Revista Perspectivas en Inteligencia
Revista Científica en Ciencias Sociales e Interdisciplinaria
Bogotá D.C., Colombia
ISSN: 2145-194X (impreso), 2745-1690 (en línea)
Página Web: https://revistascedoc.com/index.php/pei

Ciberseguridad, un desafío para las Fuerzas Militares colombianas en la era digital

Autores:

Jeison Stiven Peña Suárez
https://orcid.org/0009-0003-1399-6433
Universidad Santo Tomás
✉ jeisonpena@usantotomas.edu.co

Citación APA: Peña Suárez, J.S. (2023). Ciberseguridad, un desafío para las Fuerzas Militares colombianas en la era digital. Perspectivas en Inteligencia. 15(24), 333-359. http://doi.org/10.47961/2145194X.628

Publicado en línea: 2023

Para enviar un artículo:
https://revistascedoc.com/index.php/pei/about/submissions

PERSPECTIVAS EN INTELIGENCIA 2023

Revista Científica en Ciencias Sociales e Interdisciplinaria
Bogotá D.C., Colombia
Volumen 15, N° 24, Enero - Diciembre 2023, pp. 333-359
http://doi.org/10.47961/2145194X.628

Ciberseguridad, un desafío para las Fuerzas Militares colombianas en la era digital

Cybersecurity, a challenge for the Colombian Military in the digital age

Jeison Stiven Peña Suárez[1]

(1) Universidad Santo Tomás, Bogotá, D. C. – Colombia,
✉ jeisonpena@usantotomas.edu.co

"Ataca cuando no estén preparados, muéstrate cuando no eres esperado"
Sun Tzu

Resumen

El propósito de este artículo de revisión es analizar los desafíos a los que se enfrentan las Fuerzas Militares colombianas en términos de ciberseguridad. En cuanto al diseño metodológico, se abordó desde un enfoque cualitativo, empleando la técnica de análisis documental con el fin de obtener y examinar fuentes de información, tales como libros y artículos académicos. Las instituciones castrenses tienen la responsabilidad de salvaguardar los intereses del Estado en el dominio cibernético. Dado que es un deber constitucional de las Fuerzas Militares garantizar la protección de la soberanía digital y física, resulta fundamental fortalecer constantemente sus capacidades y colaborar activamente con actores internacionales y locales para robustecer los sistemas de protección de las infraestructuras críticas. Esto es con el fin de hacer frente a las amenazas cibernéticas que utilizan tecnologías disruptivas, mediante inteligencia artificial y virus informáticos, las cuales tienen como objetivo generar pánico en la población mediante la difusión de ataques a la infraestructura crítica, afectando los entornos sociales, económicos y políticos de la población, además de otras amenazas, como las operaciones de información con el fin de desestabilizar los gobiernos de turno.

Según el artículo 217 de la Constitución Política de Colombia, se ordena a las Fuerzas Militares proteger la soberanía y el orden nacional en cualquier dominio, promoviendo la

Fecha de recepción: 26/05/2023 | Fecha de aprobación: 18/09/2023

seguridad digital mediante la cooperación con la OTAN. Se destaca que esta organización ha desarrollado equipos de última tecnología; asimismo, cuenta con el personal militar idóneo para adelantar operaciones defensivas y ofensivas en el ciberespacio. Por último, es competencia de las Fuerzas Militares colombianas proteger la infraestructura crítica, ya que cualquier afectación a esta podría generar alteraciones en el orden político, económico, social y ambiental de la nación en su conjunto.

Clasificación JEL: K24, N4, N46.

Palabras clave: Ciberseguridad; infraestructura crítica; Fuerzas Militares; amenazas cibernéticas; ciberespacio.

Abstract

The purpose of this review article is to analyze the challenges faced by the Colombian Military Forces in terms of cybersecurity. As for the methodological design, it was approached from a qualitative approach, using the documentary analysis technique in order to obtain and examine sources of information, such as books and academic articles. Military institutions are responsible for safeguarding the interests of the State in the cyber domain. Since it is a constitutional duty of the Military Forces to ensure the protection of digital and physical sovereignty, it is essential to constantly strengthen their capabilities and actively collaborate with international and local actors to strengthen critical infrastructure protection systems. This is in order to address cyber threats that use disruptive technologies, through artificial intelligence and computer viruses, which aim to generate panic in the population by spreading attacks to critical infrastructure, affecting the social, economic and political environments of the population, in addition to other threats, such as information operations in order to destabilize the governments in power.

According to Article 217 of the Political Constitution of Colombia, the Military Forces are ordered to protect sovereignty and national order in any domain, promoting digital security through cooperation with NATO. It should be noted that this organization has developed state-of-the-art equipment; it also has the appropriate military personnel to carry out defensive and offensive operations in cyberspace. Finally, it is the responsibility of the Colombian Armed Forces to protect the critical infrastructure, since any damage to it could generate alterations in the political, economic, social and environmental order of the nation as a whole.

Keywords: Cybersecurity; critical infrastructure; Military Forces; Cyber threats; cyberspace.

Introducción

La proliferación de medios electrónicos como consecuencia de la cuarta revolución industrial ha llevado a un aumento en el acceso a internet, por parte de los habitantes del mundo, en la creación del ciberespacio[1]. Esto ha generado una serie de oportunidades en el desarrollo de las sociedades mediante una mayor cooperación entre los actores de la sociedad internacional, como resultado de la globalización. Desde la disciplina de la ciberseguridad[2], se analiza esta situación con un enfoque holístico y multidisciplinario, con el objetivo de proteger la infraestructura crítica. Esto se debe a que tanto los actores privados como los públicos se han vuelto más dependientes del ciberespacio, ya que facilita los procesos operativos y reduce costos económicos y humanos. No obstante, el ciberespacio, al ser un lugar intangible, ha sido propicio para acciones ilícitas realizadas por actores de la delincuencia transnacional y células terroristas.

Como consecuencia de esto, las instituciones militares han desarrollado nuevos mecanismos para enfrentar el surgimiento de amenazas a la seguridad nacional, siendo Colombia el primer país de Latinoamérica en adoptar lineamientos de política pública mediante el CONPES 3701 de 2011. En el contexto actual, los ciberataques[3] han aumentado la frecuencia y la sofisticación de estos. Por lo tanto, resulta imperativo implementar medidas de seguridad robustas y estar preparados para hacer frente a las amenazas que puedan comprometer la integridad de los sistemas digitales y la información sensible del Estado (Cujabante et al., 2020).

Las operaciones de las Fuerzas Militares en los últimos años se han desarrollado en un entorno multidominio que abarca el aire, la tierra, el mar, el espacio y el ciberespacio. El ciberespacio ha adquirido una importancia especial, debido a la constante evolución y adaptabilidad de los grupos delincuenciales y células terroristas a las nuevas tecnologías[4] (Carvajal, 2022). Sin embargo, las Fuerzas Militares colombianas requieren equipos de última tecnología que les permitan enfrentar y llevar a cabo operaciones cibernéticas con el fin de garantizar la seguridad de las infraestructuras críticas. Es importante porque las transacciones comerciales, los sistemas de información y las comunicaciones se realizan en entornos digitales; es fundamental desarrollar estrategias efectivas para proteger el ciberespacio de posibles amenazas a la soberanía digital.

1 Se define ciberespacio como el dominio global dentro del entorno de la información que consiste en la red interdependiente de infraestructuras de tecnología de la información y datos residentes, incluyendo internet, redes de telecomunicaciones, sistemas informáticos y procesadores y controladores integrados (Departamento de Defensa Estados Unidos, 2016).

2 Se refiere generalmente a la capacidad de controlar el acceso a las redes, sistemas de información y todo tipo de recursos de información (Leiva, 2015).

3 Son acciones realizadas por individuos, con el objetivo de vulnerar la seguridad de sistemas y equipos de información, mediante el uso de malwares o phishing.

4 Se refieren a: inteligencia artificial, internet de las cosas, realidad virtual y aumentada, blockchain.

La seguridad en el ciberespacio es un tema de suma importancia en la era digital actual. En este entorno, las amenazas convencionales se han transformado en amenazas híbridas[5] que engloban una variedad de actividades, como ciberataques a la infraestructura crítica[6], difusión de propaganda con fines terroristas y manipulación de la información por medio de las redes sociales. El reclutamiento por parte de actores subversivos también es una preocupación relevante, y el paro nacional de 2021 en Colombia, ejemplo de la hibridación de conflictos, ya que combinó una serie actividades que implicaron la manipulación de información, con el fin de desestabilizar al gobierno de turno. Asimismo, al vulnerar el activo estratégico más importante de un Estado: la información, ya que proporciona la base para la toma de decisiones en los ámbitos de la seguridad nacional, la política exterior y el desarrollo económico (Miguel-Gil, 2019).

