%
Mediano	46%	15%	29%	8%	25%
Totalmente	10%	82%	67%	70%	57%
TOTAL	100%	100%	100%	100%	100%

Figura 4

Gráfico del análisis dimensión institucional – Amenazas cibernéticas



Los resultados de la variable dependiente amenaza cibernética donde interviene la dimensión institucional, en el promedio del 57% en el nivel TOTALMENTE de los indicadores sugeridos, determinó la necesidad de capacitación para hacer frente a las ciberamenazas que afectan a las infraestructuras críticas, responsabilidad de FF.AA. para lo que además es indispensable conocer los lineamientos y alcances de los nuevos términos que nacen de los cambios tecnológicos para una preparación correcta. Un indicador que influye de manera indecisa a este total es la percepción de preparación de FF. AA para enfrentar las amenazas híbridas en el ciberespacio, determinado por un 43% como NADA preparada; 46% MEDIANAMENTE preparada y 10% TOTALMENTE preparada.

Ciberespionaje y cibersabotaje - Dimensión tecnológica –

Pregunta 7

¿Cuenta el Ejército con equipo actualizado para el control del ciberespacio?

Tabla 12

Control del ciberespacio

OPCIÓN	FRECUENCIA	PORCENTAJE
No	110	88%
Mas o menos	0	0%
Si	15	12%

Pregunta 8

¿Qué tan importante es el equipamiento militar para el control del ciberespacio?

Tabla 13

Equipamiento militar

OPCIÓN	FRECUENCIA	PORCENTAJE
No es importante	10	8%
Importante	17	14%
Muy importante	98	78%
TOTAL	125	100%

Pregunta 9

¿En qué nivel ubicaría usted a las FF. AA ecuatorianas frente a su similares de la región en la preparación frente a las amenazas provenientes del cibersabotaje y ciberespionaje?

Tabla 14

Nivel para de FF. AA ecuatorianas enfrentar las amenazas del cibersabotaje y ciberespionaje

OPCIÓN	FRECUENCIA	PORCENTAJE
Nada óptimo	87	70%
Medianamente óptimo	29	23%
Óptimo	9	7%
TOTAL	125	100%

Pregunta 10

¿Conoce usted de las Amenazas Persistentes Avanzadas (APT)?

Tabla 15

Amenazas persistentes Avanzadas (APT)

OPC IÓN	FRECUENCIA	PORCENTAJE
No	102	82%
Mas o menos	0	0%
Si	23	18%

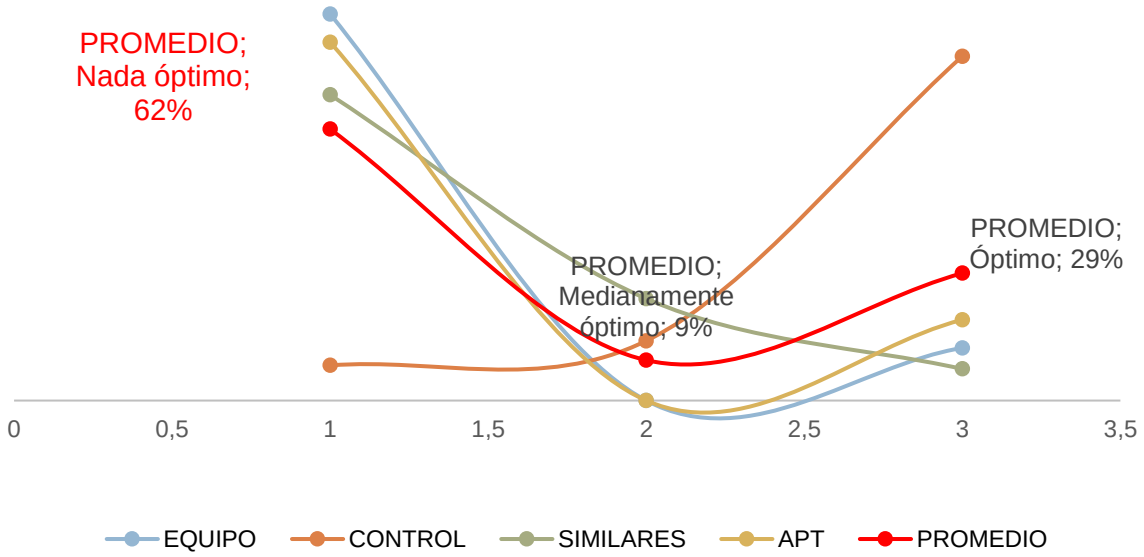
Tabla 16

Análisis Ciberespionaje y cibersabotaje - Dimensión tecnológica

	EQUIPO	CONTROL	SIMILARES	APT	PROMEDIO
Nada óptimo	88%	8%	70%	82%	62%
Medianamente óptimo	0%	14%	23%	0%	9%
Óptimo	12%	78%	7%	18%	29%
TOTAL	100%	100%	100%	100%	100%

Figura 5

Gráfico análisis ciberespionaje-cibersabotaje – Dimensión tecnológica



Los indicadores de equipo apropiado para el control y su importancia para el control del ciberespacio, ubicándose a la par de los ejércitos similares de la región, los encuestados calificaron a esta dimensión tecnológica de NADA ÓPTIMA con el 62%, MEDIANAMENTE ÓPTIMA CON EL 9% y ÓPTIMO con el 29%. El desconocimiento hacia las Amenazas Persistentes Avanzas es de NADA el 82%; POCO el 0% y SI conocen de las APT el 12%.

Estos resultados concuerdan con el análisis de la variable anterior que afirma que las FF. AA no está prepara para enfrentar las ciberamenazas, faltando equipo, capacitación adecuada, a su vez se conjuga con la variable independiente que confirmo la carencia de un marco legal pertinente que permita a las FF. AA estar a la vanguardia de la tecnología al igual que los otros países de Latinoamérica.

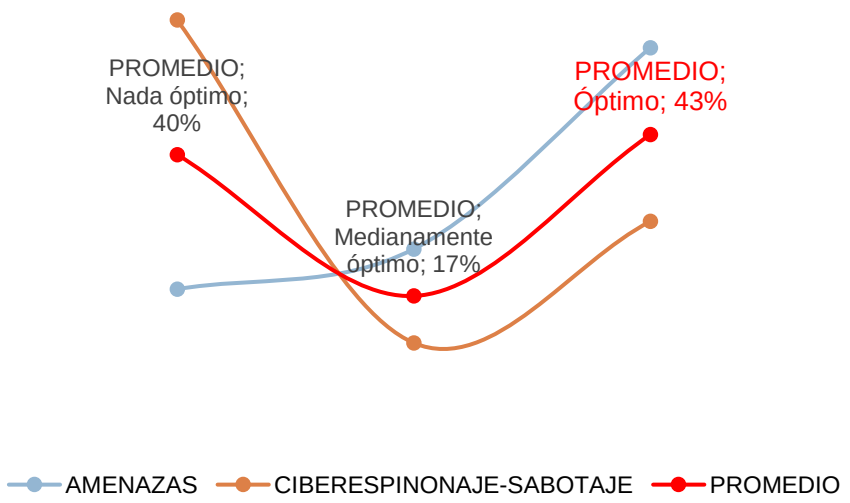
Tabla 17

Correlación dimensiones variable dependiente

	AMENAZAS	CIBERESPINONAJE-SABOTAJE	PROMEDIO
Nada óptimo	18%	62%	40%
Medianamente óptimo	25%	9%	17%
Óptimo	57%	29%	43%
TOTAL	100%	**100%**	100%

Figura 6

Correlación variable dependiente



Los resultados de la variable dependiente en la dimensión relacionada a las amenazas cibernéticas y sus indicadores le ubican en ÓTIMO con el 57%, contrario a la dimensión de ciberespionaje con el 62%, esto coloca a la variable dependiente en 43% en el nivel ÓPTIMO, NADA ÓPTIMO el 40% y MEDIANAMENTE el 17%.

