EL ESTADO Y LA DEFENSA DEL CIBERESPACIO

Tcrn. de E.M. Angelo Semanate Esquivel [1]
Mayo. (S.P) Luis Lenin Recalde [2]

Resumen

Ante la proliferación de amenazas cibernéticas, el Ecuador promulgó políticas y estrategias enfocadas a garantizar un ciberespacio seguro, sin embargo, la aparición de nuevas amenazas nos hace pensar si el Ecuador está realmente protegido. El presente trabajo de investigación, a través de una perspectiva literaria, pretende visualizar cómo se encuentra la ciberseguridad, ciberdefensa, la inteligencia artificial y la infraestructura crítica en el marco de la defensa del Estado ante las amenazas emergentes del ciberespacio.

Palabras clave: Ciberespacio, Ciberseguridad, Ciberdefensa, Inteligencia Artificial, Amenazas emergentes, Infraestructura crítica digital.

Abstract

Faced with the proliferation of cyber threats, Ecuador enacted policies and strategies focused on guaranteeing a safe cyberspace, however, the appearance of new threats makes us wonder if Ecuador is really protected. The present research work, through a literary perspective, aims to visualize how cybersecurity, cyberdefence, artificial intelligence and critical infrastructure are found within the framework of the defense of the State against emerging threats from cyberspace.

Keywords: Cyberspace, Cybersecurity, Cyberdefense, Artificial Intelligence, Emerging threats, Critical digital infrastructure.

[1] Academia de Guerra del Ejército - Profesor de la Academia de Guerra del Ejército - angelosemanate@gmail.com
[2] Universidad de Fuerzas Armadas - ESPE - Profesor titular del Departamento de Seguridad y Defensa - llrecalde@espe.edu.ec

DOI: https://dx.doi.org/10.24133/RCSD.VOL16.N01.2023.07
Revista Academia de Guerra del Ejército Ecuatoriano, Volumen 16. Núm. 1 abril 2023. pp. 99 - 109

Introducción

El avance tecnológico y la interconexión global permite interactuar desde cualquier parte del planeta, facilitando un acceso oportuno a la información y comunicación, pero que propicia también vulnerabilidades ante nuevas amenazas que aparecen en el ciberespacio. Nuestra hipótesis principal es verificar si la Política de Ciberseguridad Nacional del Ecuador ha fortalecido en el aseguramiento del ciberespacio.

La segunda hipótesis en verificar si el Estado ecuatoriano es vulnerable frente a las nuevas amenazas.

La tercera hipótesis es proponer una catalogación y categorización de la infraestructura critica digital (ICD) del Estado.

El presente trabajo académico inicia realizando un breve análisis de las guerras cinéticas y no cinéticas, luego examinará los enfoques de la ciberseguridad, la ciberdefensa y la inteligencia artificial (IA) en la defensa del Estado, y finalmente propondrá la categorización de la ICD del Estado.

Para cumplir con esta perspectiva académica se ha organizado esta investigación en tres bloques: primero se hace referencia a las transformaciones de la guerra, buscando establecer la evolución de las mismas en el posmodernismo; el segundo bloque estudia la ciberseguridad y la ciberdefensa en el Ecuador; en el tercer bloque se realizará el análisis de la defensa de ICD del Estado, finalmente se presentarán las conclusiones del estudio.

El desarrollo del presente trabajo se realizó aplicando la metodología de la investigación descriptiva, cimentada en la revisión sistemática de artículos científicos y la lectura de revistas relacionada a la evolución y transformación de las guerras, la ciberseguridad y la ciberdefensa el marco de la cuarta revolución industrial.

1. LAS TRANSFORMACIONES DE LA GUERRA HASTA LA ACTUALIDAD

Desde la existencia del hombre ha existido y todavía en la actualidad surgen conflictos y guerras por la posesión de recursos y la expansión territorial, conflictos que se originaron por motivos de orden étnico, religioso, político, económico y de poder. En la era moderna, las guerras se produjeron por razones de carácter comercial, geopolítico y tecnológico. En este contexto se podría establecer que una de las razones fundamentales de la atemporalidad de la guerra es sencillamente, el hecho de que los Estados posean la capacidad de administrar la violencia militar (Romero, 2008).

Bajo esta perspectiva se puede considerar que la guerra está en constante evolución, ya sea por los nuevos escenarios de confrontación, los cambios de los esquemas de pensamiento y la aparición de nuevas amenazas. Algunos autores consideran entonces que se pueden clasificar a las guerras en distintas generaciones, tal como lo describe Federico Aznar Fernández-Montesinos en su artículo "Las Generaciones de las Guerras":

> La Primera Generación estaría marcada por el desarrollo y consolidación del concepto Estado; las guerras de Segunda Generación implicarían el compromiso societario en la causa y sus epítomes serían la Revolución Francesa y las revoluciones industrial y de los transportes que posibilitaron su extensión y ampliaron el espectro de los objetivos; las guerras de Tercera Generación se fundamentan en la tecnología, y el factor que coadyuva a la definición de las de Cuarta es la globalización y el retorno al hombre (Fernández & Montesinos, 2015).

El modelo de guerra tradicional se enfoca fundamentalmente al empleo de operaciones "cinéticas" (adjetivo que significa movimiento) que se caracterizan por el uso de la fuerza letal mediante el despliegue de tropas y medios ya sean terrestres, navales o aéreos para atacar e infringir daños físicos que permitan la destrucción de los recursos, activos y fuerzas adversarias. Es decir, las guerras cinéticas se enfocan en los dominios físicos con el fin de alcanzar el debilitamiento del poder militar y económico del adversario, empleando doctrina, planes, estrategias y armas convencionales.

La evolución de las guerras en la era posmoderna, en la cual se establecen escenarios de conflictos en ambientes mucho más complejos, ambiguos, inciertos y volátiles, con amenazas híbridas, difusas y no convencionales, así como el avance vertiginoso de las tecnologías ha originado un nuevo paradigma de los conflictos, las llamadas guerras "no cinéticas" que el Instituto de Estudios, Investigación y Análisis Estratégicos la define como "el uso de herramientas informativas, psicológicas, diplomáticas, económicas, sociales y tecnológicas del arte de gobernar para lograr intereses y objetivos nacionales mediante la manipulación o el deterioro de la voluntad nacional del adversario[1]".