Como consecuencia de lo anterior, la actual política de seguridad y convivencia ciudadana "*Garantías para la vida y la paz*", ha establecido nuevos lineamientos en la política de seguridad y defensa para abordar los desafíos emergentes en el ámbito cibernético. Reconociendo la creciente importancia de la ciberseguridad en el escenario contemporáneo, el gobierno ha puesto énfasis en la necesidad de fortalecer las capacidades cibernéticas[7] de las Fuerzas Militares (Ministerio de Defensa Nacional, 2023).

De acuerdo con lo anterior, el propósito de este artículo es analizar los desafíos a los que se enfrentan las Fuerzas Militares colombianas en términos de ciberseguridad. En este sentido, se parte de una conceptualización del ciberespacio y ciberseguridad; acto seguido se describirá el papel de las Fuerzas Militares en el ámbito cibernético. Además, se identificarán los lineamientos en términos de ciberseguridad de la política de seguridad y convivencia denominada *'Garantías para la vida y la paz*'. Por último, se abordarán los nuevos desafíos en materia de ciberseguridad a los que deben enfrentarse las Fuerzas Militares colombianas.

Metodología

Para el presente artículo se utilizó una metodología cualitativa con un enfoque descriptivo, empleando la técnica de análisis documental. Esta técnica se enfoca en la recopilación de fuentes secundarias de diversos textos, como artículos y libros, con el objetivo de seleccionar y analizar los documentos necesarios de acuerdo con los objetivos establecidos en la hoja de ruta. A partir de estas fuentes se extraen diversos elementos de análisis. El análisis documental es de gran importancia en la investigación cualitativa, ya que permite obtener nuevos conocimientos en el área de las ciencias sociales (Hernández et al., 2014).

5 Son ataques que combinan elementos digitales y físicos para lograr sus objetivos.

6 Las infraestructuras y los activos vitales para la seguridad, la gobernanza, la salud y la seguridad públicas, la economía y la confianza pública de una nación (Departamento de Defensa Estados Unidos, 2016).

7 La capacidad de un ejército de llevar a cabo operaciones defensivas y ofensivas con el fin de garantizar la protección de sistemas y datos estratégicos.

Para la búsqueda de información se emplearon los motores de búsqueda académica Scopus, Jstor y Google Académico, utilizando los siguientes términos boleanos[8]: "*Cyberspace and national security*" y "*Cyberspace and hybrid threats*". En total, se obtuvieron 803 documentos, de los cuales se seleccionaron 48 debido a su rigurosidad académica y pertinencia con el tema de investigación, mediante la sistematización realizada por la herramienta Bibliometrix.

Marco Teórico

Hacia una definición de ciberespacio

Los avances tecnológicos han representado una notable ventaja en las acciones realizadas por el ser humano, ya que han mejorado la productividad, la eficiencia y el acceso a la información. Durante la época de la Guerra Fría, marcada por la rivalidad hegemónica entre los Estados Unidos y la antigua Unión de Repúblicas Socialistas Soviéticas, se llevaron a cabo significativos avances tecnológicos que han dejado una huella en la historia de la humanidad, a través de la investigación militar (Cypher, 2007), con el propósito de mejorar los artefactos militares, entre los cuales se incluyen los sistemas de misiles guiados, satélites, aviones de combate y el desarrollo de sistemas informáticos en la década de los 60. En ese contexto, surgió el proyecto ARPANET (Advanced Research Projects Agency Network), que consistía en crear un medio seguro para las comunicaciones militares, que permitía el flujo constante de información, siendo así su objetivo primordial, ser una variable comunicativa tras un ataque nuclear, mediante la interconexión de computadoras (Tesouro y Puiggalí, 2004).

Posteriormente, en la novela de ciencia ficción de Gibson, Neuromante, aparece por primera vez el concepto de "*ciberespacio*", donde Gibson (1984) lo define como un espacio multidimensional, creado por una interconexión de computadoras a nivel global, alimentado por diferentes redes de comunicación, en la que los usuarios pueden interactuar por medio de interfaces visuales, la información fluye de manera instantánea y los usuarios se desplazan por el ciberespacio utilizando sus cerebros; al mismo tiempo, la soberanía estatal es inexistente debido a la falta de barreras geográficas, creando así una nueva realidad para el ser humano. Por otra parte, El Departamento de Defensa de Estados Unidos (2016) da una definición similar, ya que lo define como: "un dominio global dentro del entorno de la información que consiste en una red interdependiente de infraestructuras de tecnologías de la información, incluyendo internet, redes de telecomunicaciones, sistemas informáticos, procesadores y controladores" (p. 58).

Teniendo en cuenta las dos definiciones expuestas con anterioridad, se puede

8 El código booleano es una técnica de análisis de datos utilizada para identificar patrones en grandes conjuntos de datos, usando los respectivos motores de búsqueda académica (Hernández et al, 2014).

afirmar que el Ciberespacio se convierte en la piedra angular y cataliza los procesos de globalización, dado que, al ser un espacio multidimensional como producto de la interconexión global de computadoras y redes, posibilita la interacción instantánea con usuarios que habitan en distintas partes del mundo. Asimismo, desempeña un papel destacado al facilitar el intercambio de información de naturaleza académica, cultural, económica y militar.

En la década de los 90, el ciberespacio fue un medio catalizador de la globalización a medida que el acceso a internet se fue expandiendo alrededor del mundo, se fue produciendo un intercambio de información, ya que fomentaba las interacciones culturales, por medio de la moda, la comida, el lenguaje y la política. Las tecnologías de la información (TIC) han llevado a replantear el entorno social del individuo, transformándolo a un ser virtual cada vez más dependiente de medios digitales y ser un ser consumidor de cultura e información, contribuyendo así con la creación de una sociedad global conectada, interdependiente y en una constante evolución (Caro, 2003).

Sin embargo, esta nueva realidad genera potenciales amenazas, como es el caso de la ciberdelincuencia, que engloba actividades como el robo bancario, el ciberacoso y el robo de datos personales. Además, se observa la participación de grupos terroristas en el reclutamiento de menores de edad para formar parte de sus células, entre otros ejemplos preocupantes. Ante estas circunstancias, es fundamental que el individuo sea consciente de estas amenazas y tome las medidas necesarias para proteger tanto su seguridad personal como la de su familia (Trujano et al., 2009).

El ciberespacio se posiciona como un dominio no convencional de la guerra, a diferencia de los dominios tradicionales (*tierra, mar, aire y espacio*). Es importante destacar que el ciberespacio es un dominio artificial creado por el ser humano, y se considera el quinto dominio de la guerra, que responde a intereses subjetivos. Si bien el ciberespacio ha sido utilizado para acciones que han mejorado la calidad de vida de la humanidad, también se ha empleado con fines bélicos. Las acciones militares en el ciberespacio representan una amenaza aún mayor en comparación con los dominios tradicionales, dado que combinan diversas acciones que pueden afectar sistemáticamente la seguridad de individuos, empresas y Estados (Semanate y Recalde, 2023). Estas acciones son posibles debido a la interconexión de la población y al aumento en el acceso a plataformas digitales.

El ciberespacio ha adquirido un papel fundamental como el nuevo campo de batalla para las Fuerzas Militares. Sin embargo, el desempeño de las instituciones castrenses en este quinto dominio presenta grandes desafíos debido a la falta de lineamientos estatales y regulaciones jurisprudenciales claras. Al ser un entorno intangible, el ciberespacio carece de roles establecidos. Como consecuencia, representa una clara vulnerabilidad a la seguridad de los estados, por el hecho de que en este entorno se encuentran sistemas

de información de alto valor estratégico. La vulneración de estos sistemas se convierte en una gran ventaja para los actores enemigos del Estado (Aguilar, 2021).

Ciberseguridad y amenazas emergentes

Con el avance de las tecnologías y la creciente interdependencia del mundo digital, la ciberseguridad ha adquirido un rol estratégico en la seguridad de los Estados. Por tal motivo, es necesario abordar este tema de manera holística debido a la abundancia de información crítica almacenada en redes de información. El estudio y la práctica de la ciberseguridad se han convertido en un desafío fundamental para las Fuerzas Militares, representando un ámbito de análisis para los Estados modernos. Las amenazas a través de medios digitales son cada vez más frecuentes y tienen un impacto significativo en los modelos de gobernanza y en el mantenimiento del orden público de la nación.

La ciberseguridad se considera un campo estratégico que requiere la implementación de un conjunto de medidas de seguridad con el objetivo de proteger las redes de información y con el propósito de garantizar un ciberespacio libre de amenazas, preservando la confiabilidad de la información crítica y salvaguardando los intereses y la soberanía del Estado (Vargas et al., 2017). Al mismo tiempo, la ciberseguridad se orienta hacia la provisión de un entorno digital seguro que permita disfrutar de la libertad y protección de los datos personales y de la privacidad. Esto se logra mediante el uso de técnicas, como el empleo de software y sistemas de encriptación. La ciberdefensa se enmarca en el concepto de ciberseguridad desde una perspectiva estatal y se refiere a la capacidad de las Fuerzas Militares para neutralizar las amenazas presentes en el ciberespacio, con el fin de salvaguardar la soberanía digital[9] del Estado.