El resultado no es alentador ya que para ser un valor realmente óptimo debe pasar el 65% para un cumplimento eficiente y eficaz, con un conocimiento basto y complementado con el equipo suficiente y actualizado.

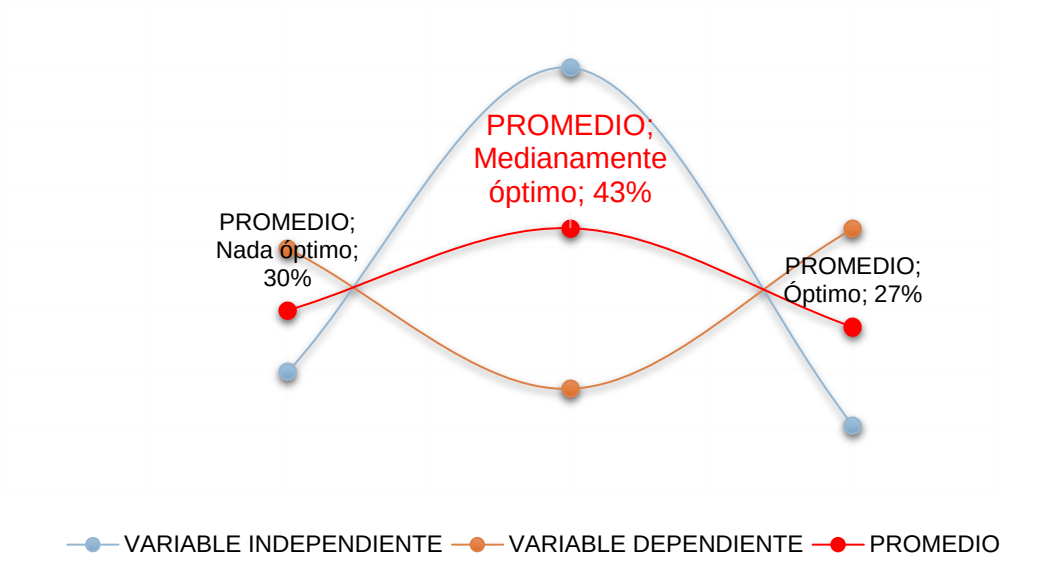
Tabla 18

Correlación entre variable dependiente e independiente

OPCIÓN	VARIABLE INDEPENDIENTE	VARIABLE DEPENDIENTE	PROMEDIO
Nada óptimo	20%	40%	30%
Medianamente óptimo	70%	17%	43%
Óptimo	11%	43%	27%
TOTAL	100%	100%	100%

Figura 7

Gráfico de correlación entre variable dependiente e independiente



Al correlacionar las dos variables: dependiente e independiente luego del análisis de resultados obtenidos a los 125 encuestados se determina que el Comando de Ciberdefensa no cumple de manera óptima sus objetivos por falta de marco legal, de igual manera, esto va acompañado de una falta equipo para el control del ciberespacio. Esta situación los entrevistados ubicaron al problema planteado en un nivel MEDIANAMENTE del 43%, NADA ÓPTIMO del 30% y ÓPTIMO 27%. Como ya se dijo estos resultados no son halagadores ya que un nivel para ser significativo en su porcentaje debe estar sobre el 65%, sobre todo en

el caso del ÓPTIMO, así se explica en el Proyecto Operaciones de FF. AA de 2016 (Comando Conjunto , 2016).

Dados estos resultados el planteamiento de estrategias para las operaciones ciberespacio que contrarresten el ciberespionaje y cibersabotaje que atentan a la Seguridad Nacional, justificando plenamente el presente trabajo.

Pregunta 11

¿El índice de ciberseguridad en Ecuador bordea los 26 puntos sobre 100, considerándose. ¿Que sería lo más importante para mejorar este índice?

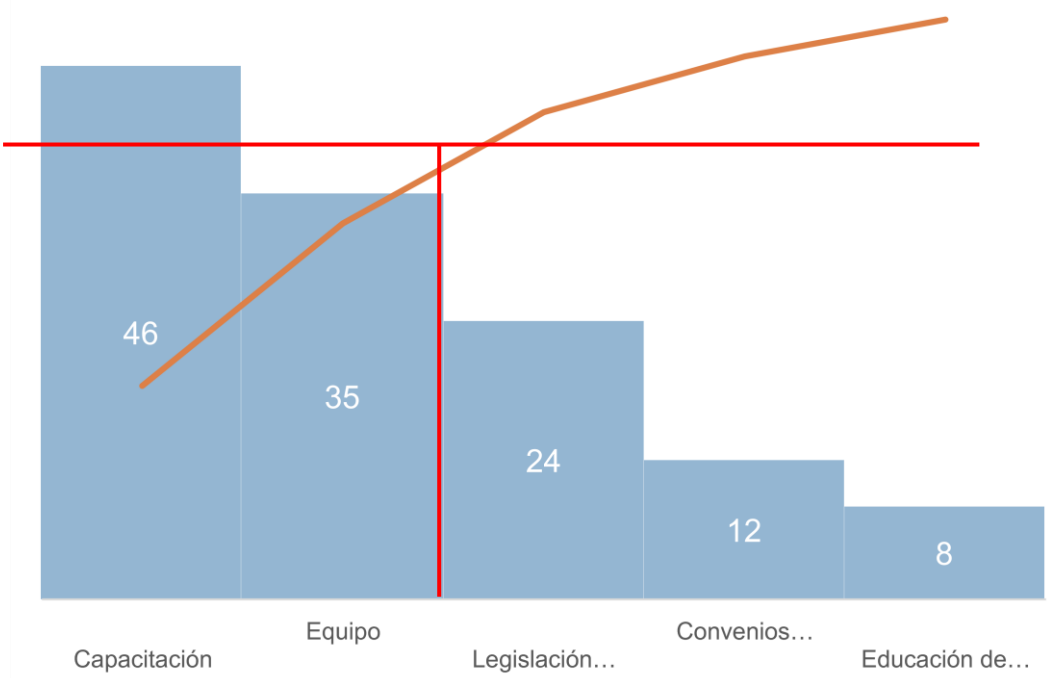
Tabla 19

Índice de ciberseguridad en Ecuador

OPCIÓN	FRECUENCIA	PORCENTAJE
Capacitación	46	37%
Convenios internacionales	12	10%
Educación de seguridad informática	8	6%
Equipo	35	28%
Legislación adecuada	24	19%
TOTAL	125	100%

Figura 8

Gráfico índice de ciberseguridad en Ecuador



Conocedores del índice de ciberseguridad en el que se ubica Ecuador, se consultó a los encuestados cuáles serían las prioridades para mejorar este índice. La respuesta rea en un 37% en la capacitación y equipo con el 28%. Esta respuesta afirma los resultados anteriores y en el diagrama de Pareto certifica la prioridad de las dos opciones planteadas.

Pregunta 12

¿Cuáles son los actores que intervienen en el ciberespacio para control del ciberespionaje y el cibersabotaje?