Entonces, las guerras no cinéticas, se caracterizan por el empleo de nuevos escenarios de conflicto: La guerra electrónica (EW), la guerra de información (IW), la ciberguerra (CW) y la guerra no cinética (NKW) que incluye el "uso de herramientas informativas, psicológicas, diplomáticas, económicas, sociales y tecnológicas del arte de gobernar para lograr intereses y objetivos nacionales ya sea consintiendo o menoscabando la voluntad nacional del adversario" (Lehto & Henselman, 2020).

En la Figura 1 se realiza una breve explicación de las diferencias entre las guerras cinéticas y las guerras no cinéticas para una mejor comprensión de los fines, métodos y medios que emplean cada una de estas.

1 Persona, grupo que compite con otro por los mismos objetivos

Figura 1
Las guerras cinéticas vs las guerras no cinéticas

2. LA CIBERSEGURIDAD Y LA CIBERDEFENSA EN EL ECUADOR

Antes de iniciar contextualizando la ciberseguridad y la ciberdefensa es importante plasmar algunos conceptos fundamentales que permitirán esclarecer de mejor forma el desarrollo de este artículo. De esta manera, se reducirá la dispersión de terminología como un elemento indispensable en el abordamiento de conceptos importantes como ciberespacio, ciberseguridad, ciberdefensa, ciberataques, operaciones multidominio, inteligencia artificial, guerra no cinética, entre otros.

2.1. El ciberespacio como nuevo escenario de confrontación

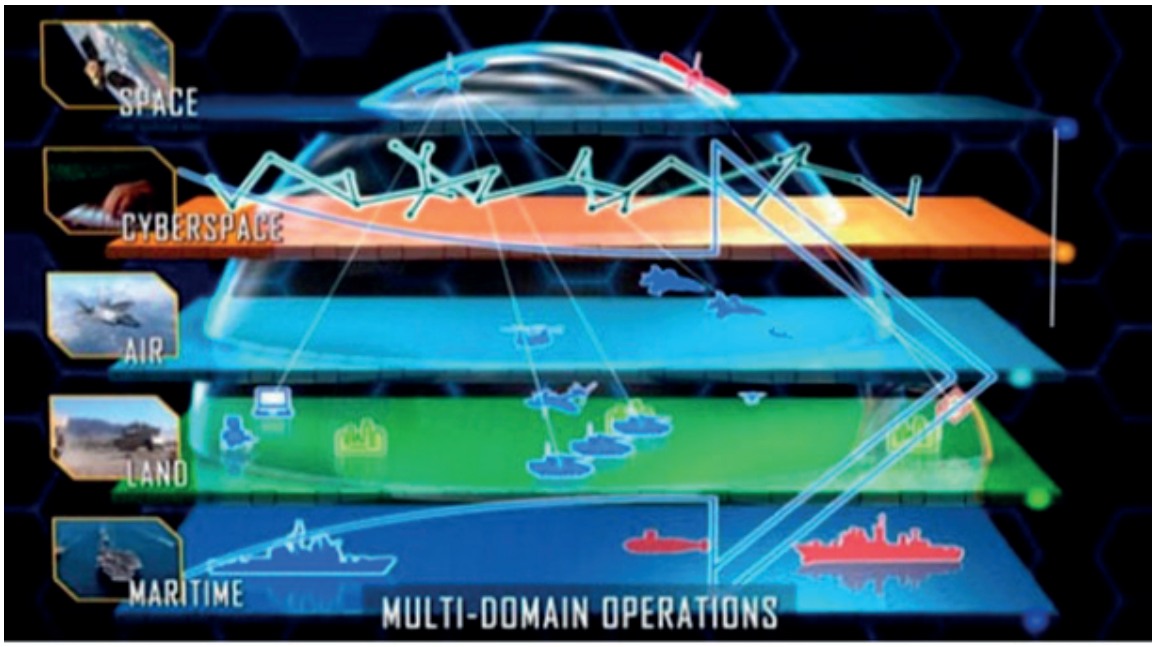
La evolución histórica del poder y el interés en la búsqueda del poder han marcado hitos importantes desde el génesis de la humanidad, pensando en darle sentido a la capacidad de decisión sobre un grupo de seres humanos. Moncayo (2022) manifiesta que el poder es el resultado de la conjugación de voluntades, propósitos y recursos orientados a lograr un fin, donde la voluntad califica y valora los medios para satisfacer necesidades y aspiraciones de una persona o grupo. En tal virtud, la lucha por el poder ha decantado en la violencia, donde el único protagonista es el ser humano, con acciones propias que tratan de imponer su voluntad en desmedro del adversario.

El poder como dominio natural ha sido innato en el ser humano, con la necesidad de mantener el control como una demostración de sometimiento, donde muchas sociedades buscan expandir su cultura imponiendo su accionar a otras menos desarrolladas, esto ha obligado a las sociedades vecinas a defenderse a través de la conformación de una fuerza beligerante que se encargue de la seguridad y la defensa de los intereses de sus miembros.

En el siglo pasado las grandes guerras protagonizadas por los países más poderosos iniciaron sus confrontaciones en tierra, después conquistaron los océanos, y en la Segunda Guerra Mundial el espacio aéreo cobró fuerza; posteriormente, en la Guerra Fría se pone de manifiesto la globalización, el desarrollo tecnológico, la puesta en órbita de satélites de gran escala, apareciendo el dominio espacial. Bien hace De la Guardia (2017) en afirmar que en la cumbre de Varsovia en 2016 se reconoció el ciberespacio como el quinto dominio para el enfrentamiento bélico, añadiendo a los tradicionales de tierra, aire, mar y espacio.

Hoy en día, la seguridad y defensa no se ven en el campo de batalla tradicional, dependen de las conexiones entre dominios, tecnologías y amenazas emergentes; las próximas guerras se visualizan en un nuevo mundo virtual. En el contexto militar, las grandes guerras se enfocan en el quinto dominio de la guerra denominado ciberespacio, pero no de manera aislada, por lo contrario, de una forma conjunta articulada y eficiente entre los cinco dominios ya mencionados; estas se denominan operaciones multidominio (OMD) que según Perkins (2018) son las fuerzas conjuntas que usarán la velocidad de reconocimiento, decisión y acción para explotar las oportunidades de superioridad en el dominio con operaciones enfocadas en la fuerza para destruir capacidades enemigas clave.