En el contexto colombiano, los primeros lineamientos en ciberseguridad fueron establecidos por el CONPES 3701 de 2011. Este documento tenía como objetivo establecer una estrategia nacional a largo plazo para proteger al Estado de las nuevas amenazas[10] y contrarrestar el accionar de grupos de delincuencia transnacional en el ciberespacio. Asimismo, buscaba prevenir el uso ilegal de las nuevas tecnologías de la información para crear amenazas que afectaran al bienestar de la sociedad. Es responsabilidad del Estado contar con lineamientos efectivos para hacer frente a estas nuevas amenazas a la seguridad (CONPES, 2011). En este sentido, el Ministerio de Defensa Nacional, en coordinación con las Fuerzas Armadas, ha establecido el Comando Conjunto Cibernético como entidad encargada de proteger la soberanía digital y la infraestructura crítica del país. Su función principal es la detección y prevención de ataques, recopilando y analizando información para comprender las dinámicas de los adversarios. Además, el Comando

9 Implica la capacidad de ejercer la autonomía y la autoridad en el ámbito digital, protegiendo los derechos de privacidad, seguridad y acceso a la información.

10 Los desafíos y riesgos emergentes que afectan la seguridad de un país en el ámbito interno o externo. Estas amenazas van más allá de los tradicionales conflictos militares.

Conjunto Cibernético lleva a cabo operaciones ofensivas y defensivas para proteger los intereses del Estado. Adicionalmente, el Comando Conjunto Cibernético promueve la cooperación con entidades gubernamentales, el sector privado y la sociedad civil con el objetivo de fortalecer la seguridad cibernética en el país (Cujabante et al., 2020).

Por otro lado, una amenaza híbrida se caracteriza por combinar varios dominios de la guerra de manera sincrónica. Principalmente, se asocia con el ciberespacio y tiene como objetivo atacar activos estratégicos del Estado mediante tecnologías físicas o digitales. Sin embargo, las amenazas híbridas pueden abarcar diversas situaciones, desde ataques terroristas y ciberataques hasta acciones de grupos delictivos armados y operaciones militares encubiertas, entre otras.

Es importante destacar que las amenazas híbridas pueden ser perpetradas tanto por Estados como por actores subestatales ilegales, quienes pueden utilizar diversas formas de violencia, ya sea física o psicológica (Cajas, 2022). Aunque el término "*guerra híbrida*" se utiliza a menudo como sinónimo de amenaza híbrida, desde una perspectiva académica y militar no se pueden considerar iguales. La guerra híbrida implica la combinación de acciones convencionales[11] y no convencionales[12] por parte de los ejércitos estatales contra grupos terroristas, que pueden recurrir a ciberataques, desinformación o propaganda ideológica dirigida a la población civil. Por lo general, estos grupos están respaldados por un Estado (Bartolomé, 2019). La diferencia fundamental radica en que la guerra híbrida se centra en un conflicto armado, mientras que la amenaza híbrida se refiere a la utilización de diferentes métodos para socavar la estabilidad y la seguridad del Estado.

En este contexto, el rápido avance de las capacidades tecnológicas ha dado lugar a nuevos conflictos en los que el Derecho Internacional Humanitario no ha evolucionado al mismo ritmo de las guerras. En particular, el ciberespacio representa un desafío para las Fuerzas Militares, ya que va más allá de la noción tradicional de seguridad al no poseer una soberanía física como campo operativo. Por otro lado, el ecosistema de la información está experimentando una completa digitalización de la sociedad, impulsada por el uso de las redes sociales; esto ha llevado a una velocidad sin precedentes en la difusión de noticias. La desinformación se está convirtiendo en elementos constantes que maximizan la desconfianza en las instituciones gubernamentales. La naturaleza de la guerra y los conflictos han experimentado una constante evolución desde la Segunda Guerra Mundial, y han dado lugar a la aparición de un nuevo dominio: el ciberespacio. En este dominio han surgido amenazas híbridas en las que la población civil se encuentra cada vez más involucrada. Por último, los conflictos actuales reflejan un cambio

11 Se refieren a las estrategias y tácticas tradicionales empleadas por las fuerzas armadas estatales. "Capaces de llevar a cabo operaciones utilizando armas no nucleares, acciones distintas de las designadas como fuerzas de operaciones especiales" (Departamento de Defensa Estados Unidos, 2016).

12 Son estrategias en donde la amenaza es irregular, se realizan tácticas y métodos de combate. Estas acciones incluyen la guerra de guerrillas, terrorismo y ciberataques.

generacional y las aspiraciones cambiantes de los Estados en el sistema internacional. Ya no se trata únicamente de una lucha ideológica entre el comunismo y el capitalismo en el contexto de la Guerra Fría, sino que la globalización y la interdependencia entre regiones del mundo han generado nuevas aspiraciones en las que el Estado ya no es el único actor relevante.

La teoría del complejo de seguridad

La seguridad es entendida desde el realismo como concepción netamente desde el campo militar y los intereses estatales. Para los críticos de las teorías tradicionalistas[13], como el autor Cepik (2001), "Seguridad nacional se entiende aquí una condición relativa de protección colectiva e individual de los miembros de una sociedad frente a amenazas plausibles a su supervivencia y autonomía" (p.3). Desde un enfoque estructuralista, la seguridad no solo corresponde al ámbito militar; se enmarca en toda situación que ponga en riesgo la supervivencia del individuo.

La seguridad, como objeto de estudio en el campo de las relaciones internacionales, comenzó a desarrollarse después de la finalización de la Segunda Guerra Mundial. La unidad de análisis en este campo se centra en la amenaza a la fuerza y en la fuerza como instrumento defensivo, adoptando una perspectiva Estado-céntrica influenciada por el realismo clásico (Bárcena, 2000). Como resultado, surgieron los estudios de seguridad con un enfoque predominantemente militar. Desde esta perspectiva, la seguridad se consideraba como una fuerza disuasoria para cada Estado en el sistema internacional.

La teoría del complejo de seguridad se enmarca en dos corrientes de pensamiento: los estudios de seguridad desarrollados por la Escuela de Copenhague y la teoría del sistema internacional y la orden mundial propuesta por la Escuela Inglesa, en la cual se produce una convergencia entre el realismo y el liberalismo (Sisco y Chacón, 2004). En la década de los 90, Barry Buzan, en la Universidad de Copenhague, desarrolló la teoría del complejo de seguridad ofreciendo una noción contemporánea de los estudios de seguridad. El nuevo escenario del sistema internacional posterior a la Guerra Fría amplía la concepción tradicional de seguridad, y debe ser analizado considerando la participación de diversos actores en la sociedad internacional, como las multinacionales, ONG, organizaciones internacionales, movimientos sociales y organizaciones terroristas. En este sentido, la seguridad internacional no debe limitarse únicamente al análisis de los Estados como objeto principal, ya que la seguridad abarca más allá que las amenazas militares. Existen diversas dinámicas subestatales que deben ser consideradas, dado que el sistema de seguridad internacional se encuentra interconectado entre todos los actores que conforman la sociedad internacional (Otálvaro, 2004).

13 Las teorías tradicionalistas de las relaciones internacionales son enfoques teóricos desarrollados en el siglo XX, donde la unidad de análisis son los Estados y se destaca la competencia por el poder.

La teoría del complejo de seguridad amplía la visión tradicional de la seguridad al incorporar dimensiones adicionales, como la económica, la ambiental, la social y la ontológica. Estas dimensiones interactúan entre sí y afectan la estabilidad de los actores dentro del marco de la teoría del complejo de seguridad. En esta teoría, la premisa central es que los problemas de seguridad no deben ser analizados de forma aislada, sino que requieren un enfoque holístico que considere las interconexiones y relaciones entre las diversas dinámicas de la seguridad. Buzan y Wæver (2003), argumentan que comprender las distintas dimensiones de la seguridad es esencial para promover la paz, la estabilidad y el desarrollo en un mundo cada vez más complejo y globalizado. Debido a esto, es necesario hacer una comprensión completa de los diferentes aspectos y dimensiones de la seguridad, los cuales se pueden ver clasificados y definidos en la Tabla 1.

TABLA 1. Niveles de seguridad

Niveles de seguridad	Característica
Sistema Internacional	Ámbito global.
Subsistemas	Interdependencia entre unidades regionales. Ejemplo, la Unión Europea.
Unidades	Estados debido a que son actores que poseen independencia y coherencia.
Subunidades	Grupos dentro de la Unidad, que tienen influencia positiva o negativa (delincuencia organizada, empresas e instituciones).
Individuos	Actúan en el sistema, debido a su racionalidad.

Nota. La tabla muestra los niveles de seguridad internacional
Fuente: Elaboración propia, con datos del libro Regions and Powers the Structure of International security (Buzan y Wæver, 2003)

La teoría del complejo de seguridad de Buzan se centra en los subsistemas como nivel de análisis y proporciona una perspectiva de investigación que abarca las dimensiones política, militar y social. El autor destaca la importancia de los subsistemas regionales al argumentar que las integraciones intrarregionales de los Estados poseen cierta autonomía en relación con el sistema internacional. Esto se debe a que las interacciones entre los

Estados dentro de una integración son más intensas que las interacciones con naciones externas (Buzan y Wæver, 2003).