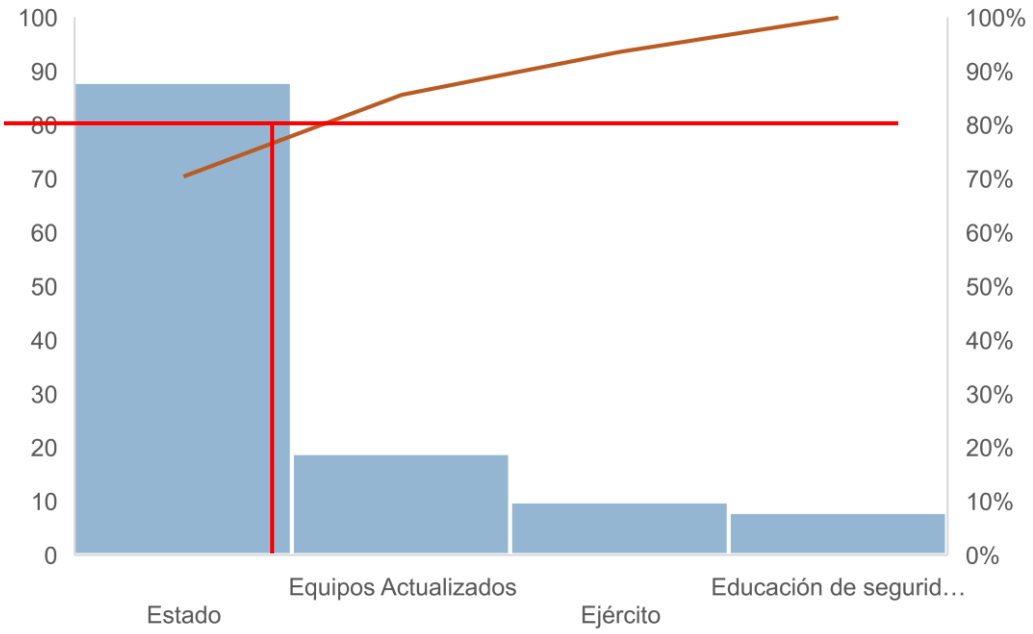
Tabla 20

Actores que intervienen en el ciberespacio

OPCIÓN	FRECUENCIA	PORCENTAJE
Educación de seguridad informática	8	6%
Ejército	10	8%
Equipos Actualizados	19	15%
Estado	88	70%
TOTAL	125	100%

Figura 9

Gráfico de los actores que intervienen en el ciberespacio



En cuanto a los actores que intervienen en el control del ciberespionaje y el cibersabotaje es directamente el Estado y este debe trabajar para que los responsables de la seguridad nacional, en este caso el Ejército cuente con equipos actualizados.

Discusión de resultados

Presentados los resultados con enfoque cuantitativo aplicado para este trabajo se puede definir que existe congruencia total en estos.

Los valores obtenidos en la variable independiente en relación al trabajo que realiza el Comando de Ciberdefensa de FF. AA está limitado por la falta de un marco legal que le permita realizar eficaz y eficientemente para el cumplimiento de sus objetivos.

En esta investigación se pudo concretar de manera fehaciente la falta de equipo del que carece FF. AA para el control del ciberespacio, así como de capacitación. Estos factores están influyendo de manera persistente, al comparar la situación del Ejército ecuatoriano con otros de la región, sobre todo con los vecinos Perú y Colombia.

Se conoce que el índice de ciberseguridad de Ecuador es de 26,3 puntos sobre 100, comprobando la alta vulnerabilidad que presenta el país ante las amenazas cibernéticas y en estas el cibersabotaje y ciberespionaje, directamente bajo la responsabilidad del Ejército.

Lo dicho está demostrado en el documento publicado por el Plan Nacional de Desarrollo y que se plantea en el objetivo 10:

Objetivo PND 10: Garantizar la soberanía nacional, integridad territorial y seguridad del Estado.

Política del PND: 10.1: Fortalecer al Estado para mantener la confidencialidad, integridad y disponibilidad de la información frente a amenazas provenientes del Ciberespacio y proteger su infraestructura crítica.

Indicador: Índice de Ciberseguridad Global (GCI)

Meta: Incrementar el índice de ciberseguridad global de 26,3 a 51,3 al 2024

Para definir esta meta se comparó con los índices de Perú con el 55,67 y Colombia con el 63,72. Los limitantes para el cumplimiento de esta meta, han sido direccionados a la falta de recursos necesarios para el fortalecimiento de la ciberseguridad (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2021).

Un estudio presentado por el Servicio de Investigación Criminal (NCIS) corrobora los resultados obtenidos en este trabajo que confirma en un 67% la responsabilidad de FF. AA frente a las amenazas híbridas concurrentes también en el ciberespacio y que afectan a las infraestructuras críticas. El estudio explica que las ciberamenazas conjugan todo tipo de crimen, volviéndose también en híbridas dentro de este espacio, con un detonante mayor, que no solo atacan en tiempos guerra.

El sorprendente logro del delito y el espionaje cibernéticos, a los que las fuerzas del orden y la contrainteligencia ha encontrado poca respuesta, insinúa que los ataques cibernéticos más serios en las infraestructuras críticas son sólo cuestión de tiempo. Aun así, los planificadores de la seguridad nacional deberían abordar todas las amenazas con método y objetividad (Geer, 2019).

Un concepto poco conocido que en este análisis demostró en un 82% su desconocimiento total es el de las Amenazas Persistentes Avanzadas (APT), cuya intervención es únicamente el ciberespacio. Estas han sido detectadas desde 2004 y en los últimos años el centro de sus ataques han sido los Parlamentos de Noruega, Alemania, Estados Unidos y otros. Las acciones primordiales de los grupos APT en el ámbito militar son el ciberespionaje y el ciberataque. Con el fin de extorsionar los ataques provocados por actores estatales y no estatales son disruptivos, aplicando la extorsión a través de la publicación de información confidencial.

Con esto se puede demostrar que falta capacitación para actualizar los múltiples conceptos que ha consecuencia de los cambios y avances tecnológicos han surgido. Esta premisa se comprueba con un 70% al afirmar los encuestados que los lineamientos de las nuevas amenazas han generado nuevos conceptos que hacen necesario revisar su alcance para su total comprensión análisis.

Un indicador que demuestra la descompensación de FF. AA para enfrentar el cibersabotaje y ciberespionaje es la falta de equipo tecnológico. Los encuestados en un 88% opinaron que el Ejército no cuenta con el equipo adecuado. Sobre este particular Puime (2019) opina que:

En primer lugar un sistema nacional de seguridad y respuesta para el ciberespacio. Este sistema debería complementarse con un programa continuo de reducción de amenazas y vulnerabilidades. Además, según aparecen tecnologías nuevas, se identifican vulnerabilidades nuevas, de modo que la normativa debe ser genérica y revisarse cíclicamente (pág. 49).

Para conseguir esto es indispensable un equipo modernizado defensivo, que permita identificar el ataque y de pararlo para mitigar sus efectos. Personal bien capacitado de manera permanente y la obtención de sistemas de información y de inteligencia.

Lo expuesto queda demostrado la importancia de plantear estrategias para las operaciones del ciberespacio que contrarresten el ciberespionaje, cibersabotaje atentando a la seguridad nacional.

Comprobación de la hipótesis

Una vez cuantificada la hipótesis a través de las variables que le conforman se aplicó el análisis estadístico de t sutend, cuyos resultados determinaron la aceptación de la hipótesis alterna:

H_0 A partir de la creación del Comando de Ciberdefensa hasta el 2022, el análisis de la capacidad de FF.AA. para utilizar las operaciones militares del ciberespacio no permitirá enfrentar el ciberespionaje y el cibersabotaje.

H_1 A partir de la creación del Comando de Ciberdefensa hasta el 2022, el análisis de la capacidad de FF.AA. para utilizar las operaciones militares del ciberespacio permitirá enfrentar el ciberespionaje y el cibersabotaje.

