Implicaciones de la guerra cibernética como amenaza a la seguridad nacional de Colombia.

Mayor (EJC) Víctor Alfonso Gómez Guzmán

Articulo para optar al título profesional:

Magister en Ciberseguridad y Ciberdefensa

Escuela Superior de Guerra “General Rafael Reyes Prieto”
Bogotá D.C., Colombia
2025

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia

DATOS GENERALES		
Nombre del estudiante	**:**	Mayor (EJC) Víctor Alfonso Gómez Guzmán
Identificación	**:**	80´902.628
Programa académico	**:**	Maestría en Ciberseguridad y Ciberdefensa
Tutor metodológico	**:**	Coronel Aldemar Serrano Cuervo PhD
Tutor temático	**:**	Mayor R Oscar Orlando Porras Rodríguez PhD
Fecha de entrega	**:**	25 de agosto de 2025
Extensión	**:**	10434 palabras

DECLARACIÓN DE ORIGINALIDAD Y CESIÓN DE DERECHOS

El autor declara que este artículo fue escrito de acuerdo con la normatividad de la Escuela Superior de Guerra "General Rafael Reyes Prieto" (ESDEG) y no existe ningún potencial conflicto de interés relacionado con este. Las posturas y aseveraciones presentadas son resultado de un ejercicio académico e investigativo que no representan la posición oficial ni institucional de la ESDEG, las Fuerzas Militares de Colombia o el Ministerio de Defensa Nacional.

Este artículo es enteramente mi propio trabajo y no ha sido presentado para la obtención de un título en esta u otra Institución de Educación Superior. Se han referenciado todos los trabajos y puntos de vista de otros autores, así como los datos de otras fuentes utilizadas. No se emplearon herramientas de generación de contenido por Inteligencia Artificial para su elaboración.

El autor acepta ceder los derechos de publicación en favor de la ESDEG y su Sello Editorial de acuerdo con los términos de la licencia Creative Commons: Reconocimiento-NoComercial-SinObrasDerivadas.

AUTORIZACIÓN DE PUBLICACIÓN

El autor autoriza que este artículo sea publicado por el Sello Editorial ESDEG en su repositorio institucional y esté disponible bajo una modalidad de acceso abierto.

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia

Implicaciones de la guerra cibernética como amenaza a la seguridad nacional de Colombia.

Implications of cyberwarfare as a threat to Colombia's national security

Víctor Gómez[1]
Escuela Superior de Guerra "General Rafael Reyes Prieto"

Resumen: Este artículo presenta el diseño conceptual de una plataforma integral orientada a fortalecer la gestión del riesgo cibernético en el Ejército Nacional de Colombia, utilizando un enfoque basado en la gestión del riesgo de desastres. Ante la creciente sofisticación y recurrencia de amenazas cibernéticas que afectan infraestructuras críticas militares, se propone una estructura sistemática, proactiva e integral para identificar, analizar, mitigar y responder a estos riesgos. La plataforma contempla la aplicación de procesos de evaluación del riesgo, implementación de sistemas de alerta temprana, monitoreo continuo y coordinación interinstitucional, alineados con las políticas nacionales de ciberseguridad y estándares internacionales. Asimismo, se resalta la importancia de una cultura organizacional orientada a la prevención, la capacitación permanente del personal y la incorporación de tecnologías adaptativas. Este diseño conceptual busca establecer una base estratégica para el desarrollo e implementación de mecanismos robustos de defensa cibernética dentro de las estructuras operativas y administrativas del Ejército.

Palabras clave: Ciberseguridad, Gestión del riesgo cibernético, Defensa cibernética.