El desarrollo tecnológico desempeña un papel determinante en las operaciones militares, ya que brinda un mayor número de opciones y estrategias operativas. No obstante, es fundamental comprender las dinámicas de las amenazas en el entorno digital. En este sentido, la teoría del complejo de seguridad amplía la concepción clásica al reconocer que las amenazas ya no provienen únicamente de actores beligerantes estatales, sino que han adquirido un carácter multidimensional. La seguridad multidimensional ha sido adoptada por los países del hemisferio sur, especialmente después de la Declaración de Seguridad de las Américas en 2003. En este enfoque, la seguridad abarca aspectos económicos, políticos, sociales y ambientales. Se han identificado amenazas no tradicionales, como la delincuencia organizada transnacional, el tráfico de armas y de drogas, el lavado de dinero, las pandemias y los ataques cibernéticos, entre otras. Por lo tanto, es necesario abordar estas amenazas no tradicionales de manera integral y cooperativa entre los Estados del hemisferio sur (Gallardo, 2019).

Actualmente, el ciberespacio se ha convertido en un entorno propicio para actores involucrados en actividades ilícitas, debido a su fácil acceso y bajo riesgo de detección. Dado que el ciberespacio es un dominio abstracto, las agencias de inteligencia y seguridad de los Estados enfrentan dificultades para garantizar la seguridad total de la infraestructura crítica. Por otro lado, la delincuencia organizada transnacional se define como un grupo estructurado que comete múltiples delitos y traspasa las fronteras físicas de un Estado, generando recursos a partir de afectaciones internacionales (Unodc.org., 2010). Sin embargo, se considera una subunidad, ya que es un actor que influye negativamente dentro de la unidad estatal y subregional, afectando a los individuos. Esto da lugar a la hibridación del conflicto, que se caracteriza por la combinación de daños reales y virtuales, así como por su naturaleza compleja y multidimensional, amenazando directamente la seguridad interna de los Estados y debilitando el Estado de Derecho (Bartolomé, 2019).

La ubicación geoestratégica de Colombia la hace vulnerable a los efectos directos de la delincuencia organizada transnacional. Dado que el país tiene acceso tanto al océano Atlántico como al Pacífico, además cuenta con fronteras porosas con Ecuador y Venezuela, lo que lo convierte en un territorio atractivo para actividades como el tráfico de armas y de drogas. Estas acciones tienen un impacto negativo en el orden público, ya que se ha observado un recrudecimiento de la violencia atribuido a estos fenómenos de crimen transnacional. Los delincuentes se aprovechan del ciberespacio para llevar a cabo transacciones en línea y establecer comunicaciones con actores aliados, aprovechando la facilidad de acceso y el anonimato que ofrece el entorno digital (Erazo et al., 2022).

En este contexto, la cooperación internacional se vuelve esencial para hacer frente al modus operandi de los actores ilegales, por medio de alianzas entre las fuerzas

militares que desempeñan un papel clave en la implementación de operaciones conjuntas multidominio, centradas en el desarrollo de capacidades cibernéticas. Las capacidades cibernéticas permiten recopilar información en tiempo real sobre los adversarios y llevar a cabo acciones que mitiguen este fenómeno delictivo (Miranzo, M., & Del Río, 2014). La colaboración entre países se vuelve crucial para intercambiar información y coordinar esfuerzos en la lucha contra la delincuencia transnacional, tanto en el ciberespacio como en el mundo físico. A través de estas acciones y estrategias se busca contrarrestar los efectos negativos de la delincuencia en la seguridad y estabilidad de Colombia.

Rol de las Fuerzas Militares colombianas en el dominio ciber

A comienzos del siglo XX, las guerras se libraban principalmente en los dominios tradicionales, como lo son la tierra y el mar. Sin embargo, a lo largo de los siglos XX y XIX, los avances tecnológicos introdujeron en las Fuerzas Militares tres nuevos dominios (aire, espacio y ciberespacio), lo que cambió la lógica del planteamiento y las operaciones relacionadas con la seguridad y defensa de las naciones. El papel de las instituciones militares en el ciberespacio está estrechamente vinculado a una lógica de seguridad global, dada la interconexión mundial y la ausencia de barreras físicas. Los activos estratégicos de los Estados se encuentran en el ciberespacio, así como también las actividades comerciales. Por lo tanto, la seguridad digital requiere una protección global y la cooperación militar se vuelve esencial para hacer frente a las amenazas híbridas. Las Fuerzas Militares colombianas tienen la responsabilidad de proteger la infraestructura crítica y garantizar la seguridad digital (Poveda y Álvarez, 2022).

En Colombia, las Fuerzas Militares son las instituciones encargadas de velar por la protección de la soberanía, el territorio y la población; asimismo, deben contar con capacidad de adaptabilidad al contexto nacional y global, para poder llevar a cabo su misión constitucional consagrada en el artículo 217 de la Constitución Política (1991):

> *"La Nación tendrá para su defensa unas Fuerzas Militares permanentes constituidas por el Ejército, la Armada y la Fuerza Aérea. Las Fuerzas Militares tendrán como finalidad primordial la defensa de la soberanía, la independencia, la integridad del territorio nacional y del orden constitucional"* (Pag, 53).

De acuerdo con lo anterior, es responsabilidad constitucional de las Fuerzas Militares garantizar el orden público en los cinco dominios, especialmente en el ciberespacio, que se ha convertido en un nuevo campo de conflictividad. Es necesario que las Fuerzas Militares se adentren por completo en este dominio tan complejo. Las instituciones castrenses deben adaptarse rápidamente a este escenario para prepararse y hacer frente a futuras confrontaciones o afectaciones a la soberanía y los intereses de la nación. Estos desafíos representan una tarea considerable tanto en términos de seguridad informática como en la toma de decisiones, abarcando desde el procesamiento y análisis de la información hasta la anticipación de las acciones de adversarios estatales y no

estatales, especialmente cuando la seguridad digital se encuentra bajo ataque.

TABLA 2. Unidades Cibernéticas de las Fuerzas Militares

Fuerza Militar	Unidades Cibernéticas
Ejército Nacional	Comando de Apoyo Operacional de Comunicaciones y Ciberdefensa (CAOCC)
Armada Nacional	Dirección Cibernética Naval
Fuerza Aérea colombiana	Dirección Cibernética Aérea

Fuente: Elaboración propia, con información extraída del artículo "*Amenazas cibernéticas a la seguridad y defensa nacional. Reflexiones y perspectivas en Colombia* (Realpe y Cano, 2020)"

Las unidades militares mencionadas en la tabla anterior desempeñan funciones interinstitucionales con el propósito de proteger la infraestructura crítica de la nación en el ciberespacio. Su objetivo es avanzar hacia el desarrollo e implementación de planes de protección para activos estratégicos. Como resultado se han establecido acuerdos entre diferentes actores del país, a fin de cooperar y compartir información sobre amenazas, para prevenir su materialización. No obstante, a pesar de las acciones llevadas a cabo por estas unidades militares cibernéticas, se ha evidenciado la falta de directrices concretas que describan de manera detallada las posibles amenazas a las que las Fuerzas Militares podrían enfrentarse en el ámbito ciberespacial. Por lo tanto, resulta necesario establecer marcos de acción que permitan alcanzar los objetivos nacionales en este ámbito (Realpe, 2019).

Lineamientos en términos de ciberseguridad de la Política de seguridad, defensa y convivencia ciudadana "*Garantías para la vida y la paz*"

El 25 de abril de 2023, el ministro de Defensa, Iván Velázquez, lanzó los lineamientos de la Política de seguridad y defensa '*Garantías para la vida y la paz*'. Estos lineamientos establecen los objetivos y principios que guían las acciones y estrategias de seguridad durante los cuatro años de gobierno. En general, se abordan aspectos como la protección de la vida, la integridad territorial y de los ciudadanos, así como del medio ambiente, la promoción de la paz y la lucha constante contra amenazas internas y externas (Ministerio de Defensa Nacional, 2023). Esta política de seguridad tiene una característica diferenciadora y es que por primera vez se tiene un abordaje concreto sobre las capacidades defensivas y ofensivas que deben tener las Fuerzas Militares en el ciberespacio. En los últimos años, el uso de las herramientas digitales se ha masificado; los actores privados, como las organizaciones gubernamentales, guardan información estratégica en sus redes informáticas. En caso de un ciberataque, esta información puede afectar su funcionamiento y perjudicar las dimensiones políticas y económicas de la

nación (Villalba y Corchado, 2017). Por ello, nace la necesidad de proteger la soberanía en el espacio ciber.