Si el valor de p es menor a 0.05 se debe aceptar la hipótesis nula

Si el valor de p es mayor a 0.05 se debe rechazar la hipótesis nula y aceptar la alterna

Tabla 21

Prueba t studen

Prueba t para medias de dos muestras emparejadas

	VARIABLE INDEPENDIENTE	**VARIABLE DEPENDIENTE**
Media	0.3333	0.3329
Varianza	0.1006	0.0205
Observaciones	3.0000	3.0000
Grados de libertad	2.0000	
Estadístico t	0.0016	
P(T<=t) una cola	0.4994	
Valor crítico de t (una cola)	2.9200	
P(T<=t) dos colas	0.9989	
Valor crítico de t (dos colas)	4.3027	

Utilizando el programa Minitab para análisis estadísticos se obtuvo un valor de p de 0.999 superior a la significancia utilizada de 0.05, por lo tanto la hipótesis aceptada es la alterna que dice:

H_1 A partir de la creación del Comando de Ciberdefensa hasta el 2022, el análisis de la capacidad de FF.AA. para utilizar las operaciones militares del ciberespacio permitirá enfrentar el ciberespionaje y el cibersabotaje.

Capítulo V

Propuesta

Datos informativos

Título

Análisis de las operaciones de Fuerzas Armadas ecuatorianas en el ciberespacio y los medios necesarios para contrarrestar el ciberespionaje y el cibersabotaje desde la creación del Comando de Ciberdefensa hasta el 2022.

Institución

Fuerzas Armadas del Ecuador

Beneficiarios

Directos. -

El primer beneficiario de este trabajo investigativo son las Fuerzas Armadas del Ecuador, permitiendo el planteamiento de estrategias para las operaciones del ciberespacio que contrarresten el ciberespionaje, cibersabotaje que atentan a la seguridad nacional.

Indirectos. –

Todas las instituciones e infraestructuras críticas que están bajo el resguardo de Fuerzas Armadas, cuyo fin es mantener la seguridad y defensa en todos las dimensiones de su entorno.

Ubicación

Distrito Metropolitano de Quito

Antecedentes de la propuesta

El dominio ciberespacial es un dominio global virtual, compuesto de redes interconectadas como por redes independientes. Para el funcionamiento de estas redes la interoperabilidad es fundamental, evitando que esta interoperabilidad sea alterada con ataques provenientes de otras redes ilegales o criminales. Esta interconectividad dentro del ciberespacio y la dependencia de tecnología similar requiere un enfoque integral tanto a nivel nacional como internacional. los actores militares, civiles, públicos y privados no

presentan un espacio definido en el ciberespacio, por lo que es necesario la cooperación entre todas las partes intervinientes.

Para el sector militar específicamente, las operaciones de ciberseguridad están conformadas por un conjunto de medidas y acciones enfocadas a que las redes y sistemas operen con seguridad preventiva, de protección y de apoyo a la recuperación (Centro Criptológico Nacional, 2012). Están encaminadas a la defensa, vigilancia y reconocimiento y a las acciones ofensivas contra agentes hostiles que afectan a la integridad y seguridad cibernética, pudiendo “fracasar cuando hay un nivel inadecuado de concienciación y educación sobre seguridad cibernética” (Organización del Tratado del Atlántico Norte, 2018).

Con este antecedente la OTAN recomienda que la estrategia para las operaciones militares en el ciberespacio debe orientarse a: un enfoque integral, al fortalecimiento de la defensa cibernética, desarrollar la capacidad militar con operaciones propiamente cibernéticas, incluyendo equipo y tecnología apropiada, apoyarse en las operaciones de inteligencia en el ciberespacio, fortalecer el conocimiento, la innovación, capacitación de personal; y el refuerzo nacional e internacional con el fin de operar conjuntamente (Ministerio de Defensa - Países Bajos, 2020).

Desplegando lo expuesto, para las FF.AA. el enfoque integral radica en la posibilidad de respaldar y reforzar las capacidades operativas en todos los dominios, por lo tanto, la estrategia para las operaciones en el ciberespacio debe generar, fuerza, apoyo operativo, sostenimiento, tanto de manera independiente, dentro de la doctrina y misión militar, como con el aporte civil.

Para el fortalecimiento de la defensa cibernética, la prioridad debe residir en la protección de la información y el intercambio de información. Además, los sistemas deben ser resistentes al poder responder rápidamente a los ataques y adaptarse para seguir funcionando. Las capacidades cibernéticas defensivas disponibles deben ser capaces de proteger la infraestructura de TI de la organización de Defensa, así como los sistemas de armas y sensores que utiliza (Ministerio de Defensa - Países Bajos, 2020).

Una capacidad cibernética ofensiva puede ser un multiplicador de fuerza y, por lo tanto, aumentar la efectividad de las FF. AA. La intervención de las operaciones de inteligencia aumenta la seguridad de la defensa, para influir o inhabilitar las acciones del oponente. Las operaciones deben disponer de los conocimientos y capacidades suficientes para poder realizar operaciones ofensivas en el ciberespacio, con el fin de realizar una defensa eficaz y operaciones de apoyo.

En cuanto a las operaciones de inteligencia es indispensable identificar los ataques e intentos de ataques en el espacio ciber es trabajo de la inteligencia cibernética, si no es posible reconocer el origen, autor y objetivos del ataque, las posibilidades de respuesta son limitadas.

Las estrategias deben incluir la urgencia de capacitación de personal, esto requiere investigación adicional sobre el impacto de los equipos cibernéticos que dispone FF.AA. para incrementar la capacidad operativa con tecnología, dentro de una marco legal y evitando la posible interrupción de los procesos ya establecidos, o en caso contrario, actualizar estos procesos para que la capacitación del personal sea integra, desarrollando el conocimiento y la experiencia del personal en el cambo cibernético.

Por último, la cooperación nacional como internacional, con socios de todos los sectores. Un aporte fundamental son las universidades y el sector privado en el área de investigación y desarrollo.

La propuesta planteada está enfocada en estos parámetros para garantizar que las FF.AA. puedan operar de manera efectiva y eficiente en el ciberespacio, sobre todo poder contrarrestar el ciberataque y el ciberespionaje.

Justificación

En el transcurso de esta investigación se evidenció que el ciberespacio es la nueva arena de interacción, cooperación y conflicto de la política global, así como de la intrusión del delito y del crimen, manejados por grupos ilegales afines a grandes y pequeñas organizaciones criminales, con fines económicos o desestabilizadores actúan en un campo difícil sino se está plenamente preparado.

Los avances tecnológicos han dado impulso para las acciones beligerantes se realicen con mayor fuerza en el ciberespacio, esto en concordancia con las operaciones militares para la defensa del ciberespacio, no ha sido homogéneo. El Estado ha presentado deficiencias marcadas, rezagando la construcción de capacidades ciber para la defensa, demostrándose en el bajo posicionamiento de Ecuador en el Índice de Ciberseguridad Global (ICG), 26%., mientras que Colombia presenta el 64% y Chile el 69%, dentro de los mejor punteados de Latinoamérica.

En el caso de FF.AA. esto se ha demostrado de manera evidente. Uno de los indicadores que conforman el ICG son las operaciones cibernéticas militares, donde este aporte para el Ejército chileno es del 100%, para el colombiano es del 67%; y para el Ejército ecuatoriano es el 66% (National Cyber Security Index, 2022).

Para fortalecer las operaciones en el ciberespacio con los medios apropiados que contrarresten el ciberespionaje y el cibersabotaje, es perentorio el planteamiento de estrategias específicas para ser practicadas en el ciberespacio.

Objetivos

Objetivo general

Plantear estrategias para las operaciones militares en el ciberespacio que contrarresten el ciberespionaje, cibersabotaje que atentan a la seguridad nacional.