Abstract: This article presents the conceptual design of an integrated platform aimed at enhancing cyber risk management within the Colombian National Army, using principles and methodologies adapted from disaster risk management. Given the increasing complexity and frequency of cyber threats targeting critical military infrastructure, it is essential to adopt a comprehensive, proactive, and systematic approach. The proposed platform incorporates risk identification, analysis, mitigation, response, and recovery processes, aligned with national cybersecurity policies and international standards. By drawing parallels between cyber risks and disaster scenarios, the framework facilitates a better understanding of vulnerabilities and promotes resilience through early warning systems, continuous monitoring, and inter-agency coordination. The study also emphasizes the importance of organizational culture, training, and technological adaptability in mitigating cyber threats. The results

[1] Mayor del Ejército Nacional de Colombia. Candidato a magíster en Ciberseguridad y Ciberdefensa, Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia. Profesional en Ciencias Militares, Escuela Militar de Cadetes "General José María Córdova", Colombia. https://orcid.org/my-orcid?orcid=0009-0005-7000-0967 - Contacto: victor.gomez@esdeg.edu.co.

of this conceptual design aim to serve as a strategic foundation for the development and implementation of robust cyber defense mechanisms within the Army's operational and administrative structures.

Keywords: Cybersecurity, Cyber Risk Management, Cyber Defense.

Introducción

El ciberespacio se ha consolidado como un dominio estratégico de confrontación, donde los ciberataques representan una amenaza directa a la soberanía y estabilidad de los Estados. En el caso de Colombia, la creciente vulnerabilidad de los sistemas de mando, control, comunicaciones e inteligencia frente a acciones como el espionaje, el sabotaje o las campañas de desinformación demuestra que las agresiones en el entorno digital pueden tener consecuencias comparables a un enfrentamiento militar convencional. Este escenario revela que la seguridad nacional ya no se limita al ámbito físico, sino que depende de la protección de infraestructuras críticas y de la capacidad para anticipar y responder a operaciones hostiles en un entorno híbrido y en constante evolución.

A pesar de la existencia de avances normativos y políticos, como la Política Nacional de Confianza y Seguridad Digital (CONPES 3995 de 2020, p. 27.), persisten brechas estructurales en materia de prevención, monitoreo, coordinación interinstitucional y cultura de seguridad digital. La ausencia de un enfoque integral de gestión del riesgo cibernético limita la resiliencia institucional y expone al país a consecuencias no solo técnicas, sino también económicas, políticas, sociales y psicológicas, afectando la gobernabilidad y la confianza ciudadana.

En este marco, la presente investigación planteó como problema central la vulnerabilidad de Colombia frente a la guerra cibernética y la necesidad de comprender sus implicaciones estratégicas. Por ello, se formuló la pregunta orientadora: ¿Por qué la guerra cibernética representa una amenaza para la seguridad nacional de Colombia y qué desafíos implica?

Se desarrolló a partir del objetivo general, analizar las implicaciones de la guerra cibernética como una amenaza a la seguridad nacional de Colombia. Para ello, se planteó cuatro objetivos específicos: (1) describir el contexto espacio-temporal en el que se libran actualmente las guerras; (2) identificar las vulnerabilidades y amenazas de las infraestructuras asociadas a la seguridad nacional de Colombia, así como las capacidades actuales para librar una guerra cibernética; (3) evaluar los efectos tecnológicos y geopolíticos que tendría para el país verse inmerso en una guerra cibernética y/o híbrida; y (4) señalar las implicaciones de diferente naturaleza que estas amenazas suponen para la seguridad nacional.

La evolución del ciberespacio como dominio de operaciones ha transformado profundamente la dinámica de los conflictos internacionales, dando lugar a las denominadas guerras cibernéticas, las cuales se caracterizan por la utilización de medios digitales para alterar, destruir o manipular infraestructuras críticas, datos e información estratégica (Kello, 2017; Rid, 2013). Según (Nye 2010, p. 3), el ciberespacio es un entorno que rebasa las fronteras físicas tradicionales, convirtiéndose en un campo de batalla donde las armas son códigos maliciosos, ataques de denegación de servicio y operaciones de manipulación de la información.