Figura 2
Operaciones multidominio



Nota. Obtenida de revista El Radar, 2020 (Gráfico del U.S Army)

El ciberespacio es un término que no puede dejarse de referenciar en este artículo, es el punto de inflexión de la seguridad y la amenaza; el ciberespacio es un término empleado por algunos escritores con diferentes apreciaciones en su conceptualización. Sin embargo, se hará una aproximación a la definición de ciberespacio, considerando que es un concepto muy amplio que muchos autores lo definen con una perspectiva diferente.

Espinosa (2021) manifiesta que el ciberespacio se ha convertido en un ámbito esencial para el funcionamiento económico y social a escala mundial, dados los beneficios asociados a la velocidad, capacidad, agilidad y eficiencia que ofrece. En tal virtud, se puede decir que el ciberespacio es el entorno virtual que no tiene fronteras físicas y que a través de una conexión a internet permite la interacción de las personas y los medios de comunicación, generando un impacto social en este mundo globalizado.

Es evidente en este mundo hiperconectado, que la sociedad en general interactúa en una red de intercomunicación global, en un espacio virtual en donde se conjugan la tecnología con la mano de hombre, siendo este último el factor decisivo en las operaciones que hace eco al concepto de noosfera[2]. Sobre esto último (López, 2012) afirma que es un medio artificial, creado por el hombre, por lo que este es un factor crítico en su desarrollo y evolución.

2.2. Las nuevas amenazas en el ciberespacio

El internet en los 90 alcanza un comportamiento tal que le permite en los 2000 marcar un punto de inflexión en el desarrollo socioeconómico de todo el mundo. El alto tráfico de información llevado a cabo en la red creció paralelamente con las amenazas, hasta considerar que la evolución y cuantificación tecnológica atente inconscientemente a la seguridad nacional de un Estado.

Ante la vertiginosa proliferación de las amenazas cibernéticas, los gobiernos han comenzado a poner en marcha estrategias de seguridad digital, adoptado de forma urgente políticas de ciberseguridad como una herramienta que garantice los derechos y libertades de sus ciudadanos. En este sentido, la OTAN en enero de 2008 en la Cumbre de Bucarest aprueba su primera política de defensa cibernética, en la que enfatiza la necesidad de asegurar sus propias redes, pero también de reforzar las capacidades globales de los aliados (Fuente, 2022).

En Latinoamérica las amenazas cibernéticas han venido ganando importancia a medida que existe más población conectada a internet, aumentando las actividades delictivas por parte de los delincuentes informáticos. Bajo este contexto, KPMG (2022) corrobora que el fraude y la ciberseguridad se superponen en un grado cada vez mayor. Los tipos de ciberataques han aumentado, incluyen phishing 44%, estafa 33%, software espía 22% y ransomware 20%.

En ese sentido, los ataques cibernéticos en el año pasado han sido notables, como destaca Iris Montoya

2 Espacio compuesto por toda la conciencia y el pensamiento humano.

Ricaurte en su artículo "Pymes en Latinoamérica: hasta cuatro veces más ciberataques en 2022":

> En México pasaron de 123.640 en 2021 a 323.434 en 2022; Brasil había registrado 88.432 asaltos en 2021, cifra que llegó a los 215.580 en 2022; mientras tanto, Colombia pasó de 39.627 ataques denunciados en 2021 a 161.589 en 2022 y; por su parte, Chile tuvo un incremento considerable también, de 17.069 ataques descubiertos en 2021 a 80.546 en 2022. Estos indicadores implican un aumento del 261 %, 243 %, 407 % y 471 %, respectivamente (Montoya, 2022).

El Ecuador enfrentó el mayor ataque cibernético de su historia en abril de 2019, luego que el gobierno del Ecuador decidió retirar el asilo diplomático a Julián Assange, fundador de WikiLeaks. Según fuentes oficiales, se registraron más de 40.000.000 ataques a diferentes instituciones públicas y privadas ecuatorianas en pocos días, lo que puso en evidencia la vulnerabilidad del país en el aseguramiento del ciberespacio (Rivadeneira, 2019).

En el Ecuador el sector gubernamental y no gubernamental han sido vulnerados en la seguridad de la información, sufriendo grandes afectaciones en las organizaciones y el desarrollo de sus procesos. Además, en el campo militar ya hubo la manifestación de ciberataques afectando la infraestructura crítica digital de la Escuela de Formación de Soldados del Ejército (ESFORSE) y la Dirección Nacional de Espacios Acuáticos (DIRNEA). La Marina del Ecuador sufrió un ataque informático, afectando el Sistema de Gestión Marítima (SIGMAR) el 23 de enero del presente año, sus expertos detectaron una vulneración en el Sistema de Gestión Marítima" (Mella, 2022, P. 6).

Varios analistas prevén que en el Ecuador las ciberamenazas se incrementarán en los próximos años; la estrategia para hacer frente a estas amenazas cibernéticas debe ser planificada y coordinada de una forma integral donde todos los actores del Estado orienten sus esfuerzos en la misma dirección. "Para que la estrategia tenga éxito es fundamental enfocar de manera estructurada su ejecución, con los recursos humanos y financieros adecuados, enfoque que debe considerarse parte de su desarrollo" (Unión Internacional de Telecomunicaciones, 2018, p. 24).

2.3. El panorama de la ciberseguridad

La seguridad, a más de ser valorada como un bien público, se le cataloga como una sensación de ausencia de riesgos y de amenazas, es un derecho que todos los seres humanos desean alcanzar de la mano de un Estado que brinde la protección, la estabilidad y el bienestar a su pueblo. La seguridad en un Estado se visualiza desde los diferentes espacios, que de acuerdo al CESEDEN (2012) lo contextualiza como la defensa territorial, la defensa aérea, la defensa de las fronteras, la defensa económica y como uno de estos espacios es precisamente el espacio de la cibernética o ciberespacio.

La seguridad digital ha evolucionado como parte de la globalización con un flujo masivo de datos, creando la necesidad de proteger la información de forma permanente para minimizar el impacto del acecho de los delincuentes cibernéticos que atacan desde el anonimato, por esta razón es importante saber a qué tipos de amenazas se está expuesto y qué actitud debe tomarse ante estos ciberdelincuentes. "Es imprescindible saber hoy ante qué ciberamenazas se está enfrentando y qué estrategia se debe adoptar para reducir la vulnerabilidad y de la sociedad en su conjunto" (Ballestero, 2020).