Objetivos específicos

1. Identificar las amenazas y oportunidades, así como las fortalezas y debilidades de las operaciones de Fuerzas Armadas ecuatorianas en el ciberespacio.
2. Estructurar la matriz FODA que permita establecer las estrategias adecuadas a ser planteadas.
3. Plantear las estrategias esenciales para las operaciones en el ciberespacio

Fundamentación de la propuesta

Los resultados obtenidos en el transcurso de este trabajo determinaron la necesidad de plantear estrategias para las operaciones militares en el ciberespacio, considerado como

el quinto dominio donde estas operaciones deben actuar al igual que en los otros dominios, con destreza y manteniendo liderazgo en su capacidad operativa.

Estos resultados determinaron algunos puntos clave que fundamentan esta propuesta: las estrategias deben ser integradoras, el fortalecimiento de la defensa cibernética, el desarrollo de la capacidad militar cibernética, fortalecimiento de la inteligencia cibernética, la necesidad de una capacitación constante; y el fortalecimiento de la cooperación bilateral.

Estas estrategias, al igual que otras, no podrán alcanzar su propósito sino son evaluadas a través de indicadores que determinen su avance y cumplimiento, o en el caso contario aplicar correctivos para poder prevenir las amenazas en el ciberespacio.

Diseño de la propuesta

Siguiendo el diseño de esta investigación y luego de haber trabajado con un diseño transversal exploratorio descriptivo, la propuesta ha sido diseñada bajo el mismo criterio.

El enfoque cuantitativo proporcionó los resultados que definieron la capacidad de FF.AA. en el ciberespacio. A partir de esto se pudo plantear la propuesta de tipo analítico descriptivo.

Metodología para ejecutar la propuesta

Análisis FODA

Para concretar el objetivo de plantear estrategias para las operaciones militares en el ciberespacio que contrarresten el ciberespionaje, cibersabotaje que atentan a la seguridad nacional, se realizó un análisis de las amenazas y oportunidades, así como de las fortalezas y debilidades. Estructurada la matriz FODA, se procedió a sintetizar la matriz de impacto cruzado (CAME) y finalmente se validó de manera cuantitativa para definir los factores de mayor influencia.

Tabla 22

Interpretación cuantitativa de la matriz FODA

Factor Interno	Calificación	Factor Externo	Calificación
Debilidad mayor	1	Oportunidad mayor	4
Debilidad menor	2	Oportunidad menor	3
Fortaleza menor	3	Amenaza menor	2
Fortaleza mayor	4	Amenaza mayor	1

Con estas calificaciones se procedió a dar un valor ponderativo a cada factor interno y externo. La suma de estas ponderaciones determina la puntuación ponderada de cada factor y definen el diagnóstico para determinar los valores de la Matriz de Factores Externos (EFE) y la Matriz de Factores Internos (EFI).

Tabla 23

Análisis amenazas

MATRIZ DE FACTORES EXTERNOS				
FACTORES	**AMENAZAS**	**VALOR**	**CALIFICACIÓN**	**PONDERACIÓN**
Político	La Política de Estado en el campo de la ciberdefensa no es completa, falta lineamientos precisos.	2	0,09	0,18
	El nuevo Plan de Desarrollo es muy escueto en los objetivos y políticas para incrementar el índice de ciberseguridad de 26.3 a 55,67.	1	0,03	0,03
Económico	Recursos escasos para la implementación de equipos y la debida capacitación.	1	0,09	0,09
Tecnológico	Los actores ilegales cuentan con tecnología para operar en el ciberespacio.	2	0,04	0,08
	FF. AA no cuenta con equipo actualizado para actuar de manera precisa en el ciberespacio y enfrentar el ciberespionaje y el cibersabotaje.	1	0,09	0,09
Social	Aumento de ciberataques provenientes de grupos delictivos.	2	0,03	0,06
	Faltan leyes para la regulación del uso de internet y redes sociales.	2	0,09	0,18

MATRIZ DE FACTORES EXTERNOS				
Legal	Marco legal inadecuado para garantizar la intervención de FF. AA en el ciberespacio.	1	0,04	0,04
		TOTAL	0,5	0,75
		PROMEDIO	0,063	0,094

Tabla 24

Análisis de las oportunidades

	OPORTUNIDADES	VALOR	CALIFICACIÓN	PONDERACIÓN
Político	Decisión del Estado por mejorar las condiciones de la seguridad en el ciberespacio con intervención de FF.AA.	4	0,125	0,5
Tecnológico	Crecimiento Tecnológico apropiado para operaciones en el ciberespacio	4	0,125	0,5
Social	Alto nivel de confianza por la institución	4	0,125	0,5
Social	Colaboración con entidades educativas para la innovación de tecnología a través de programas I+D+i	4	0,125	0,5
		TOTAL	0,5	2
		PROMEDIO	0,125	0,50

OPORTUNIDADES	VALOR	CALIFICACIÓN	PONDERACIÓN
MATRIZ EFE	1		2,75

Tabla 25

Análisis debilidades

MATRIZ DE FACTORES INTERNOS				
FATORES	**DEBILIDADES**	**VALOR**	**CALIFICACIÓN**	**PONDERACIÓN**
Estructura organizacional	Operaciones en el ciberespacio centralizadas en el Comando de Ciberdefensa de FF.AA.	1	0,1	0,1
	Escaso personal capacitado para operaciones de inteligencia para el control de cibersabotaje y ciberespionaje.	2	0,045	0,09
Talento Humano	Inadecuada capacitación para hacer frente a las amenazas del ciberespacio.	1	0,1	0,1
	Desconocimiento de la magnitud y alcance de las nuevas amenazas híbridas del ciberespacio y Amenazas Persistentes Avanzadas.	2	0,055	0,11

MATRIZ DE FACTORES INTERNOS				
Tecnología de información y comunicación	Equipo tecnológico caduco para interceptar las amenazas del ciberespacio.	1	0,15	0,15
Finanzas	Escaso presupuesto para una actualización técnica y tecnológica constante.	1	0,05	0,05
		TOTAL	0,5	0,6
		PROMEDIO	0,083	0,100

Tabla 26

Análisis fortalezas

FACTOR	FORTALEZA	VALOR	CALIFICACIÓN	PONDERACIÓN
Planificación	Estructura jerárquica propia de las FF. AA fortalecen todas las operaciones militares	4	0,2	0,8
Talento humano	Personal de inteligencia disponible para las operaciones en el ciberespacio.	4	0,05	0,2
Procesos	Conocimiento del ciberespacio con información de primera mano al nivel político estratégico	4	0,1	0,4

Compromiso de FF. AA por mantener la seguridad en todas las dimensiones.	4	0,15	0,6
	TOTAL	0,5	2
	PROMEDIO	0,13	0,500
	MATRIZ EFI	1	2,6