Las guerras cibernéticas, aunque no son recientes, han alcanzado mayor sofisticación desde finales del siglo XX. Casos como el ataque a Estonia en 2007 (Schmidt, 2013), Stuxnet en 2010 (Zetter, 2014). y los ataques atribuidos a actores estatales en las elecciones de diversos países han evidenciado la creciente relevancia de estos conflictos.

Healey (2011) y Libicki (2007) destacan su carácter asimétrico, donde actores con menores recursos desafían a potencias, mientras que Singer y Friedman (2014) subrayan

cómo Internet permite la participación de actores no estatales y criminales, complicando la defensa en este nuevo entorno.

En Colombia, la ciberseguridad se ha posicionado como un asunto estratégico. Pese a los avances normativos como la Política Nacional de Seguridad Digital (MinTIC, 2022), aún existen desafíos significativos. El Observatorio Colombiano de Ciberseguridad (2023) advierte un incremento en incidentes como ransomware y phishing.

Las guerras cibernéticas trascienden el ámbito tecnológico, ya que sus efectos alcanzan dimensiones sociales, económicas, políticas y culturales. La afectación de infraestructuras críticas puede paralizar servicios esenciales, debilitar la confianza en las instituciones y generar inestabilidad política, mientras que los impactos económicos derivados de un ataque exitoso pueden ser tan graves como los de una agresión militar convencional. Por esta razón la interdependencia digital de Colombia con actores internacionales amplifica el carácter transnacional de estas amenazas, comprometiendo la seguridad regional y hemisférica, lo que evidencia la urgencia de consolidar capacidades de ciberdefensa bajo un enfoque integral y multidimensional, fortaleciendo las capacidades de ciberdefensa y diseñando políticas públicas.

Además, el Ejército Nacional enfrenta retos crecientes derivados de su dependencia de sistemas interconectados que sostienen operaciones estratégicas y de mando. Las amenazas, que van desde el espionaje y sabotaje hasta la manipulación de información y ataques de denegación de servicios, demandan un modelo de gestión del riesgo que supere las respuestas técnicas fragmentadas. De ahí la relevancia de diseñar una plataforma integral inspirada en la gestión del riesgo de desastres, que contemple prevención, preparación, respuesta y recuperación. Este enfoque permitiría al país fortalecer su resiliencia, garantizar

la continuidad de sus operaciones y afrontar de manera efectiva un entorno de confrontación híbrida y de alta complejidad. El desarrollo de esta propuesta se fundamenta en la necesidad de contar con una estrategia sistemática y proactiva, alineada con las políticas nacionales de ciberseguridad y con estándares internacionales, como el marco del NIST (National Institute of Standards and Technology, 2018) y las recomendaciones de la Estrategia Nacional de Ciberseguridad de Colombia (MinTIC, 2020). De igual manera el diseño de una solución adaptable y centrada en la gestión de riesgos permitirá avanzar hacia una defensa cibernética más efectiva, integral y sostenible.

Estado del arte

El estudio de las guerras cibernéticas y su impacto en la seguridad nacional ha evolucionado de manera significativa en la última década, consolidándose como un campo interdisciplinario que combina perspectivas tecnológicas, políticas, geopolíticas y sociales, autores como Rid (2013) y Kello (2017), han debatido la definición precisa de "guerra cibernética" y su diferenciación de otros fenómenos como el ciberespionaje o el hacktivismo. (Rid, 2013, p. 6-15) sostiene que la mayoría de los ataques cibernéticos no constituyen guerras en sentido estricto, sino operaciones de espionaje o sabotaje, mientras que (Kello, 2017, p 30-37) argumenta que los ataques cibernéticos pueden escalar y tener efectos equiparables a un conflicto armado tradicional, especialmente cuando se dirigen a infraestructuras críticas.