En Latinoamérica en la última decada han emergido nuevos desafios para los Estados en cuanto a ciberseguridad, obligando a proponer políticas públicas e instrumentos jurídicos en diferentes sectores, como describe Bustos & Aguerre (2021) las políticas sobre ciberseguridad están caracterizadas por dinámicas de innovación, proyectando a la política de ciberseguridad como punto de confluencia de los diferentes sectores con interés concurrente en la actividad; se entiende como sectores de interés a los actores del sector privado, la academia y organizaciones no gubernamentales.

Es importante destacar que la política de ciberseguridad de Brasil según Cruz (2017) fue aprobada por el Ministerio de Defensa en 2012, denominada Política Cibernética de Defensa que establece los principios, objetivos y directrices para las actividades en ese sector, con significativas contradicciones que resultan de problemas institucionales y administrativos de sus políticos. La imprecisión de las intenciones gubernamentales que no han sido acertadas en el desarrollo de Políticas de Ciberseguridad en la última década quiere equilibrar su enfoque en la comprensión de las tácticas técnicas y procedimientos de los delincuentes cibernéticos.

Colombia, a través del Consejo Nacional de Política Económica y Social (CONPES) establece los lineamientos de Política de Ciberseguridad y Ciberdefensa para proteger la infraestructura crítica digital. Según Cáceres (2017) Colombia adoptó una Política Nacional de Seguridad Digital, después de cinco años de presentada la primera, cuyo objetivo general es fortalecer las capacidades del Estado para responder a las amenazas en materia de seguridad cibernética. Todo esto con la finalidad de fortalecer la ciberseguridad en la búsqueda y prevención de los ciberataques para identificar, enmarcar, proponer, y coordinar respuestas proactivas y reactivas ante amenazas a la confidencialidad, integridad y disponibilidad.

La ciberseguridad como política pública en Chile está regentada por el Ministerio de Defensa Nacional, que con la necesidad de actualizar sus planes de seguridad dispone la elaboración de una Política de ciberseguridad "En esta línea, ya en abril de 2017, el Ejecutivo a través del Ministerio de Defensa Nacional emitió la Política Nacional de Ciberseguridad 2017-2022, que se convirtió en el primer instrumento estatal dirigido a desplegar una estrategia nacional en este ámbito" (Jarufe, 2022, P. 2)

Por lo anotado anteriormente, se puede afirmar que las Políticas de Ciberseguridad en la mayoría de los países de América Latina tienen su órgano rector al Ministerio de Defensa Nacional, mientras que en el Ecuador el campo de la ciberseguridad esta regentado por el Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL) que a través del acuerdo ministerial 006-2121 del 17 de mayo del 2021 publica la Política Nacional de Ciberseguridad (PNC). Según Michellena (2021) para proteger las infraestructuras críticas del Estado y de seguridad a la población en el ciberespacio, sustentan su línea de acción orientadas en 7 pilares[3] para garantizar las libertades de los ciudadanos.

El Plan Específico de Seguridad Pública y Ciudadana 2019-2030 fija objetivos para detener los delitos transnacionales, entre ellos el delito cibernético y en el Art. 154 de la Constitución de la República del Ecuador confiere a los ministros de Estado, además de las atribuciones establecidas en la ley, la rectoría de las políticas públicas del área a su cargo. Bajo este contexto, Gobierno Nacional a través del MINTEL publica la Estrategia Nacional de Ciberseguridad en el Ecuador (ENCE). Instrumento para mantenerse alertas ante los ciberdelincuentes, donde la evolución de la amenaza es dinámica y vertiginosa (Maino, 2022).

Con esta concepción, el MINTEL como órgano rector de la ENCE en estrecha relación con actores nacionales e internacionales tiene por objeto establecer la dirección y un marco para alcanzar objetivos específicos y claros con una aplicación de 3 años (2022-2025), se basa en "seis ejes de acción que abarcan temas coyunturales y prioritarios para el país: Gobernanza y coordinación nacional; Resiliencia cibernética; Prevención y combate a la ciberdelincuencia; Ciberdefensa; Habilidades y capacidades de ciberseguridad; y Cooperación internacional" (MINTEL, 2022, P. 3).

Para el cumplimiento y la ejecución de la política de Estado antes mencionada es necesario articular acciones y establecer responsables permanentes de los objetivos y los pilares ya citados, sin descuidar la estrecha coordinación estratégica de las instituciones responsables en materia de ciberseguridad. La perspectiva de la situación actual de la ciberseguridad en el Ecuador "persigue fortalecer el ciberespacio, crear planes, guías y metodologías para este ámbito; pero es innegable que también es fundamental a priori la promulgación de leyes que centren y regulen todos los aspectos relacionados a la ciberseguridad en este país" (Cedeño, 2022, P. 59).

3 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.

2.4. La Ciberdefensa y la infraestructura crítica del Estado

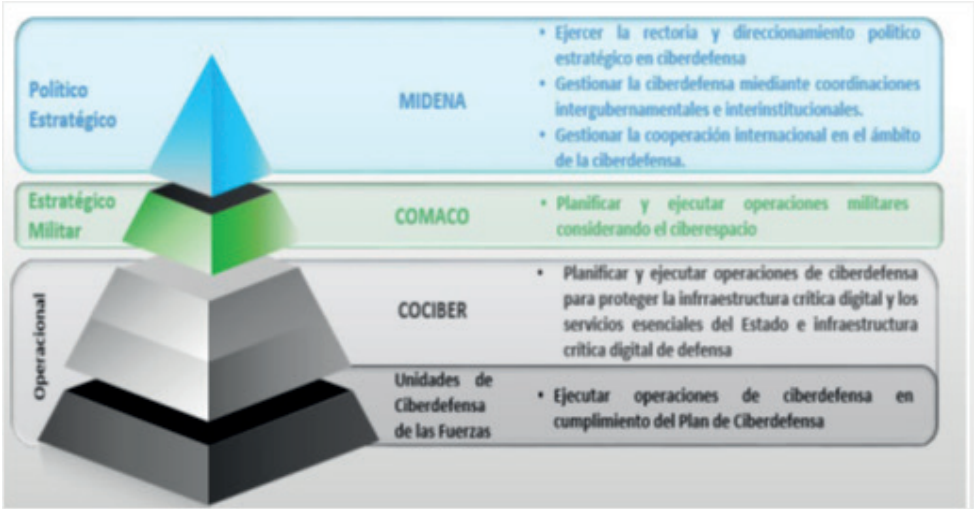
Durante la Guerra Fría se prioriza la seguridad en la protección de documentos relacionados a operaciones externas, producción de armamento y otro tipo de estrategias que con el tiempo han sido cambiantes, donde las instituciones deben adaptarse a estos cambios para tener la capacidad de enfrentar la problemática difusa que se manifiesta en el ciberespacio para proteger la infraestructura crítica digital (ICD) de cada Estado. Muchas de las acciones que se encuentran hoy en los nuevos conflictos geopolíticos se traducen en operaciones políticas, económicas, psicológicas y cibernéticas (Rivas, 2021).