Diagnóstico FODA

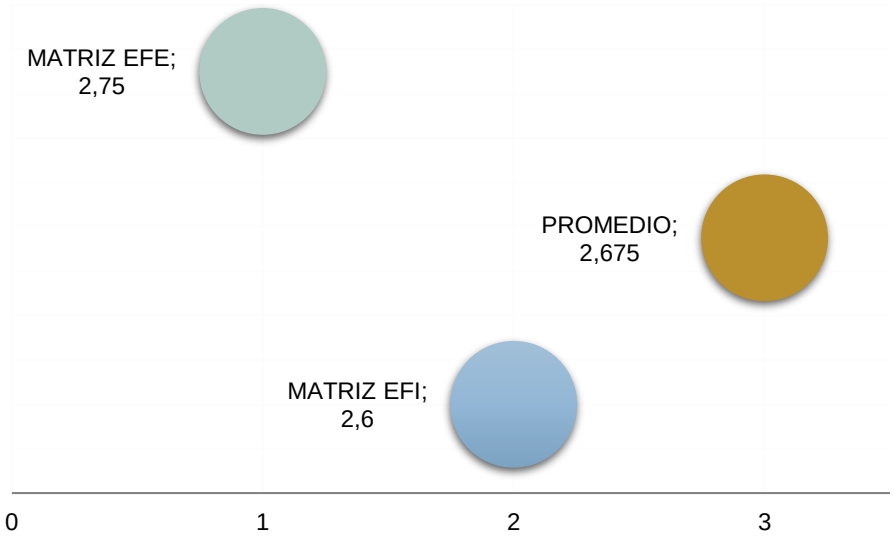
Tabla 27

Diagnóstico FODA

FACTORES EXTERNOS		FACTORES INTERNOS	
Oportunidades	2.00	Fortalezas	2.00
Amenazas	0.75	Debilidades	0.60
MATRIZ EFE	**2.75**	**MATRIZ EFI**	**2.60**

Figura 10

Gráfico del diagnóstico FODA



Para la Matriz EFE, la puntuación ponderada total más alta posible de 4.0 indica que la organización o institución analizada responde sorprendentemente bien a las oportunidades y amenazas existentes. Un 2.5 es una puntuación ponderada total promedio. Y la puntuación ponderada total más baja posible de 1.0 significa que las estrategias de la institución no están ayudando a evitar amenazas externar ni a capitalizar oportunidades (Mena, 2015).

Para la Matriz EFI, la puntuación ponderada total puede abarcar desde un mínimo de 1.0 hasta un máximo de 4.0 con una puntuación promedio de 2.5 sin importar cuántos

factores se incluyan en una matriz EFI. Las puntuaciones ponderadas totales muy inferiores a 2.5 son características de organizaciones con grandes debilidades internas, mientras que las puntuaciones muy superiores a 2.5 indican una posición interna fuerte (Mena, 2015).

En el caso de las matrices EFE y EFI analizadas, las dos con un valor de 2,75 y 2,60 respectivamente, están sobre el valor promedio lo que indica que los factores internos y externos son favorables para las operaciones en el ciberespacio, sin embargo los externos son ligeramente superiores y de mayor influencia. Los valor expuestos también reflejan que los elementos negativos: amenazas y debilidades son totalmente superables con las oportunidades y fortalezas.

El último paso es definir el promedio de las dos matrices y establecer el tipo de estrategia a plantear.

Tabla 28

Diagnóstico de matrices EFE y EFI

MATRIZ EFE	MATRIZ EFI	PROMEDIO
2,75	2,60	2,675

Figura 11

Gráfico de diagnóstico matrices EFE y EFI

El promedio de las dos matrices recae en las ESTRATEGIAS DEFENSIVAS destinadas a MANTENER las fortalezas y afrontar las amenazas.

Validación de la propuesta

Cumpliendo con el objetivo de plantear estrategias para las operaciones militares en el ciberespacio que contrarresten el ciberespionaje, cibersabotaje que atentan a la seguridad nacional y luego de seguir un proceso analítico para direccionar las estrategias de acuerdo con los resultados obtenidos se plantea las siguientes estrategias:

Propuesta

Estrategias para las operaciones militares en el ciberespacio que contrarresten el ciberespionaje, cibersabotaje que atentan a la seguridad nacional

Objetivo general: Lograr que las operaciones militares en el ciberespacio hagan uso de sistemas de información y telecomunicación seguro para prevenir, detectar y proporcionar una respuesta inmediata a las amenazas del ciberespacio.

Objetivo 1: Potencial la implantación de un marco legal nacional, coherente e integrado a las políticas del Estado, así como a todas las instituciones civiles y militares, públicas y privadas para garantizar la protección de la información, los sistemas y servicios interconectados y las redes que los soportan.

Acción 1.1. Contar con recursos técnicos y humanos para integral un sistema seguro.

Acción 1.2. Mejorar la ciberseguridad en todos los campos, difundiendo cultura de protección de información.

Acción 1.3. Colaborar con la experiencia y liderazgo de la institución para promulgar el uso seguro y responsable de la tecnología de la información y comunicación.

Acción 1.4. Promover la capacitación adecuada y constante al personal específico y destinado al manejo de información y transmisión de datos.

Objetivo 2: Garantizar que las redes, los datos y los sistemas que operan en las FF.AA. estén protegidos contra ataques cibernéticos.

Acción 2.1. Diseñar e implementar un marco legal interinstitucional que limite el uso de redes no autorizadas.

Acción 2.2. Implementar medidas de seguridad para fortalecer una red o sistema para hacerlo más robusto contra ataques.

Acción 2.3. Utilizar la experiencia institucional, capacidades e influencia únicas para lograr un cambio radical en la seguridad cibernética nacional para responder a las amenazas cibernéticas.

Acción 2.4. impulsar la capacidad de generación y desarrollo de I+D+i en el ciberespacio obteniendo productos propios, seguros y certificados.

Objetivo 3: Proteger el tráfico de Internet y telecomunicaciones contra el secuestro por parte de actores malintencionados para evitar el ciberespionaje y el cibersabotaje.

Acción 3.1. Promover la soberanía tecnológica aprovechando de las oportunidades que ofrece la transformación digital, desarrollando industria propia de sistemas de información y comunicación.

Acción 3.2. Mantener la cooperación regional y de países desarrollados para la estabilidad del ciberespacio, sobre todo en lo relacionado al ciberespionaje y cibersabotaje.

Acción 3.3. Fomentar acuerdos bilaterales y multilaterales que aporten con la capacitación de profesionales con conocimientos y habilidades explicitas para el control de las operaciones de inteligencia en el ciberespacio.

Acción 3.4. Proteger las infraestructuras críticas para garantizar el normal funcionamiento y perjuicios al país.

Objetivo 4: Incrementar las capacidades de prevención, detección, reacción, recuperación, recuperación, investigación y coordinación para hacer frente a las actividades de actores ilegales que incurren en el ciberespacio.

Acción 4.1. Mejorar las capacidades de detección y análisis de las ciberamenazas para reaccionar con tiempo ante un ataque cibernético que podría afectar a una infraestructura crítica.

Acción 4.2. Fortalecer la cooperación judicial y policial nacional e internacional a través del intercambio de información y de los canales propios de la inteligencia ciberespacial.

Acción 4.3. Desarrollar procesos de prevención y detección incluyendo procedimientos de respuesta ante situaciones de crisis, así como planes contingencia que estén apoyados en el Plan de Seguridad Integral.

Acción 4.4. Fomentar la colaboración ciudadana con información de interés militar para prevenir ataques en el campo cibernético.

Acción 4.5. Potenciar las capacidades de cibersabotaje y ciberespionaje, mejorando las operaciones de ciberinteligencia.

Objetivo 5: Implementar sistemas de información y telecomunicación seguros en las infraestructuras críticas para evitar el cibersabotaje y el ciberespionaje.

Acción 5.1. Impulsar la creación de una normativa para protección de información y transmisión de datos de las infraestructuras críticas.

Acción 5.2. Fomentar la cultura de protección de datos en todas las instituciones públicas y privadas, inclusive en sistemas personales particulares que podrían ser víctimas de un cibersabotaje.

Acción 5.3. Establecer indicadores de avances en el control y manejo de la información y realizar evaluaciones periódicas para identificar posibles entradas de espionaje o amenazas cibernéticas.