Según datos del Centro Cibernético de la Policía en 2022, los ciberataques a infraestructura crítica y redes informáticas aumentaron un 27,7%; si no se tiene un lineamiento concreto sobre la prevención de crímenes y ataques en el domino ciber, estas cifras van a seguir aumentado, afectando considerablemente la seguridad de las personas (Policia.gov.co, 2023). Cabe resaltar que las Fuerzas Militares, desde el año 2011, están en un proceso de innovación estratégica con el fin de anticiparse a las amenazas del futuro. Sin embargo, sus capacidades de acción en dominio ciber son completamente nulas por el hecho de que solo se limitan a actividades de recolección de información, con el objetivo de prevenir las amenazas que puedan volverse tangibles (Rojas, 2017).

Los lineamientos sobre la innovación de capacidades en el ciberespacio se encuentran abordados en el tercer objetivo específico de la Política de seguridad y defensa, el cual es *'Salvaguardar la integridad territorial, la soberanía, la independencia nacional y el orden constitucional*'. Esto implica proteger y preservar la integridad de las fronteras y el territorio de agresiones que puedan afectar la soberanía de la nación en los diferentes dominios. Al mismo tiempo, se busca trabajar en pro de mantener la estabilidad y el orden constitucional, garantizando el cumplimiento de los derechos fundamentales de los ciudadanos (Ministerio de Defensa Nacional, 2023).

El ciberespacio ha sido durante mucho tiempo un campo de batalla abstracto, donde las redes terroristas y delincuenciales representan una amenaza para la soberanía digital. Por lo tanto, resulta fundamental contar con capacidades militares que se enfoquen en prevenir cualquier tipo de amenaza cibernética que pueda afectar la soberanía nacional y los principios constitucionales, además de proteger la infraestructura crítica y defenderla de cualquier perturbación (Ministerio de Defensa Nacional, 2023). Esto permite al país estar preparado y responder de manera efectiva ante posibles ciberataques, asegurando así la soberanía digital. Además, esto demanda la construcción y fortalecimiento de nuevas capacidades cibernéticas, como la ciberinteligencia y las operaciones cibernéticas defensivas y ofensivas, para mantener una fuerza dinámica y lista para satisfacer los requisitos de seguridad y defensa del pueblo colombiano (Mozo y Ardila, 2022).

Por otro lado, Colombia, al ser el principal socio de la OTAN (*Organización del Tratado del Atlántico Norte*) en América Latina, debe fortalecer la cooperación en el ámbito militar cibernético. La OTAN, desde 2006, ha desarrollado capacidades militares cibernéticas enfocadas en la defensa colectiva de sus miembros, centrándose en la protección de redes informáticas, sistemas de información e infraestructura crítica. Para ello, ha establecido el Centro de Operaciones Cibernéticas con el objetivo de anticipar amenazas. Así mismo, lleva a cabo ejercicios militares en el ciberespacio, en colaboración con sus miembros. Igualmente, mantiene una estrecha colaboración con el sector privado para compartir información y mejorar la seguridad cibernética (Fuente, 2022).

En este contexto, es fundamental que la OTAN capacite al personal militar colombiano y realice ejercicios militares en el ciberespacio de manera conjunta. De esta manera, Colombia podrá desarrollar sus capacidades en ciberdefensa, ciberinteligencia y ciberpatrullaje. Esto permitirá fortalecer la seguridad y protección de la infraestructura crítica del país. La cooperación entre la OTAN y Colombia en estas áreas será de gran importancia para enfrentar los desafíos cibernéticos ante la implementación de nuevas herramientas digitales en un futuro cercano.

Nuevos desafíos en términos de ciberseguridad par las Fuerzas Militares colombianas

El desarrollo tecnológico nos ha vuelto interdependientes de los medios digitales, lo cual ha impulsado transformaciones en los ámbitos económico, cultural y político de la sociedad internacional. Sin embargo, junto con estos avances también han surgido problemas complejos para la seguridad de los Estados, como es el caso del ciberespacio. La ciberseguridad se ha convertido en objeto de estudio primordial para las Fuerzas Militares colombianas, dado que las amenazas en el espacio cibernético representan desafíos que requieren estrategias por parte de los organismos de inteligencia. Los nuevos desafíos derivados del dominio cibernético incluyen actividades delictivas, guerra cibernética y operaciones de información, con el fin de desestabilizar al gobierno y realizar ciberataques contra la infraestructura crítica mediante el uso de inteligencia artificial.

Ciberguerra

A comienzos del siglo XXI, con la popularización de internet y su masivo uso por millones de personas, el ciberespacio se convirtió en un escenario idóneo para la materialización de nuevas amenazas. Entre estas se incluyen la desinformación, los ataques a infraestructura crítica y el terrorismo. Además, los actores estatales, e insurgentes, han innovado en nuevas modalidades de acciones bélicas en un escenario físico, aprovechando el espacio cibernético. Según Ferrero (2013), esto ha generado un nuevo campo de batalla, en el que aquellos con mayores recursos tecnológicos tienen una ventaja militar. Como resultado, se ha cuestionado la eficacia de las capacidades militares disuasorias y defensivas tradicionales. Por tanto, los Estados se han visto obligados a incrementar sus capacidades militares cibernéticas, tanto defensivas como ofensivas, debido a la alta probabilidad actual de sufrir ciberataques. Estos ataques permiten al enemigo obtener información valiosa y estratégica sobre las capacidades militares del Estado colombiano.

La ciberguerra se caracteriza como un conflicto entre entidades políticas y ejércitos tecnológicamente avanzados, quienes a menudo poseen habilidades especiales en el ámbito cibernético. En ocasiones, también puede involucrar actores asimétricos. Estos conflictos se desarrollan de manera aislada y se centran en acciones cuyo propósito es

perturbar las redes y obtener información de los enemigos. Una de las características distintivas de la ciberguerra es la dificultad para identificar y localizar al enemigo, debido a que un ataque se puede hacer desde cualquier parte del mundo, ya que solo se necesita una sencilla conexión a internet mediante el uso de virus informáticos que pueden robar, bloquear o eliminar información (Lodeiro, 2011).

Los conflictos en el ciberespacio se desarrollan de manera aislada, y se refieren a las acciones realizadas con el propósito de perturbar las redes y obtener información de los enemigos, causando daños físicos tales como impacto en la economía local e interrupción en las instituciones gubernamentales, afectando a diferentes sectores de la sociedad, convirtiéndose en una amenaza tanto para la paz nacional como internacional. Por esta razón, se reconoce al ciberespacio como un arma presente y se espera que su uso aumente en el futuro (Mancera, 2014).

TABLA 3. Clasificación de la autoría de los ciberataques

Clasificación de los ciberataques	Característica
Patrocinados por Estados	Estos ataques son llevados a cabo muchas veces por organismos de inteligencia y contrainteligencia, los cuales cuentan con equipos tecnológicamente avanzados, con el objetivo de robar información, sabotear las infraestructuras críticas y manipular la información que llegará a los medios de comunicación.
Ataques de delincuencia organizada	Los ciberataques llevados a cabo por la delincuencia organizada se caracterizan por su interés económico, por medio de robo de información bancaria y secuestro de datos, ya que emplean una variedad de herramientas cibernéticas, como lo son phishing, malware o ransomware.
Terrorismo a partir de ideología política	Los ciberataques realizados por grupos terroristas con ideología política se caracterizan por el empleo de plataformas digitales para difundir información, reclutar seguidores y coordinar ataques, tales como sabotear información con el fin de desestabilizar gobiernos, robos en línea y ataques a infraestructura crítica.

Fuente: Elaboración propia, con información extraída del artículo "*La Ciberguerra, génesis y evolución* (Ferrero, 2013)"

La ciberguerra plantea un desafío significativo en términos de seguridad para las Fuerzas Militares colombianas, debido a su alta dependencia de las redes de información. Un ciberataque exitoso tiene el potencial de interrumpir o causar graves daños a las infraestructuras críticas, afectando la capacidad operativa de las Fuerzas

Militares. Ante este desafío, es fundamental que las Fuerzas Militares colombianas actúen de manera proactiva y adopten medidas defensivas concretas para fortalecer los sistemas de ciberseguridad. Esto implica la detección y respuesta efectiva a los ataques cibernéticos. Además, deben desarrollar estrategias específicas y líneas de acción que les permitan aumentar sus capacidades tanto defensivas como ofensivas en el ciberespacio, contrarrestando cualquier perturbación que afecte su seguridad (Villanueva, 2015).

Una estrategia ofensiva busca acceder a la información y sistemas que protegen las infraestructuras críticas del adversario. Esto se logra mediante el uso de diversas ciberarmas como, por ejemplo, virus informáticos, gusanos (worm), ransorware y botnets. Usados con el objetivo de obtener información estratégica del adversario y neutralizarlo. Cabe destacar que estas operaciones ofensivas pueden llevarse a cabo tanto en conflictos con actores estatales como con actores asimétricos.