La defensa de la ICD y del ciberespacio se relaciona con la estrategia de la ciberdefensa en la concepción estratégica militar, donde la ciberdefensa describe una visión de la situación, principios y enfoques para comprender las necesidades del Estado. Las estrategias variarán según el país, el enfoque puede estar en proteger la infraestructura crítica, en resguardar los datos, tal vez otros países no las tienen definidas y al no saber qué infraestructura crítica proteger, se torna difícil cumplir con la misión de ciberdefensa. Por lo que se puede suponer que cada país define en su constitución política, o en otra instancia que es deber del Estado proteger la vida y la salud de sus ciudadanos (Peréz, 2022).

El Ministerio de Defensa Nacional (MDN), con fecha el 12 de septiembre de 2014, mediante Acuerdo Ministerial No. 281 acuerda la creación del Comando de Ciberdefensa de Fuerzas Armadas (COCIBER), con la misión de "ejecutar operaciones de defensa y exploración en el ciberespacio en forma permanente, para proteger la ICD y servicios esenciales del Estado de infraestructura crítica digital de Fuerzas Armadas y con orden, cumplir operaciones de respuesta para neutralizar ciberamenazas" (Ministerio de Defensa Nacional, 2021a, P. 67).

La Política de la Defensa Nacional del Ecuador de 2018 expedida mediante Decreto Ejecutivo N° 633 de 8 de enero de 2019 establece: "(…). El sector Defensa impulsa la coordinación interinstitucional de la ciberdefensa en el marco de la seguridad cibernética nacional y posee una capacidad considerable para defender la infraestructura crítica digital de las Fuerzas Armadas (…)"; en tal virtud, el MDN el 11 de mayo del 2021, con Acuerdo Ministerial Nº 199 ACUERDA: Expedir la Política de Ciberdefensa para el Sector Defensa "Art. 1.- Establecer la nueva estructura de ciberdefensa del sector defensa, en los niveles político-estratégico, estratégico-militar y operacional, que permitan implementar políticas y estrategias de ciberdefensa" (Ministerio de Defensa Nacional, 2021b, p. 3).

Figura 3
Estructura de Ciberdefensa del Sector Defensa



Nota. Obtenido del Ministerio de Defensa Nacional (Orden Ministerial Nº119)

Como se deduce de la Figura 2, el MDN, el COMACO y el COCIBER son los tres niveles encargados de la rectoría, de la planificación y de la ejecución de las operaciones de Ciberdefensa, respectivamente. En el Nivel Político Estratégico, el MDN establece el Plan de Desarrollo de la Ciberdefensa (PDC) con un mapa de ruta que garantice la ejecución de la ciberdefensa y la protección de la ICD del Estado, basado en tres fases: 1) Fundamentación Estratégica, 2) Desarrollo de Capacidades en Ciberdefensa y 3) Fortalecimiento de Capacidades en Ciberdefensa, en los siguientes términos:

> El desarrollo de estas fases se extiende por un periodo de 10 años, periodo en el cual se incluyen cinco áreas de objetivos para que el Ministerio de Defensa y el COCIBER incremente sus capacidades de ciberdefensa. Estas incluyen: 1) fundamentación estratégica; 2) establecer las estructuras de políticas y de gobernanza; 3) mejorar la resiliencia operativa y de la red; 4) capacitar y desarrollar la fuerza cibernética; 5) cultura de Conciencia Cibernética desarrollada dentro del MDN (Ministerio de Defensa Nacional, 2021c, P. 56).

Al momento nos encontramos en la primera fase del PDC y es necesario continuar con el levantamiento de ICD del Estado, puesto que en el Ecuador hasta el momento no están definidas en su totalidad, por lo que es indispensable en la defensa y seguridad de los servicios esenciales de todos los ecuatorianos. Este criterio se sostiene en la afirmación que se hace en la Estrategia Nacional de Ciberseguridad (2021) cuando afirma que "la protección de las ICD nacionales no está actualmente cubierta de forma exhaustiva por el marco jurídico, lo que plantea un desafío para la aplicación de los principios de seguridad y la supervisión normativa para garantizar el cumplimiento" (p. 23). Estrategia que en este nivel debe definirse.

En el nivel estratégico militar, el COMACO es el responsable de planificar y ejecutar operaciones militares, actividad que está siendo desarrollada de una manera muy tenue puesto que el PDC está en un proceso inicial, proceso que es indispensable continuar cumpliendo con la fundamentación estratégica como paso obligatorio en la protección de la información estratégica y la infraestructura crítica del país, donde el ente planificador es clave pensando en su capacidad estratégica para la conducción efectiva de operaciones conjuntas en los diferentes niveles.

En el nivel Operacional, el COCIBER opera las capacidades de defensa, explotación y respuesta en el espacio cibernético de forma limitada por la falta de infraestructura tecnológica moderna y capacitación especializada de sus operarios, siendo urgente disponer de un Centro de Operaciones de Seguridad (SOC), articulando la plataforma de ciberinteligencia, el servicio de vigilancia, el rastreo y el análisis de la WEB. La integración efectiva de las operaciones cibernéticas defensivas y ofensivas, la vigilancia y el reconocimiento, así como con las capacidades de ataque cinético, impone la necesidad de contar con sofisticados sistemas de gestión de la batalla (Bobadilla, 2022).

El nuevo escenario y la proliferación de ciberamenazas obligan que la ciberseguridad y ciberdefensa sean las herramientas fundamentales en la política y estrategia de un Estado en el campo de seguridad y defensa, por lo que es necesario diferenciar los conceptos de ciberseguridad y ciberdefensa; donde el primero de ellos es mucho más amplio, abarcando todos los ámbitos del Estado, mientras que el segundo es una responsabilidad propia de Fuerzas Armadas en post de la protección de la ICD.