Conclusiones y Recomendaciones

Conclusiones

En el espacio cibernético las amenazas fluyen sin limitación, muchas acogidas a objetivos tradicionales pero con un amplio uso de la tecnología, aprovechando de los canales de información y transmisión de datos, han surgido las amenazas híbridas conjugadas con la transmisión digital. Estas acciones coordinadas y sincronizadas están dirigidas a atacar las vulnerabilidades de toda institución, llegando al espionaje y sabotaje con el fin de presionar económica y/o políticamente.

Aplicando el enfoque cuantitativo y utilizando el diseño transversal descriptivo, se llegó a determinar algunas falencias para el cumplimiento de los objetivos del Comando de Ciberdefensa, ubicándole en un manejo medianamente óptimo del 68%.

La correlación de las variables dependiente e independiente y los indicadores trabajados, ubican en un nivel medianamente óptimo del 43% las operaciones militares en el ciberespacio.

Los factores que aportan para este porcentaje son: la falta de equipo tecnológico, capacitación del personal, influyendo de manera constante en las operaciones militares en el ciberespacio.

Un índice que ha sido analizado en este trabajo es el Índice de Ciberseguridad Global de Ecuador que se sitúa en el 26% y en el puesto 89 de 150 países analizados. Este índice, abarca algunos indicadores entre los que se analiza las operaciones cibernéticas militares, para el Ejército ecuatoriano es del 66%, mientras que el de Chile es del 100%.

Con estos resultados y dando cumplimiento al tercer objetivo específico de este trabajo, se establece el planteamiento de estrategias para las operaciones militares en el ciberespacio que contrarresten el ciberespionaje, cibersabotaje que atentan a la seguridad nacional.

Para determinar las estrategias, se trabajó con el análisis FODA, concluyendo con las Matrices EFE y EFI. Al validar las matrices se definió que las ESTRATEGIAS OFENSIVAS son las específicas para este propósito.

El trabajo realizado, siguiendo un proceso minucioso demostró la hipótesis alterna que afirma que el análisis de la capacidad de FF. AA para utilizar las operaciones militares del ciberespacio permitirá enfrentar el ciberespionaje y el cibersabotaje.

Recomendaciones

Las FF.AA. se enfrentan a situaciones difíciles ante las amenazas híbridas cibernéticas. La tecnología, aprovechando la transferencia digital, aumentan los riesgos en los sistemas de información y transmisión de datos.

La responsabilidad de FF.AA. para la seguridad en todas las dimensiones de las infraestructuras críticas y de sus propios sistemas digitales, obliga a establecer estrategias actualizadas, integrales, direccionadas a la capacitación del personal idóneo, equipamiento, concientización en el manejo seguro de la información y de los sistemas que controlan las redes.

Se recomienda implementar estas estrategias, así como actividades para el desarrollo y evaluación de las acciones a seguir, para un control constante que permita correcciones inmediatas, logrando capacidades preventivas, proactivas y reactivas, para dar una respuesta oportuna.

Establecer programas y proyectos de I+D+i propios de FF.AA. para implementar sistemas de información y comunicación seguros. En estos se deberá mejorar la interoperabilidad interna y externa bajo normas estándares internacionales que aseguren la inviolabilidad de las redes digitales.

Bibliografía

Abc tecnología. (2013). *Estas son las diez ciberamenazas más comúnes*. Obtenido de https://www.abc.es/tecnologia/redes/20140404/abci-amenazas-ciber-201404031906.html

Acronic. (2020). *2021 en revisión: las últimas amenazas cinernéticas que surgieron cómo mantenerse protegido*. Obtenido de https://www.acronis.com/es-es/articles/latest-cyber-threats-2020/

Aguilar, J. (2021). Retos y oportunidades en materia de ciberseguridad de América Latina frente al contexto global de ciberamenazas y la seguirdad naciona y política exterior. *Instituto de Estudios Internacionales*, 169-197.

Alvarez, A. (2021). Ciberseguridad y ciberdefensa ¿Estamos preparados? *Revista ESGE*, 20-33.

Argumosa, J. (2020). Las operaciones en el ciberespacio. *Academia de las Ciencias y las Artes Militares*, 1-4.

Arreola, A. (2016). Ciberespacio, el campo de batalla de la era tecnológica. *Estudios en Seguridad y Defensa*, 109-138.

Asamble Nacional Constituyente. (2008). *Constitución de la República del Ecuador*. Obtenido de https://www.oas.org/juridico/pdfs/mesicic4_ecu_const.pdf

Asamblea Nacional. (2021). *Proyecto de Ley Orgánica de Seguridad Cibernética.* Obtenido de https://asobanca.org.ec/wp-content/uploads/2021/06/PROYECTO-DE-LEY-ORGA%CC%81NICA-DE-SEGURIDAD-CIBERNE%CC%81TICA-Asamblei%CC%81sta-Jose%CC%81-Serrano.pdf

Asamblea Nacional Constituyente. (2014). *Código Orgánico Integral Penal, COIP*. Obtenido de https://www.defensa.gob.ec/wp-content/uploads/downloads/2018/03/COIP_feb2018.pdf

Beckvard, H., & Zotz, P. (2021). Consideraciones cibernéticas para movilidad militar. *Nato Cooperative Cyber Ddefence Centre of Excellence*, 1-11.

Bernal, C. (2016). *Metdología de la Investigación.* México: Pearson Educación.

Caro, M. (2021). Alcance y ámbito de la seguridad nacional en el ciberespacio. En I. E. Estratégicos, *Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio* (págs. 49-82). Madrid: Ministerio de Defensa.

Casas, J., Repullo, J., & Donado, J. (2003). La encuesta como técnica de investigación. Elaboración de cuestionarios y tratamiento estadístico de los datos (I). *Aten Primaria, 31*(8), 527-38. Obtenido de http://www.unidaddocentemfyclaspalmas.org.es/resources/9+Aten+Primaria+2003.+La+Encuesta+I.+Custionario+y+Estadistica.pdf

Castellón, J., & López, M. (2016). Crisis y ciberespacio: hacia un modelo integral de respuesta en el Sistema de Seguridad Nacional. En I. E. Estratégicos, *Ciberseguridad: la cooepración público-privada* (págs. 65-95). Madrid: Ministerio de Defensa.

Castro, E. (2015). Estudio prospectivo de la ciberdefensa en las Fuerzas Armadas del Ecuador. *Universidad de las Fuerzas Armadas*, 1-73.

Centro Criptológico Nacional. (2012). *Operaciones en el ciberespacio*. Obtenido de https://www.ccn-cert.cni.es/pdf/documentos-publicos/xiii-jornadas-stic-ccn-cert/ponencias/4390-s16-11-02-planeamiento-operaciones-en-el-ciberespacio/file.html

Comando Conjunto . (2016). *Actualzización Proyecto Sostenimiento operacional de Fuerzas Armadas año 2012-2015 Fase II*. Obtenido de https://www.defensa.gob.ec/wp-content/uploads/downloads/2016/01/dic_15sostenimiento-operacional-de-FFAA.pdf

Comando de Educación y Doctrina del Ejército. (2015). *Manual de Conducción Militar.* Obtenido de Ejército ecuatoriano: https://www.academia.edu/34370475/EJ%C3%89RCITO_ECUATORIANO_MI3_TASE1_02_MANUAL_DE_CONDUCCI%C3%93N_MILITAR

Díaz del Río, J. (2010). La ciberseguridad en el ámbito militar. En I. E. Estratégicos, *Ciberseguridad, retos y amenazas a la seguridad nacional en el ciberespacio* (págs. 217-256). Madrid: Imprenta Ministerio de Defensa.

Domínguez, J. (2017). La ciberguerra como realidad. *Revista de Pensamiento Estratégico y Seguridad CISDE*, 18-32.