En este mismo sentido, Libicki (2007) ofrece una taxonomía de las operaciones cibernéticas, distinguiendo entre guerra cibernética, criminalidad informática y activismo político. Según este enfoque, la guerra cibernética se caracteriza por la motivación política y

la intencionalidad de afectar la soberanía y la seguridad nacional, aspectos fundamentales para el análisis de la amenaza en Colombia.

Vulnerabilidades y amenazas a infraestructuras críticas

Un aspecto central en la literatura especializada es el análisis de las vulnerabilidades inherentes a las infraestructuras críticas. (Lewis, 2014, p. 15-16) enfatiza que la interconexión digital de estos sistemas incrementa su exposición a ataques. A nivel latinoamericano, (Méndez, 2020, p 45) señala que las brechas tecnológicas y la falta de inversión en ciberseguridad convierten a países como Colombia en objetivos atractivos para actores hostiles.

A su vez el informe del Observatorio Colombiano de Ciberseguridad (2023) ofrece datos empíricos sobre los incidentes registrados en los últimos años, confirmando el aumento sostenido de ataques a sistemas de información en sectores estratégicos como la banca, la energía y la salud. Este diagnóstico es consistente con el análisis de Álvarez y Castillo (2021), quienes resaltan la necesidad de fortalecer la cultura de seguridad digital y mejorar la coordinación interinstitucional.

Efectos tecnológicos, económicos y geopolíticos

(Singer y Friedman, 2014, p. 67-110) destacan que las guerras cibernéticas tienen un impacto transversal, afectando no solo la infraestructura tecnológica, sino también la confianza pública y la estabilidad política. (Nye, 2010, p123-125) introduce el concepto de "poder cibernético" como un nuevo elemento en las relaciones internacionales, sugiriendo que los conflictos en el ciberespacio pueden redefinir los equilibrios geopolíticos tradicionales.

Por su parte, (Zetter, 2014, p 20-25), a partir del caso de Stuxnet, ilustra cómo las herramientas cibernéticas pueden ser utilizadas para sabotear objetivos estratégicos sin recurrir a la fuerza convencional. Este enfoque resulta particularmente relevante para Colombia, dado el riesgo de verse afectada por actores externos o internos que busquen alterar la estabilidad nacional mediante ataques híbridos.

Síntesis de la literatura y vacíos identificados

La revisión de la literatura evidencia que las guerras cibernéticas constituyen un fenómeno complejo, con implicaciones tecnológicas, geopolíticas, económicas y sociales. Los estudios revisados coinciden en señalar la importancia de contar con capacidades robustas de defensa y políticas públicas coherentes, pero también destacan la falta de investigaciones específicas sobre el contexto colombiano y las amenazas particulares que enfrenta el país en el actual escenario internacional.

Por lo tanto, el presente artículo busca aportar a la comprensión de estos desafíos desde una perspectiva contextualizada, describiendo el panorama actual, identificando las vulnerabilidades y capacidades nacionales, evaluando los efectos potenciales y señalando las implicaciones multidimensionales que enfrenta Colombia en el contexto de las guerras cibernéticas y los conflictos híbridos.

Marco teórico

El fenómeno de las guerras cibernéticas, entendido como el uso de herramientas digitales para atacar o defenderse en el marco de un conflicto interestatal o interestatal, ha tema de intensos debates en la literatura académica. Esta discusión se estructura en torno a diferentes

enfoques teóricos que permiten analizar y comprender la magnitud del desafío que enfrentan las infraestructuras y capacidades nacionales de países como Colombia.

1. El escepticismo sobre la guerra cibernética

Rid (2013), en su obra *Cyber War Will Not Take Place*, sostiene que, a pesar de la creciente preocupación por los ciberataques, no se han registrado guerras cibernéticas en sentido estricto. Según este autor, la mayoría de los incidentes en el ciberespacio corresponden a espionaje, sabotaje o subversión, pero carecen de la violencia directa, el umbral letal y la escala de un conflicto bélico convencional. Esta perspectiva crítica plantea un marco de contra argumentación frente a las narrativas alarmistas que ubican a los ciberataques como equivalentes a guerras tradicionales.