La ciberseguridad para la Unión Internacional de Comunicaciones (UTI) es "el conjunto de herramientas políticas, guías de acción, abordajes de gestión, acciones, mejores prácticas y tecnologías empleados para proteger la disponibilidad integridad y confiabilidad de activos en las infraestructuras interconectadas" (UTI, 2018, p. 13). En definitiva, son las acciones preventivas y reactivas para el aseguramiento del ciberespacio frente a las amenazas cibernéticas.

La ciberdefensa se conceptúa como las capacidades defensivas y ofensivas de las Fuerzas Armadas que tienen un Estado para proteger su ICD, evitando los accesos no deseados causados por amenazas proveniente del ciberespacio. En todo el mundo, los actores gubernamentales y no gubernamentales han desarrollado capacidades cibernéticas, tanto ofensivas como defensivas, que han desencadenado una reexaminación de las nociones tradicionales del poder global, la influencia, e incluso la guerra (Ganuza, 2020).

2.5. La inteligencia artificial en la defensa del Estado

La Política de la Defensa y la Seguridad de un Estado gesta el objetivo más importante de una nación, la seguridad multidimensional derivado de los elementos que conforman y se acoplan a la realidad del avance tecnológico, donde cada vez es sustancial la integración de la inteligencia humana con los medios tecnológicos, para tomar decisiones inteligentes dentro de escenarios disruptivos. En este sentido, hay que ser realistas y conscientes que las nuevas tecnologías emergentes son parte del ciberespacio y otras continúan apareciendo como un desafío cambiante, como el big data, robots sociales y la inteligencia artificial.

El empleo racional de la IA facilitará el trabajo en sectores de la industria, salud, transporte, energía y por supuesto en el campo de la defensa, en este último ayuda a detectar las amenazas, automatizar las respuestas y acelerar la defensa. Sin embargo, el mal uso de IA, puede traer irremediables consecuencias nocivas para la humanidad, ya sea con drones asesinos y humanoides podrían afectar la seguridad de los Estados en los campos de seguridad digital, física o política (Romero, 2019).

En los últimos años las grandes industrias y las potencias mundiales compiten por conseguir la hegemonía del manejo de la IA como el nuevo poder geopolítico global, no les conviene quedarse al margen de esta revolución tecnológica de difícil previsión, considerando que un nuevo mundo ha nacido con el uso de la Inteligencia Artificial en el ámbito militar. En la actualidad existe una nueva carrera armamentista en la que China, Estados Unidos y Rusia pugnan por tener hegemonía en lo que para muchos autores se conoce como "La guerra fría de la Inteligencia Artificial" (Calvo, 2023).

Esta última referencia de alguna manera hace notar la trascendencia de la IA en el ámbito militar, donde los sectores de defensa, vigilancia y seguridad de un Estado no pueden aislarse de esta cuarta revolución industrial, por lo contrario, deben articular esfuerzos pensando en la seguridad internacional y la política exterior como estrategia de defensa. La IA ha sido considerada como una tecnología de desequilibrio en el empleo de las fuerzas militares, siendo un elemento disruptivo de orden económico, industrial y social que afecta en forma inmediata el contexto estratégico internacional (Romero, 2019b).

Trejo (2019) expresa que la gran magnitud de las aplicaciones de inteligencia artificial, en las áreas civil y militar, la convierte en un tema de relevancia mundial que rebasa las capacidades de las grandes potencias y las mayores empresas tecnológicas. Bajo este contexto, China y Estados Unidos, a pesar de disputar el poder hegemónico mundial, han promovido investigaciones tecnológicas de gran magnitud de forma coordinada con grupos capacitados y expertos tecnológicos comunes en base a la intervención mutua en los ámbitos científico y económico.

Orientando la conceptualización anterior a la región Latinoamericana es perentorio formalizar convenios de cooperación y defensa con otros Estados en materia de IA, así como con la academia y actores no estatales que vienen trabajando con resultados significativos en el tema. Latinoamérica y los países en desarrollo en forma general no han tenido un despunte en el campo de IA, considerando la carencia de personal técnico capacitado, buen manejo de bases de datos, infraestructura investigativa, alianza estratégica con las industrias y sobre todo la falta de inversión como una Política de Estado que abarque los ámbitos tecnológicos y de la Defensa.

El uso de la inteligencia artificial en el Ecuador ha experimentado un crecimiento atomizado en los sectores públicos y privados, sumado a esto la carencia de una política pública de IA, lo que ha agravado el desarrollo de este campo tan importante. Como corrobora Albornóz (2020) desde el 2018 el Ecuador ha iniciado la construcción de una política digital sin lograr diseñar instrumentos de política de IA. Esto se debe a que los emprendimientos de IA en el país están creciendo de manera parsimoniosa y desarticulada.

El empleo de la IA en la defensa del Estado es de gran valía, puesto que permitirá detectar las posibles amenazas, automatizar las respuestas y aligerar la defensa. Es decir, el empleo de Inteligencia Artificial "producirá un impacto importante en determinados tipos de operaciones militares en los tres niveles. La inteligencia artificial cambiará el carácter de la guerra, pero no modificará su naturaleza como un enfrentamiento humano incierto y complejo que busca un fin político" (Roldán, 2018, p. 114).

En las Fuerzas Armadas ecuatorianas no se ha evidenciado un despunte en el empleo de la IA, aún no se ha visto un desarrollo importante en el tema, razón por la que es necesario realizar el acercamiento

adecuado con la academia y la empresa privada, para articular acciones que permitan a la institución armada a proyectarse en miras de la defensa del Estado en base a un proceso de transformación que permita encauzar las futuras investigaciones donde el sector público y privado conjuguen esfuerzos para desarrollar capacidades tecnológicas con normas éticas para el empleo de la IA.

Finalmente, tras esta rápida visión, del ciberespacio, de la ciberseguridad, de la ciberdefensa y la Inteligencia Artificial en el entorno en el que se desarrollan, se puede considerar que existen diversas oportunidades de mejora orientadas a la defensa del Estado, puesto que en este momento las Fuerzas Armadas se encuentra en un proceso de transformación, innovación y modernización tecnológica, proyectando el desarrollo de las investigaciones al sector de seguridad y defensa, orientando su esfuerzo al aseguramiento de los dominios y la infraestructura crítica del Estado, esfuerzo que está girando en los nuevos retos de la cuarta revolución industrial.