El Comercio. (2021). El Consejo de Comunicación sufrió un ataque cibernético. págs. https://www.elcomercio.com/actualidad/politica/consejo-comunicacion-sufrio-ataque-cibernetico.html.

Enriquez, C. (2012). Estrategias internacionales para el ciberespacio. En C. S. Nacional, *El ciberespacio. Nuevo escenario de confrontación* (págs. 71-116). Madrid: Imprenta del Ministerio de Defensa.

Feliu, L. (2021). La ciberseguridad y la ciberdefensa. En C. S. Nacional, *EL ciberespacio. Nuevo escenario de confrontación* (págs. 35-69). Madrid: Ministerio de Defensa.

Feliú, O. (2012). *El espacio cibernético nuevo escenario de confrontación.* Obtenido de Cuadernos del CESEDEN febrero 2012: http://www.defensa.gob.es/ceseden/Galerias/destacados/publicaciones/monografias/ficheros/126_EL_ESPACIO CIBERNÉTICO_NUEVO_

Férnandez, Á. (2014). *Investigacón y técnicas de mercado.* Madrid: ESIC Editores.

García, J. (2018). *Operaciones cibernéticas.* Obtenido de https://www.uexternado.edu.co/wp-content/uploads/2018/10/TENIENTEDENAVIOJUANGARGIA.pdf

Geer, K. (2019). La amenaza cibernética para Infraestructuras Nacionales Críticas: más allá de la teoría. *Revista de Seguridad de la Información: una perpectiva global*, 1.7.

Geers, K. (2019). La ciberamenaza a las infraestructuras críticas nacionales: más allá de la teoría. *Information Security Journal: A Global Perspective*, 1-7.

Gil, J. (2017). La integración del ciberespacio en el ámbito militar. *Grupo de estudios de Seguridad Internacional*, 1-17.

Infodefensa.com. (2021). Ecuador crea el Comando de Ciberdefensa para blindar al país ante ataques cibernético. *Infodefensa*.

Jácome, J. (2020). *CIberdensa de las Fuerzas Armadas del Ecuador para el 2021 .* Obtenido de http://world_business.espe.edu.ec/wp-content/uploads/2020/07/23.5-Ciberdefensa-en-las-Fuerzas-Armadas-del-Ecuador-para-el-2021.pdf

Kutt, A. (2021). La importancia de dominar los global commons en el siglo XXI. *Instituto Español de Estudios Estratégicos*, 1-21.

López, P. (2004). Población muestra y muestreo. *Punto Cero*, 69-75.

Mena, G. (2015). *Diseño de un modelo organizacional y propuesta de implementación. Caso UWC Ecuador*. Obtenido de http://repositorio.puce.edu.ec/bitstream/handle/22000/8983/TRABAJO%20DE%20TITULACION%20-%20GABRIELA%20MENA.pdf;sequence=1

Ministerio da Defensa. (s.f.). *Doctrina Militar de Defensa CIbernética.* Obtenido de https://bdex.eb.mil.br/jspui/bitstream/123456789/136/1/MD31_M07.pdf

Ministerio de Defensa - Países Bajos. (2020). Obtenido de La estrategia cibernética de Defensa: file:///C:/Users/Usuario/Downloads/Netherlands_2020_NDL-Cyber_StrategyEng.pdf

Ministerio de Defensa. (2018). *Política de la Defensa Nacional del Ecuador "Libro Blanco".* Quito: Instituto Geográfico Militar.

Ministerio de Defensa Nacional. (2019). *Plan Nacional de Seguridad Integral*. Obtenido de https://www.defensa.gob.ec/wp-content/uploads/downloads/2019/07/plan-matriz-web.pdf

Ministerio de Defensa Nacional del Ecuador. (2014). *Agenda Política de la Defensa 2014-2017.* Obtenido de https://www.defensa.gob.ec/wp-content/uploads/downloads/2014/06/Agenda-Politica-Defensa.pdf

Ministerio de Telecomunicaciones. (2020). *Ecuador ocupa sexto lugar en la región, según Índice de Ciberseguridad*. Obtenido de https://www.telecomunicaciones.gob.ec/ecuador-ocupa-sexto-lugar-en-la-region-segun-indice-de-ciberseguridad/

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2021). *FIcha Metodológica de metas del Plan Nacional de Desarrollo*. Obtenido de https://www.planificacion.gob.ec/wp-content/uploads/2021/09/Meta-10.1.1.pdf

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2021). *Política de Ciberseguridad.* Obtenido de Registro Oficial N° 479 Acuerdo Ministerial 006-2021: https://www.telecomunicaciones.gob.ec/wp-content/uploads/2021/06/Acuerdo-No.-006-2021-Politica-de-Ciberseguridad.pdf

Minsiterio de Defensa Nacional. (2017). *Plan Estratégico Institucional de defensa 2017-2021.* Obtenido de https://www.defensa.gob.ec/wp-content/uploads/downloads/2020/02/PEI-2017-2021.pdf

Molina, F. (2021). Geopolítica espacial y búsqueda de recursos. *Instituto Español de Estudios Estratégicos*, 1-19.

Naghi, M. (2015). *Metodología de la investigación.* México: Llimusa.

National Cyber Security Index. (2022). *Ecuador*. Obtenido de https://ncsi.ega.ee/country/ec/

Organización del Tratado del Atlántico Norte. (2018). *Marco Nacional de CIberseguridad*. Obtenido de https://ccdcoe.org/uploads/2018/10/NCSFM_0.pdf

Ponce, H. (2007). La matriz FODA: alternativa de diagnóstico y determinación de estartegias de intervención en diversas organizaciones. *Enseñanza e Investigación en Psicología*, 113-130.

Puime, J. (2019). EL Ciberespionaje y la CIberseguridad. *Dialnet*, 45-77.

Sánchez-Román, G. (2020). Amenazas Persistentes Avanzadas (APT) como medida de disuasión en el espacio. *Instituto Español de Estudios Estratégicos*, 1-14.

Santa-Bárbara, P. (2021). Geopolítica de la Luna: el amanecer de una nueva era espacial. *Instituto Español de Estudios Estratégicos*, 1-21.

Santos, C. (2016). *Oepraciones en el ciberespacio.* Obtenido de https://www.ccn-cert.cni.es/pdf/documentos-publicos/xiii-jornadas-stic-ccn-cert/ponencias/4390-s16-11-02-planeamiento-operaciones-en-el-ciberespacio/file.html

Secretaría Nacional de Planificación. (2021). *Plan de Creación de Oportunidades 2021-2025.* Quito: Secretaría Nacional de Planificación.

Soler, C. (2001). El uso de hipótesis en la investigación científica. *Elsevier, 21*(3), 172-178.

Suarez, J. (2018). *Modalidad de la Investigación*. Obtenido de https://slideplayer.es/slide/13958449/

Tancara, C. (210). La investigación documental. *Revista de Temas Sociales*, 91-114.

Toffler, A. (1973). *El "Shock" del futuro.* Barcelona: Gráficas Guada.

Torres, M. (2019). El futuro de la competencia estratégica a través del ciberespacio. *Instituto Español de Estudios Estratégicos*, 1-19.

Velázquez, J. (2013). El derecho del espacio ultraterrestre en tiempos decisivos: ¿estabilidad, monopolización o universalidad? *Anaurio Mexicano de Derecho Internacional, XIII*, 583-638.

Vergara, E., & Trama, G. (2017). *Operaciones miliatres cibernéticas.* Obtenido de https://esgcffaa.edu.ar/pdf/ESGCFFAA-2016_pdf-49.pdf

Apéndices