Desde este punto de vista, el debate sobre las guerras cibernéticas en Colombia debe considerar que muchos incidentes catalogados como amenazas cibernéticas podrían no constituir en sí mismos una "guerra", sino más bien una dimensión de la competencia interestatal o de conflictos internos con impacto digital.

2. La expansión del concepto de guerra cibernética

Frente a la posición escéptica de Rid, Kello (2017) propone una visión más amplia en *The Virtual Weapon and International Order*, donde argumenta que las guerras cibernéticas pueden tener un carácter híbrido y difuso, pero con efectos estratégicos comparables a las guerras convencionales. Según Kello (2017) p. 62, la ausencia de destrucción física directa no significa que estos conflictos carezcan de consecuencias políticas, económicas y sociales graves.

Este enfoque es relevante para Colombia, pues permite argumentar que las vulnerabilidades cibernéticas de infraestructuras críticas, combinadas con la desinformación digital y la manipulación de la opinión pública, pueden convertirse en un factor de desestabilización equiparable a un conflicto bélico. Así, el concepto de guerra cibernética se amplía para incluir formas de agresión que, aunque no letales, tienen el potencial de alterar la soberanía y la seguridad nacional.

3. El poder cibernético en las relaciones internacionales

Desde un enfoque más estructural, Nye (2010) p. 3-5, en su trabajo *Cyber Power*, introduce la noción de "poder cibernético" como la capacidad de los Estados y actores no estatales para utilizar el ciberespacio con fines de coerción, disuasión o influencia. Nye argumenta que el ciberespacio se ha convertido en un dominio estratégico más, al mismo nivel que la tierra, el mar, el aire y el espacio exterior, y que las guerras cibernéticas reconfiguran las dinámicas de poder global.

Para el caso colombiano, este planteamiento ofrece una base argumentativa sólida para entender cómo las guerras cibernéticas trascienden las fronteras tecnológicas y se insertan en las lógicas geopolíticas y de seguridad nacional. Además, destaca la necesidad de fortalecer las capacidades nacionales y la cooperación internacional para gestionar estos nuevos escenarios de conflicto.

4. Los ataques cibernéticos como herramientas de sabotaje estratégico

El análisis de Zetter (2014) sobre Stuxnet evidencia cómo un ciberataque puede trascender el plano digital y generar consecuencias físicas y económicas comparables a un ataque militar

convencional, lo que refuerza la necesidad de no subestimar el riesgo que representan estas amenazas para infraestructuras críticas como energía, salud o comunicaciones en Colombia. Esta postura dialoga con la visión escéptica de Rid (2013), quien cuestiona el uso del término "guerra cibernética", y con los aportes de Kello (2017) y Nye (2010), que destacan los efectos estratégicos y geopolíticos de los conflictos en el ciberespacio. En conjunto, los autores permiten una visión equilibrada que reconoce tanto la complejidad conceptual como la gravedad práctica de estas amenazas.

En el caso colombiano, estas discusiones resultan fundamentales para comprender que, aunque el país no ha enfrentado una guerra cibernética en sentido estricto, sí presenta vulnerabilidades susceptibles de ser explotadas por actores estatales o no estatales. De allí surge la importancia de fortalecer la resiliencia y preparación cibernética mediante un enfoque multidimensional que abarque lo tecnológico, lo geopolítico y lo social. Este marco no solo contribuye al debate académico sobre la naturaleza de las guerras cibernéticas, sino que también orienta la formulación de políticas públicas y estrategias de ciberdefensa adaptadas a las realidades nacionales.

Por lo que surge la pregunta ¿Por qué la guerra cibernética representa una amenaza para la seguridad nacional de Colombia y qué desafíos implica?