3. DEFENSA DE LA INFRAESTRUCTURA CRÍTICA DEL ESTADO

Propuesta para la creación de una comisión para categorizar las Infraestructuras criticas digitales del Ecuador

Conforme a lo establecido en el artículo 66 numeral 19 de la Constitución de la República, se reconoce y garantizará a las personas: "El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección…", para lo cual el Estado debe formular, implementar y evaluar políticas públicas que garanticen los derechos reconocidos por la Carta Magna.

En este sentido, el Art. 154, numeral 1 ibídem confiere a los ministros de Estado, además de las atribuciones establecidas en la ley, la rectoría de las políticas públicas del área a su cargo; así como la facultad de expedir los acuerdos y resoluciones administrativas que requiera su gestión. Concomitantemente con este mandato, el artículo 140 de la Ley Orgánica de Telecomunicaciones dispone que el Ministerio encargado del sector de las Telecomunicaciones y de la Sociedad de la Información (MINTEL) es el órgano rector de las telecomunicaciones y de la sociedad de la información, informática, tecnologías de la información y las comunicaciones y de la seguridad de la información.

Bajo esta perspectiva, mediante Acuerdo Ministerial 006-2021 de 17 de mayo de 2021, el MINTEL publica la Política Nacional de Ciberseguridad (PNC). Esta política tiene un enfoque multisectorial y multidimensional considerando el carácter transversal de la ciberseguridad, por lo que se crea el "Comité Nacional de Ciberseguridad compuesto por las siguientes instituciones: El MINTEL, quien lo preside, el Ministerio de Gobierno (MDG), el MDN, el Centro de Inteligencia Estratégica (CIES) y el Ministerio de Relaciones Exteriores y Movilidad Humana (MREMH), enfoque que se materializó como el pilar de gobernanza de la ciberseguridad de la política de ciberseguridad.

En la PNC se establece como uno de los pilares la Protección de la infraestructura crítica digital y servicios esenciales del Estado, estableciéndose entre otros como lineamiento el de Identificar y definir la infraestructura crítica digital (ICD) a nivel nacional, teniendo en cuenta que engloba múltiples sectores, basándose en consideraciones políticas, sociales, económicas y ambientales.

En este sentido, se debe considerar que la ciberdefensa es un complemento de la ciberseguridad, que proporciona la defensa contra las amenazas en el ciberespacio, siendo parte de la acción estratégica de la Política de Defensa 2018, que se articula con el inciso segundo del Art. 158 de la Constitución Política del Ecuador que establece: "… Las Fuerzas Armadas tienen como misión fundamental la defensa de la soberanía e integridad territorial y, complementariamente, apoyar en la seguridad integral del Estado de conformidad con la ley".

Basado en este mandato constitucional, el Ministerio de Defensa publica mediante Acuerdo Ministerial No. 199 de 11 mayo de 2021 y articulándose con los objetivos de la política de ciberseguridad, la Guía Político-Estratégica de Ciberdefensa, que busca orientar el accionar en el nivel político estratégico de la ciberdefensa, su relación con los otros sectores gubernamentales y su aplicación en los ejes de la seguridad integral en general y de la defensa en particular; y la Estrategia de Ciberdefensa con el propósito fundamental de establecer lineamientos para fortalecer a la ciberdefensa como una capacidad estratégica del Estado.

Actualmente, las ICD del Estado en el Ecuador hasta el momento no están definidas y más aún levantadas en su totalidad. A fin de articular adecuadamente la protección de las infraestructuras criticas digitales del Estado, como producto de la presente investigación, se plantea la siguiente propuesta:

Proponer una comisión correspondiente a identificar y definir la infraestructura crítica digital (ICD) a nivel nacional, teniendo en cuenta que engloba múltiples sectores, basándose en consideraciones políticas, sociales, económicas y ambientales; siendo parte los objetivos 3 y 4 de la PNC, estableciéndose como responsable de su ejecución al Ministerio de Defensa Nacional, se deberá crear una Comisión Multisectorial en la que se incluya a las universidades para desarrollar una metodología que permita levantar, categorizar y proteger las infraestructuras críticas digitales y desarrollar los planes de defensa que garantice al Estado ecuatoriano el seguro de sus activos digitales ante cualquier tipo de amenaza que pueda atentar sobre la soberanía e integridad de la nación.

En la comisión deben estar claramente identificados los actores con una acción unificada y articulada, que englobe el trabajo interinstitucional e intersectorial de todos los sectores para la catalogación y categorización de la ICD, de acuerdo a las siguientes consideraciones:

- Identificar y definir la ICD del Estado
- Definir líderes sectoriales
- Categorizar los equipos de trabajo sectorial
- Establecer una guía para el levantamiento de la ICD
- Levantamiento de los sectores estratégicos
- Consolidación de la información
- Catalogación y categorización de la ICD

CONCLUSIONES

Resulta inevitable establecer políticas y estrategias para hacer frente a las amenazas cibernéticas, acciones que deben ser planificadas y coordinadas de una forma integral, donde todos los actores públicos y privados del Estado orienten sus esfuerzos a la protección del ciberespacio ante las nuevas amenazas emergentes.

La Política de Ciberseguridad Nacional ha pretendido fortalecer las capacidades de defensa, buscando afianzar un ciberespacio seguro en el intercambio de la información, estableciendo directrices para encaminar las acciones en el aseguramiento del ciberespacio. Sin embargo, la democratización del uso indiscriminado del ciberespacio siempre será una amenaza latente para la defensa del Estado.

Las amenazas emergentes del ciberespacio obligan al Estado a desarrollar capacidades necesarias para prevenir, investigar y combatir este tipo de fenómenos a través de acciones de ciberseguridad y ciberdefensa. Sin embargo, seremos vulnerables, puesto que las acciones preventivas con herramientas tecnológicas, equipo tecnológico y personal técnico capacitado no serán suficientes en el cumplimiento de las actividades de seguridad cibernética.

La catalogación y categorización de la ICD de Estado recae sobre la responsabilidad del MDN, debiendo crear una Comisión Multisectorial para levantar, categorizar y proteger la ICD con una acción unificada y articulada, que englobe el trabajo interinstitucional e intersectorial de todos los actores, desarrollando planes de defensa que garantice al Estado ecuatoriano el aseguramiento de sus activos digitales ante cualquier tipo de amenaza que pueda atentar sobre la soberanía e integridad de la nación.