Por lo tanto, la seguridad de la información es parte de cada individuo, entidad o Estado; es por eso que se debe tener cuenta lo que dicen (Chaparro et al., 2020) en su artículo, quienes mencionan que:

> "*Quien controle los canales por donde circula la inmensa cantidad de datos y pueda hacerse garante de los flujos de información, tiene en su poder la ventaja de saber con antelación qué contienen esos datos, y con ello darle el uso comercial o estratégico que le favorezca*" (pág, 34).

Por otro lado, una estrategia defensiva se enfoca en proteger los propios sistemas de información mediante la implementación de medidas como firewalls, antivirus, sistemas de detección de intrusiones y ciberpatrullaje. Asimismo, es importante fortalecer las unidades de ciberinteligencia para proteger los sistemas contra amenazas externas y garantizar la protección de las infraestructuras críticas. Es crucial destacar que las capacidades disuasorias en este ámbito son inciertas debido al anonimato de los actores involucrados y a las complejidades asociadas a la identificación y localización de los mismos. Esto plantea desafíos significativos para garantizar la seguridad en el ciberespacio (Caro, 2011).

Operaciones de información con el fin de desestabilizar al Gobierno Nacional por medio de noticias falsas

Las operaciones de información son acciones estratégicas que se llevan a cabo con el objetivo de persuadir e influir en los comportamientos de una población específica. El uso de las tecnologías de la información (TIC) ha provocado cambios significativos en la forma de comunicar la información. Actualmente los medios tradicionales, como la televisión y la radio, han quedado en el pasado; asimismo, el auge de las redes sociales y otros medios digitales, que son utilizados para distorsionar los contenidos reales. Además, los propios cibernautas contribuyen a tergiversar la información. De esta manera surgen

las *fake news* o noticias falsas, las cuales han sido catalogadas como un fenómeno de gran importancia en el contexto de la seguridad nacional del país (Betancur, 2004).

Las noticias falsas son construcciones de información deliberadamente engañosa. Su objetivo principal es presentar hechos verídicos con el propósito de engañar, crear confusión y manipular a sectores de la sociedad. Asimismo, Estas noticias son difundidas a través de artículos en línea, videos e imágenes manipuladas que se publican en redes sociales con el fin de generar polémica y desacreditar a personas e instituciones gubernamentales, a menudo con el objetivo de obtener beneficios políticos y económicos. Las noticias falsas se difunden con rapidez por medio de la reproducción de estas en redes digitales. Así pues, el propósito de la rápida reproducción es hacer parecer verídica la información, apelando a las emociones y valores ideológicos de los individuos. Por esta razón, todos hemos caído alguna vez en la trampa de la desinformación (Chavero & Intriago, 2021).

Las noticias falsas han demostrado su capacidad para desestabilizar gobiernos por medio de la generación de revueltas y protestas violentas en varias ocasiones en Colombia, como consecuencia de la manipulación de la opinión pública y la creación de narrativas engañosas y disruptivas que incitan a la reacción violenta de la sociedad, aumentando la desconfianza en las instituciones, además de polarizar el debate político y generar un clima de incertidumbre, por medio de las redes sociales, facilitando su viralización (Castillo et al.,2021).

Las noticias falsas se caracterizan por seleccionar selectivamente la realidad y generar incertidumbre y pánico en la población. Sin embargo, la generación de noticias falsas crea una arquitectura persuasiva con el objetivo de manipular los imaginarios sociales y crear climas de desinformación. Los jóvenes, en particular, son el grupo más expuesto a este fenómeno, ya que pasan más tiempo conectados y tienden a adherirse a grupos en internet. Como resultado, pocas veces contrastan la información que reciben en sus teléfonos móviles, lo que los hace especialmente vulnerables a la propagación de noticias falsas (Cano,2022), siendo usados como herramienta desestabilizadora de la sociedad, como sucedió en el paro nacional de 2021.

El paro nacional de 2021 en Colombia constituye un ejemplo de la utilización de noticias falsas con el propósito de desestabilizar el gobierno. En particular la difusión de noticias falsas que afirmaban que, dentro de las instalaciones de la Alcaldía de Cali, se estaban reteniendo personas ilegalmente y sometiéndolas a actos de tortura. En respuesta a esta situación, la Alcaldía de Cali emitió un comunicado en el cual rechazó este tipo de afirmaciones, que buscaban generar respuestas de hostilidad por parte de los ciudadanos hacia el gobierno (Eltiempo.com, 2021).

Las Fuerzas Militares deben seguir una serie de lineamientos con el objetivo de evitar la desestabilización del Gobierno mediante noticias falsas. Es fundamental

mantener una vigilancia constante en las redes sociales para identificar cualquier evento que pueda ser materializado. Asimismo, se debe recolectar información de inteligencia, además de realizar un monitoreo de cuentas sospechosas en redes sociales, por las cuales inciten cualquier tipo de perturbación al orden público (González y Martinez, 2021). Es deber constitucional de las Fuerzas Militares garantizar la protección de las instituciones democráticas.

Ciberataques a infraestructura crítica con inteligencia artificial

La infraestructura crítica se entiende por un conjunto de activos físicos, controlados por sistemas computacionales altamente complejos; este conjunto de activos es parte esencial de la sociedad moderna, porque son servicios indispensables para los ciudadanos, por ejemplo: Las redes eléctricas, servicios hospitalarios, las redes de comunicaciones y los servicios financieros E.T.C. En dado caso de que llegaran a sufrir un ataque, generaría pérdida de vidas humanas, como resultado de lesiones que se produzcan debido al mal funcionamiento de los servicios esenciales; impacto económico, como resultado de la alteración de los mercados, y el impacto en las instituciones públicas, ya que afectaría su capacidad de brindar atención oportuna a los ciudadanos (Anabalón & Donders, 2014).

Por otro lado, en los últimos años se ha venido avanzando en temas de inteligencia artificial (IA) y se ha incorporado a la vida cotidiana de cada uno, mediante los asistentes digitales, robots que los usamos en nuestras tareas domésticas; se comienzan a desdibujar las líneas entre lo humano y lo digital. La inteligencia artificial nos ha facilitado nuestro día a día, sin embargo, actores con fines maliciosos están utilizando estas nuevas tecnologías para atacar la infraestructura crítica del Estado colombiano (Cano, 2022).

De acuerdo con lo anterior, las infraestructuras críticas han sido objeto de ciberataques mediante el uso de inteligencia artificial. Esta tecnología se emplea para generar algoritmos de aprendizaje automático que se adaptan a los sistemas de defensa, analizando patrones e identificando las vulnerabilidades de estos sistemas de defensa de infraestructura crítica; esto permite a los atacantes eludir las defensas de seguridad y propagar *malware* de manera más efectiva, aprovechando engaños y manipulaciones que van más allá de las vulnerabilidades conocidas hasta hace poco, que pueden mutar a un contexto en el que se utilicen armas autónomas altamente especializadas que tengan la capacidad de adaptar y modificar sus estrategias a medida que sean detectadas (De la Peña & Granados, 2021).

Además, la capacidad de la inteligencia artificial para procesar y analizar grandes volúmenes de datos también se utiliza en los ataques de denegación de servicio (DDOS). Los atacantes crean algoritmos de IA para coordinar ataques masivos que sobrecarguen los servidores y redes de infraestructura crítica, interrumpiendo su funcionamiento normal y causando daños significativos en la sociedad.

Por ejemplo, en el año 2021, una publicación de la revista Semana (2021) reveló un informe en que ladrones utilizaron drones equipados, diseñados con inteligencia artificial para llevar a cabo un robo. En este caso, los delincuentes lograron suplantar la voz del director de un banco en Emiratos Árabes Unidos mediante el uso de tecnología de IA. Además, activaron un malware diseñado para enviar correos electrónicos que contenían enlaces maliciosos. Estas acciones facilitaron el robo de una cantidad estimada en 30 millones de euros. Este robo destaca cómo los avances en la inteligencia artificial pueden ser aprovechados por los delincuentes para llevar a cabo acciones delictivas cada vez más sofisticadas sin que se tengan indicios de los responsables, debido al anonimato que tienen los actores en el ciberespacio. Asimismo, este robo es un ejemplo de la vulnerabilidad de nuestras infraestructuras críticas ante ataques por medio de IA.

Por otro lado, las Fuerzas Militares colombianas deben tener la capacidad de innovar en inteligencia artificial como herramienta de protección de los sistemas de infraestructura crítica. La inteligencia artificial es capaz de analizar grandes volúmenes de información, identificando patrones sospechosos y anómalos en los sistemas de protección, lo cual es crucial para la detección temprana de posibles amenazas. Además, permite minimizar los riesgos al analizar, anticipar y neutralizar amenazas cibernéticas, proporcionando información de suma importancia para la protección de los sistemas de infraestructura crítica por medio de respuestas automatizadas (Semanate y Recalde, 2023). Es esencial tener en cuenta que el uso de la inteligencia artificial en la defensa de la infraestructura crítica debe ir de la mano con políticas estatales de seguridad cibernética. Esto implica contar con personal capacitado en el manejo de las nuevas tecnologías, además de fomentar la cooperación entre los sectores militar, gubernamental y privado. Lamentablemente, en Colombia, esta colaboración para compartir información, estrategias y trabajar conjuntamente en la protección de la infraestructura crítica es inexistente. Asimismo, la inteligencia artificial representa una ventaja potencial para salvaguardar los activos estratégicos del país, desarrollando sistemas de defensa sólidos.