Metodología

Enfoque Metodológico

La metodología de esta investigación se estructura en varias fases que permiten abordar el diseño conceptual de una plataforma integral para la gestión del riesgo cibernético en el

Ejército Nacional de Colombia. Se utilizará un enfoque mixto, combinando métodos cualitativos y cuantitativos, lo cual permitirá obtener una comprensión amplia y profunda del problema, identificar vacíos en la gestión actual, y formular una propuesta basada tanto en evidencia empírica como en las percepciones de expertos.

Tipo de Investigación

El estudio se enmarca en una investigación aplicada, ya que busca generar una solución práctica y contextualizada a un problema específico. Es de tipo **d**escriptivo y propositivo, pues describe el estado actual de la gestión del riesgo cibernético en la institución y propone el diseño conceptual de una plataforma para su mejoramiento. Asimismo, el estudio tiene un carácter no experimental y transversal, dado que se recogerán datos en un solo momento temporal sin manipular las variables.

Métodos y Técnicas de Recolección de Información

Se emplearán tanto métodos cualitativos como cuantitativos, en cuanto a lo cualitativo se realizan entrevistas semiestructuradas a expertos en ciberseguridad, oficiales del Ejército y responsables de tecnologías de la información, con el fin de conocer percepciones, experiencias y necesidades institucionales y respecto a lo cualitativo se aplican encuestas estructuradas a personal técnico y operativo del Ejército, con preguntas cerradas que permitan cuantificar el nivel de preparación, percepción del riesgo y disponibilidad de recursos tecnológicos.

Técnica de Análisis de la Información

Para los datos cuantitativos, se realiza un análisis estadístico descriptivo mediante medidas de tendencia central (media, mediana, moda) y de dispersión (desviación estándar), usando Excel.

Para los datos cualitativos, se aplica un análisis de contenido temático, categorizando las respuestas de los entrevistados para identificar patrones, preocupaciones recurrentes y oportunidades de mejora (Gibbs, 2007).

Limitaciones de la Investigación

Por tratarse de una institución militar, algunos datos relevantes pueden estar clasificados o restringidos, lo que podría limitar el alcance del análisis, asimismo, la muestra no probabilística limita la generalización de los resultados al conjunto total del Ejército y algunos participantes podrían limitar sus respuestas por temor a comprometer su cargo o debido a políticas de confidencialidad institucional.

El contexto espacio-temporal actual de las guerras cibernéticas.

En el siglo XXI, el escenario global de confrontación ha sufrido una transformación radical. Las guerras cibernéticas han emergido como una forma contemporánea de conflicto que trasciende las fronteras físicas tradicionales y se instala en un nuevo dominio el ciberespacio. A diferencia de los conflictos armados convencionales, estas guerras se caracterizan por su

invisibilidad, velocidad, alcance global y la dificultad para atribuir responsabilidades directas.

Su desarrollo no está condicionado por la presencia territorial del enemigo, sino por la capacidad de acceso remoto a sistemas digitales críticos. En este contexto, el objetivo de este capítulo es analizar el entorno actual, tanto geográfico como temporal en el que se desarrollan las guerras cibernéticas, para comprender su evolución, sus características distintivas y su creciente relevancia para la seguridad nacional.

La evolución tecnológica ha transformado profundamente la forma en que los Estados y actores no estatales conciben y ejecutan sus estrategias de poder. El ciberespacio, definido por Nye (2010) como el entorno interconectado compuesto por infraestructuras digitales, redes de comunicación y sistemas informáticos, se ha consolidado como un nuevo teatro de operaciones en el que se libran disputas tan decisivas como las bélicas. Su naturaleza descentralizada, la ausencia de fronteras físicas y el bajo costo de ejecución han facilitado la expansión de ciberoperaciones de todo tipo desde el espionaje digital y el sabotaje de infraestructuras críticas hasta el ciberterrorismo y la manipulación de la opinión pública mediante campañas de desinformación.