El Ecuador requiere de forma urgente un modelo de gobernanza en materia de ciberseguridad, ciberdefensa e inteligencia artificial que articule los esfuerzos aislados del sector público y privado, lo que implica poner en marcha una estrategia nacional con acciones preventivas y con una mirada ampliadora en la defensa de la infraestructura crítica digital del Estado ante las amenazas emergentes de la cuarta revolución industrial.

Referencias

Albornóz, M. (2020). Ecuador: Inteligencia artificial sin rumbo fijo. *Empatía,* 1-3.

Ballestero, F. (2020). La Ciberseguridad en tiempos difíciles. Colaboraciones. *Boletín conómico de ICE*, 39-48.

Bobadilla, B. (2022). *El ciberespacio como nuevo escenario de conflicto. Jornada de Seguridad y Defensa*.

Bustos Frati, G., & Aguerre, C. (2021). Políticas públicas sobre ciberseguridad en América Latína: El caso de Argentina. *Centro LATAM Digital*, 1-36.

Cáceres, J. A. (2017). Colombia, estratégia nacional en ciberseguridad y ciberdefensa. *Air_space power journal*, 85-89.

Calvo, D. (2023). La inteligencia Artificial y el futuro de la guerra. *Lisa News*, 1-5.

Cedeño, R. (2022). Ciberseguridad y Ciberdefensa: Perspectiva de la situación actual de la ciberseguridad en el Ecuador. *Revista Tecnológica Ciencia y Educación, Edwards Deming*, 50-62. doi:https://doi.org/10.37957/rfd.v6i1.88

CESEDEN. (2012). *El ciberespacio, nuevo escenario de la confrontación*. Centro Superior de estudios de la Defensa Nacional.

Cruz Lobato, L. (2017). Política Brasileña de Ciberseguridad como estratégia de liderazgo nacional. URVIO, *Revista Latinoamericana de Estudios de Seguridad*(20), 16 - 30. doi:http://dx.doi.org/10.17141/urvio.20.2017.2576

De la Guardia, J. (18 de Julio de 2017). El quinto frete de batalla. *Política Exterio*r, s.n. https://www.politicaexterior.com/el-quinto-frente-de-batalla/

ENCE. (2022). *Objetivos estrategicos de Estrategia nacional de Ciberseguridad en el Ecuador*. Estrategia nacional de Ciberseguridad en el Ecuador.

Espinosa, S. (2021). *La ciberseguridad, el ciberespacio, internet y las tecnologías de la información y las comunicaciones.* Cuba, debate.

Estrategia Nacional de Ciberseguridad . (2021). Resiliencia Cibernética, *Pilar 2.* MINTEL, 20-26.

Fernández, A., & Montesinos, F. (25 de Noviembre de 2015). Las generaciones de las guerras. *Ieee.es.* Obtenido de https://www.ieee.es/

Ganuza. (2020). *Orientaciones para el diseño, plaeamiento, implementacón y desarrollo de una ciberdefensa militar.* Guía de ciberdefensa.

Íñiguez Matute, F. (2022). Estrategia Nacional de Ciberseguridad busna promover capacidades de resiliencia cibernética. *ITahora, La revista del líder de tecnología*.

Jarufe Bader, J. P. (2022). *Ciberseguridad e inteligencia artificial en Chile*. Biblioteca del Congreso Nacional Chile; asesoría ténica parlamentaria, 1 - 9.

KPMG. (2022). *Una triple amenaza en las Américas. KPMG Fraud Outlook*, 1-28.

Lehto, & Henselman. (2020). Non-Kinetic Warfare : The New Game Changer in the Battle Space. The New Game Changer in the Battle Space. In B. K. Payne, & H. Wu (Eds.), *ICCWS 2020* :. Obtenido de http://rightsstatements.org/page/InC/1.0/?language=en

López, J. (2012). *La evolución del conflicto hacia un nuevo escenario bélico*. Centro Superior de estudios de la Defensa Nacional (CESEDEN).

Maino, V. (2022). *Estrategia nacional de ciberseguridad. Ministerio de telecomunicaciones y de la seguridad de la información* (MINTEL).

Michellena, A. (2021). *Política Nacional de Ciberseguridad. En M. d. información, Política Nacional de Ciberseguridad.* Acuerdo ministerial 006-2121.

Ministerio de Defensa Nacional. (2021a). Aplicación de Ciberdefensa en Ecuador. *Guía Político-Estretégico de Ciberdefens*a, 61-71.

Ministerio de Defensa Nacional. (2021c). Fundamentación Politico -Estratégico de la Ciberdefensa. Guía Politico - Estratégico de Ciberdefensa, 47-59.

Ministerio de Defensa Nacional. (2022b). Acuerdo Ministerial. Orden General Nº71, 1-9.

MINTEL. (2022). Estrategia Nacional de Ciberseguridad. Ministerio de comunicaciones y de la Sociedad de la Información, 1-58.

Moncayo, P. (2022). Seguridad y Defensa. Quito, Pichincha: Comisión Editorial de la Universidad de las Fuerzas Armadas-ESPE.

Montoya, I. (2022). Pymes en Latinoamérica: hasta cuatro veces más ciberataques en 2022. Ventas de Seguridad, 1-3.

Peréz, J. (2022). *Infraestructura crítica y ceiberespacio*. DREAMLAB TECHNOLOGIES, s.n.

Perkins, D. (2018). Preparándonos para combatir hoy, las operaciones multidominio y el Manaul de campaña 3.0. Military Review, 12-20.

Rivas, S. (2021). El ciberespacio como zona de control geopolítico y el papel de las potencias por la supremacia de la cibernética.

Roldán , J. (2018). *La inteligencia artificial y la fricción de la Guerra.* Instituto Español de Estudios estratégicos, 113-140.

Romero, A. (2008). Guerra y paz. *Revista mexicana de sociología.* https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0188-25032008000300005

Romero, S. (2019). Inteligencia Artificial como herramienta de estratégia de seguridad para la defensa de los Estados. *Revista de la Escuela Superior Naval*, Perú, 1-9.

Telecomunicaciones, U. I. (2018). *Guía para la elaboración de una estrategia nacional de ciberseguridad*. Unión Internacional de Telecomunicaciones, 1-68.

Trejo, F. (2019). Los desafios de la inteligencia artificial en el sistema internacional. Foreign Affairs Latinoamérica, 1-3.