Conclusiones

En Colombia, las Fuerzas Militares son la institución encargada de salvaguardar la soberanía, independencia, territorio y la población, tal como se establece en el artículo 217 de la Constitución Política de 1991. Como parte de su misión constitucional, también desempeñan un papel fundamental en la definición de prioridades y directrices de las políticas de seguridad y defensa en colaboración con el Ministerio de Defensa. En el contexto actual, el surgimiento de nuevas amenazas pone en riesgo la soberanía digital. Por esta razón, es importante que los lineamientos de la política de seguridad y defensa "*Garantías para la vida y paz*" aborden estas cuestiones y actualicen las políticas adoptadas por el CONPES 3701 de 2011, garantizando la protección de la soberanía digital. En este sentido, los resultados del presente artículo están en línea con el enfoque presentado en el texto "*Ciberseguridad y ciberdefensa en Colombia: un posible modelo a seguir en las relaciones cívico-militares*". Este artículo destaca el papel constitucional

de las Fuerzas Militares en la protección del entorno digital del Estado colombiano, demostrando la intención del país de fortalecer y mejorar sus capacidades cibernéticas.

Actualmente en Colombia se observa una amplia diversidad de actores, incluyendo partidos políticos, movimientos sociales y grupos guerrilleros; estos actores aprovecharon las dinámicas sociales originadas por la recesión económica y la crisis del *Covid-19*. A través de las redes sociales, difundieron noticias falsas con el objetivo de desestabilizar las instituciones gubernamentales, manipulando a los sectores de la sociedad más joven y generando protestas violentas. Como consecuencia de lo anteriormente expuesto, estos sucesos reflejan la importancia de abordar de manera efectiva el fenómeno de las noticias falsas como un desafío a la seguridad nacional.

En este sentido, los resultados del presente artículo respaldan el enfoque presentado en el texto '*Prospectiva de ciberseguridad nacional para Colombia a 2030*', el cual enfatiza el rol de las noticias falsas en la desestabilización del gobierno de Iván Duque mediante la manipulación de las masas. Estos hallazgos demuestran la necesidad de implementar estrategias eficaces para abordar el fenómeno de las noticias falsas y así mantener la estabilidad y la seguridad en el país. Es fundamental destacar que la gestión de las noticias falsas y la protección de la sociedad frente a la manipulación de masas no deben recaer exclusivamente en la Fuerza pública. Enfrentar las ciberamenazas y promover la seguridad digital requiere la colaboración de múltiples actores y la implementación de una estrategia integral.

Por otro último, no hay que descartar las posibilidades de que ocurra un ciberataque a un objetivo estratégico; asimismo, hace necesario aumentar la capacidad de anticipación y disuasión frente a las capacidades de acción que puedan tener los adversarios. Tomemos como ejemplo los ataques a la infraestructura crítica de Estonia y Estados Unidos. Este último reveló las fragilidades de Estados Unidos, que cuenta con un comando cibernético que posee todas las capacidades ofensivas y defensivas para proteger la infraestructura crítica que afecta el dinamismo social y económico del país. Como consecuencia de lo anterior, Colombia está expuesta a múltiples riesgos de ciberataques. En caso de un ataque a la infraestructura crítica, es necesario que Colombia establezca alianzas estratégicas, como la OTAN, para ser capaz de proteger tanto la infraestructura crítica como las Fuerzas Militares, en lugar de depender exclusivamente de actores privados. Esto es crucial, ya que garantizar la integridad del territorio y la seguridad de los ciudadanos es un deber constitucional de las Fuerzas Militares.

Declaración de divulgación

Los autores declaran que no existe ningún potencial conflicto de interés relacionado con el artículo.

Financiamiento

Los autores no declaran fuente de financiamiento para la realización de este artículo.

Sobre los autores

Jeison Stiven Peña Suárez es estudiante de Gobierno y Relaciones Internacionales de la Universidad Santo Tomas (Colombia).

https://orcid.org/0009-0003-1399-6433-Contacto:jeisonpena@usantotomas.edu.co

Referencias

Aguilar Antonio, J. M. (2021). Retos y oportunidades en materia de ciberseguridad de América Latina frente al contexto global de ciberamenazas a la seguridad nacional y política exterior. *Estudios Internacionales*, 53(198), 169–197. https://doi.org/10.5354/0719-3769.2021.57067

Anabalón, J., & Donders, E. (2014). Una revisión de ciberdefensa de infraestructura crítica. *ESD. Estudios Seguridad y Defensa*, (3). https://silo.tips/download/una-revision-de-ciberdefensa-de-infraestructura-critica

Bárcena Coqui, M. (2000). La reconceptualización de la seguridad: el debate contemporáneo. *Revista Mexicana de Política Exterior*, 59, 9-31. https://revistadigital.sre.gob.mx/index.php/rmpe/article/view/988

Bartolomé, M. (2019). Amenazas y conflictos híbridos: características distintivas, evolución en el tiempo y manifestaciones preponderantes. *URVIO. Revista Latinoamericana de Estudios de Seguridad*, (25), 8–23. https://doi.org/10.17141/urvio.25.2019.4249

Betancur, J. G., (2004). La delgada línea entre la información, la desinformación y la propaganda. *Reflexión Política*, 6(12), 80-93. Recuperado de: https://revistas.unab.edu.co/index.php/reflexion/article/view/668

Buzan, B., & Wæver, O. (2003). Regions and Powers: The Structure of International Security (Cambridge Studies in International Relations). Cambridge: Cambridge University Press. https://doi.org/10.1017/CBO9780511491252 PMid: 15703609

Cajas Matute, R. A. (2022). Las amenazas híbridas, un nuevo reto para los Estados. Revista de la Academia de la Guerra del Ejército ecuatoriano, 15(1), 29-38. https://doi.org/10.24133/AGE.N15.2022.02

Cano Martínez, J. J. (2022). Prospectiva de ciberseguridad nacional para Colombia a 2030. *Revista Científica General José María Córdova*, 20(40), 815–832. https://doi.org/10.21830/19006586.866

Caro Bejarano, M. J. (2011). Alcance y ámbito de la seguridad nacional en el ciberespacio. *En M. d. Defensa*, Cuadernos de estrategia No. 149: Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio (págs. 47-82). Madrid: Ministerio de Defensa. https://www.ieee.es/publicaciones-new/cuadernos-de-estrategia/2011/Cuaderno_149.html

Caro Castaño, L. N. (2003). La postelevisión. Multimedia, internet y globalización económica. COMUNICACIÓN. *Revista Internacional de Comunicación Audiovisual, Publicidad y Estudios Culturales*, 1(2), 211–215. https://revistascientificas.us.es/index.php/Comunicacion/article/view/21448

Carvajal Peralta, J. (2022). Propuesta estratégica para la doctrina en comando y control en los ambientes aire, espacio y ciberespacio. *Escuela de posgrados Fuerza Aérea Colombiana (Colombia)*. https://repositorioslatinoamericanos.uchile.cl/handle/2250/3781834

Castillo Riquelme, V., Hermosilla Urrea, P., Poblete Tiznado, J. P., & Durán Anabalón, C. (2021). Noticias falsas y creencias infundadas en la era de la posverdad. *Universitas-XXI, Revista de Ciencias Sociales y Humanas*, (34), 87-108. https://doi.org/10.17163/uni.n34.2021.04

Cepik, M. (2001). Segurança Nacional e Segurança Humana: Problemas Conceituais e Consequências Políticas. *Security and Defense Studies Review*, 1 (1), 1-19. www.tinyurl.com/h2pdx46

Chaparro Betancourt, N., Osorio Isaza, V. & Sandoval Perdomo, A. E. (2020). China, Estados Unidos y 5G: capitalismo de vigilancia, geopolítica y geoestrategia. *Revista Perspectivas en Inteligencia*, 12(21), 33–45. https://doi.org/10.47961/2145194X.218

Chavero, P., & Intriago, D. (2021). Las fake news como herramienta política durante la pandemia del COVID-19 en Ecuador. *Cuadernos del Centro de Estudios de Diseño y Comunicación*, (136), 19-35. https://doi.org/10.18682/cdc.vi136.5038

Consejo Nacional de Política Económica y Social. Documento CONPES 3701. (2011). Lineamientos de política para ciberseguridad y ciberdefensa. *Departamento nacional de planeación*. Recuperado de https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf

Constitución Política de Colombia. (1991). https://pdba.georgetown.edu/Constitutions/Colombia/colombia91.pdf