Autores como Libicki (2009) y Rid (2013) destacan que estas acciones, al no requerir declaraciones formales de guerra ni autorización parlamentaria, se insertan dentro de estrategias híbridas más amplias y a menudo encubiertas. Singer y Friedman (2014) denominan esta zona de conflicto como un "estado gris", caracterizado por una ambigüedad estratégica donde los límites entre la guerra y la criminalidad se difuminan. En ese sentido, el tiempo y el espacio en las guerras cibernéticas ya no responden a las lógicas convencionales de duración y territorialidad, sino a patrones continuos de agresión que

pueden prolongarse de forma silenciosa durante semanas o incluso meses sin ser detectados, como lo confirma el informe Mandiant (2023).

El reconocimiento institucional del ciberespacio como un dominio de confrontación ha tenido profundas implicaciones geopolíticas. En 2016, la OTAN declaró que un ciberataque significativo puede ser considerado como motivo suficiente para activar el artículo 5 de defensa colectiva (NATO, 2016), situando al ciberespacio al mismo nivel que la tierra, el mar, el aire y el espacio exterior. Potencias como Estados Unidos, Rusia y China han integrado capacidades cibernéticas en sus doctrinas militares, creando comandos especializados como el U.S. Cyber Command o desarrollando ciberfuerzas ofensivas (Clarke & Knake, 2012). Este proceso de militarización digital ha consolidado una nueva dimensión estratégica del conflicto, donde las tecnologías de la información son empleadas como instrumentos de disuasión, sabotaje o espionaje.

Los desafíos legales y éticos derivados de este nuevo tipo de confrontación son igualmente relevantes. Las normas tradicionales del derecho internacional humanitario, como los Convenios de Ginebra, no fueron diseñadas para un entorno donde la atribución de responsabilidades es incierta y la línea entre civil y combatiente se vuelve borrosa (Schmitt, 2013). Esto no solo debilita la capacidad de los Estados para responder legalmente ante una agresión, sino que favorece la impunidad de los actores agresores, muchos de los cuales actúan bajo patrocinio estatal o mediante estructuras descentralizadas y anónimas (Tikk, Kerttunen & Vihul, 2010).

El contexto espacio-temporal de las guerras cibernéticas también se articula con la lógica de la guerra híbrida, entendida como la combinación de tácticas convencionales, irregulares, cibernéticas y psicológicas. La anexión de Crimea en 2014, así como los ataques

a infraestructuras críticas en Ucrania y las campañas de desinformación durante procesos electorales en Estados Unidos (2016) y otras democracias occidentales, evidencian cómo el ciberespacio se ha convertido en una herramienta central de intervención política y militar (Giles, 2016; Mueller, 2020).

En el caso de Colombia, aunque no se cuenta con la capacidad ofensiva de grandes potencias, el país ha sido objeto de múltiples ciberataques dirigidos a su infraestructura crítica, procesos electorales y plataformas institucionales. Estas agresiones han tenido como fin desestabilizar el sistema democrático, interrumpir operaciones estratégicas y socavar la confianza ciudadana (Ramírez, 2022). La creciente digitalización en sectores como la banca, la energía y la defensa nacional ha incrementado significativamente la vulnerabilidad ante amenazas externas e internas.

A esto se suma el carácter continuo y silencioso de este tipo de conflicto, que impone un desgaste permanente a las instituciones encargadas de la seguridad nacional. Rid (2013) y Valeriano & Maness (2015) advierten que la ciberseguridad ya no puede entenderse como una preparación para posibles agresiones futuras, sino como una gestión constante de amenazas presentes y adaptativas. El acceso sostenido a redes comprometidas durante semanas o meses, sin que se detecte la intrusión representa una forma de ocupación virtual con consecuencias reales y acumulativas.