Cujabante Villamil, X. A., Bahamón Jara, M. L., Prieto Venegas, J. C., & Quiroga Aguilar, J. A. (2020). Ciberseguridad y ciberdefensa en Colombia: un posible modelo a seguir en las relaciones cívico-militares. Revista Científica General José María Córdova, 18(30), 357–377. https://doi.org/10.21830/19006586.588

Cypher, J. M. (2007). La reestructuración de la política económica armamentista en EEUU: más allá del keynesianismo militar. *Oikos: Revista de la Escuela de Administración y Economía*, (23), 1-18. https://dialnet.unirioja.es/servlet/articulo?codigo=2562533

De la Peña, N., & Granados, O. (2021). Cuarta revolución industrial: implicaciones en la seguridad internacional. *Revista Oasis*, 33, 49-73. https://doi.org/10.18601/16577558.n33.05

Departamento de Defensa Estados Unidos. (2016). Department of Defense Dictionary of Military and Associated Terms. *Departamento de Defensa*, Joint Publication 1-02. https://fas.org/irp/doddir/dod/jp1_02.pdf

Eltiempo.com. (2021). Las noticias falsas que no debe creer en medio del paro. *Eltiempo.com*. https://www.eltiempo.com/colombia/otras-ciudades/noticias-falsas-durante-el-paro-nacional-fake-news-colombia-586098

Erazo Patiño, L. A., Cujabante Villamil, X. A., & Arenas Piedrahíta, A. J. (2022). Colombia: Avances y desafíos frente a la delincuencia organizada transnacional. Bogotá, D. C.: Editorial ESDEG, ESMIC Sello Editorial. https://doi.org/10.21830/9786289544602

Ferrero, J. A. (2013). La Ciberguerra, génesis y evolución. *Revista general de marina*, (264), 81-97. https://dialnet.unirioja.es/servlet/articulo?codigo=4160939

Fuente Cobo, I. (2022). La OTAN y el ciberespacio: un nuevo dominio para las operaciones. *Revista Ejército: de tierra español*, (972), 84-91. https://dialnet.unirioja.es/servlet/articulo?codigo=8454973

Gallardo Castañeda, M. (2019). Riesgos y amenazas para la seguridad multidimensional. Tema de Investigación Central de la Academia, Cap. 3, 65 - 83. Recuperado a partir de https://publicacionesacague.cl/index.php/tica/article/view/156

Gibson, W. (1984) Neuromancer. Canadá, Editora Ace books.

González Arencibia, M., & Martinez Cardero, D. (2021). Repensando las fake news desde la economía política. *Oikos Polis*, 6(1), 1-41. Epub 30 de junio de 2021. Recuperado en 29 de septiembre de 2023, de http://www.scielo.org.bo/scielo.php?script=sci_arttext&pid=S2415-22502021000100004&lng=es&tlng=es.

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, P. (2014). Definiciones de los enfoques cuantitativo y cualitativo, sus similitudes y diferencias. En Metodología de la investigación. Sexta edición. México, D. F.: McGRAW-HILL / Interamericana editores, S.A. de C.V.

Leiva, E. A. (2015) Estrategias nacionales de ciberseguridad: estudio comparativo basado en enfoque top-down desde una visión global a una visión local, 3(4), 161-176. https://doi.org/10.18294/relais.2015.161-176

Lodeiro Encina, A. (2011). La ciberguerra y sus dimensiones en la seguridad nacional. *Cuaderno de difusión pensamiento de Estado Mayor: las nuevas dimensiones de la guerra*, (págs. 21-40). Santiago de Chile: Ejército de Chile - Academia de guerra, (32).

Mancera, J. M. (2014). La ciberguerra China desde la lógica de la guerra irrestricta. *Ciencia y Poder Aéreo*, 9(1), 89–96. https://doi.org/10.18667/cienciaypoderaereo.137

Miguel-Gil, J. (2019). El tratamiento informativo de la guerra híbrida de Rusia. *URVIO. Revista Latinoamericana de Estudios de Seguridad*, (25), 108–121. https://doi.org/10.17141/urvio.25.2019.4006

Ministerio de Defensa Nacional. (2023). Política de seguridad, defensa y convivencia ciudadana: garantías para la vida y la paz 2022-2026. *Ddhhcolombia.org.co.*, *Plataforma colombiana de derechos humanos, democracia y desarrollo*. https://ddhhcolombia.org.co/2023/05/24/politica-de-seguridad-defensa-y-convivencia-ciudadana/

Miranzo, M., & Del Río, C. (2014). La protección de infraestructuras críticas. *Revista UNISCI Discussion Papers*, (35), 339-352. https://www.redalyc.org/articulo.oa?id=76731410018 https://doi.org/10.5209/rev_UNIS.2014.n35.46435

Mozo Rivera, O., & Ardila Contreras, J. V. (2022). El fenómeno de las ciberamenazas: afectaciones a la ciberseguridad del Ejército nacional de Colombia. *Revista Perspectivas en Inteligencia*, 14(23), 63–95. https://doi.org/10.47961/2145194X.333

Otálvaro, A. F. (2004). La seguridad internacional. A la luz de las estructuras y las dinámicas regionales: una propuesta teórica de complejos de seguridad regional.

Desafíos, 11, 222-242. Recuperado a partir de https://revistas.urosario.edu.co/index.php/desafios/article/view/669

Policia.gov.co. (2023). Ciberseguridad de la Policía Nacional. *Policía nacional de Colombia*. https://www.policia.gov.co/ciberseguridad

Poveda Zamora, G. A. & Álvarez Calderón, C. E. (2022). Integración del poder aéreo, espacial y ciberespacial. En Poder multidominio y el sistema de vigilancia y protección de la Amazonía colombiana (pp. 23-48). Bogotá, Colombia, *Editorial Escuela de Posgrados de la FAC*. https://doi.org/10.18667/9789585369658.01

Realpe Díaz, M. E. (2019). Estrategia militar de ciberdefensa para las Fuerzas Militares de Colombia de cara a las amenazas cibernéticas que imponen las tecnologías disruptivas al 2022. *Repositorio Escuela Superior de Guerra "General Rafael Reyes Prieto"*, Colombia, https://hdl.handle.net/20.500.14205/4309

Realpe, M., & Cano, J. (2020). Amenazas cibernéticas a la seguridad y defensa nacional. Reflexiones y perspectivas en Colombia. In Seguridad Informática: X Congreso Iberoamericano, CIBSI 2020 105-113. *Editorial Universidad del Rosario*. https://doi.org/10.12804/si9789587844337.10

Rojas Guevara, P. J. (2017). Doctrina Damasco: eje articulador de la segunda gran reforma del Ejército Nacional de Colombia. *Revista Científica General José María Córdova*, 15(19), 95–119. https://doi.org/10.21830/19006586.78

Semana.com. (2021). Imitando la voz del gerente con computadora, ladrones hurtan más de 35 millones de dólares a un banco. *Semana.com*. https://bit.ly/3tPlJ2F

Semanate Esquivel, A., & Recalde, L. (2023). El Estado y la defensa del ciberespacio. *Revista de la Academia de Guerra del Ejército ecuatoriano*, 16(1), 11. https://doi.org/10.24133/AGE.VOL16.N01.2023.07

Sisco Marcano, C., & Chacón Maldonado, O. (2004). Barry Buzan y la teoría de los complejos de seguridad. *Revista venezolana de Ciencia Política*, 25, 125-146. http://www.saber.ula.ve/handle/123456789/24849

Tesouro Cid, M., & Puiggalí Allepuz, J. (2004). Evolución y utilización de internet en la educación. *Pixel-Bit. Revista de Medios y Educación*, (24), 59-67. Recuperado a partir de https://recyt.fecyt.es/index.php/pixel/article/view/61231

Trujano Ruiz, P., Dorantes Segura, J., & Tovilla Quesada, V. (2009). Violencia en internet: nuevas víctimas, nuevos retos. *Revista Liberabit*, 15(1), 7-19. Recuperado

en 17 de mayo de 2023, de http://www.scielo.org.pe/scielo.php?script=sci_arttext&pid=S1729-48272009000100002&lng=es&tlng=es.

Unodc.org. (2010). The globalization of crime: A transnational organized crime threat assessment. *United Nations Office on Drugs and Crime*. https://www.unodc.org/unodc/en/data-and-analysis/tocta-2010.html

Vargas Borbúa, R., Reyes Chicango, R. P., & Recalde Herrera, L. (2017). Ciberdefensa y ciberseguridad, más allá del mundo virtual: modelo ecuatoriano de gobernanza en ciberdefensa. *URVIO. Revista Latinoamericana de Estudios de Seguridad*, (20), 31-45. https://doi.org/10.17141/urvio.20.2017.2571

Villalba, A., & Corchado, J. M. (2017). Análisis de las ciberamenazas. *Cuadernos de estrategia*, (185), 97-138. https : / / dialnet.unirioja. es / servlet / articulo ? codigo = 6115622

Villanueva Méndez, J. C. (2015). La ciberdefensa en Colombia. *Repositorio Universidad Piloto de Colombia*. http://repository.unipiloto.edu.co/handle/20.500.12277/2812