Este escenario impone la necesidad urgente de repensar las estrategias de defensa y de formular políticas públicas adaptadas a la naturaleza cambiante del conflicto digital. Para Nye (2010) y Maurer (2018), la seguridad nacional contemporánea debe ir más allá de la lógica militar tradicional e integrar herramientas tecnológicas, jurídicas y diplomáticas que permitan una respuesta integral, resiliente y democrática.

Sin embargo, también existen voces críticas que advierten sobre el riesgo de sobredimensionar la amenaza cibernética y de utilizarla como pretexto para legitimar prácticas autoritarias como la vigilancia masiva o la restricción de libertades civiles (Deibert, 2020). La comprensión del contexto espacio-temporal de las guerras cibernéticas no puede desvincularse de estos dilemas ético-políticos, que deben formar parte del análisis y del diseño de cualquier política pública en ciberseguridad.

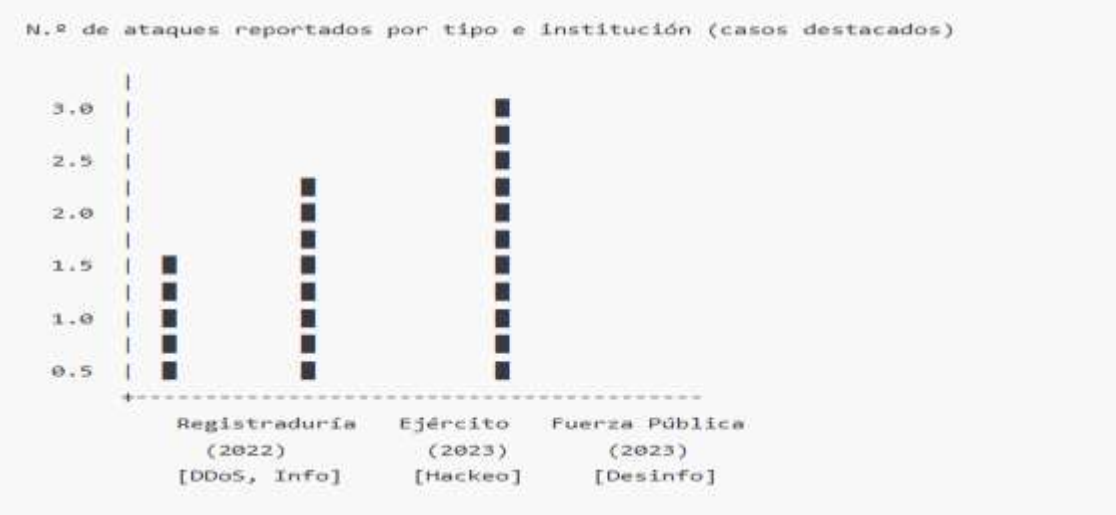
Es así que el marco espacio-temporal de las guerras cibernéticas redefine los conceptos de conflicto, poder y soberanía en el siglo XXI. Su estudio es esencial para comprender los nuevos desafíos de la seguridad nacional y para anticipar los impactos sociales, políticos y legales de una confrontación que, aunque muchas veces invisible, es constante, compleja y global.

Tabla 1: Impacto de las Guerras Cibernéticas en Colombia (2022–2023)

AÑO	INSTITUCIÓN AFECTADA	TIPO DE ATAQUE
2022	Registraduría Nacional del Estado Civil	Ataques DDoS y campañas de desinformación durante elecciones
2023	Ejército Nacional	Intentos de intrusión y robo de información clasificada
2023	Fuerzas Militares (Fuerza Pública)	Campañas de desinformación y hackeo de datos

Fuente: El Universal. (2022), Noticias RCN. (2023).

Gráfico1: Tipos de Ciberataques por Institución (2022–2023)



Fuente: El Universal. (2022), Noticias RCN. (2023).

Los casos analizados involucran manipulación psicológica o técnica digital, asimismo los ataques no se limitan al Ejército Nacional, sino que afectan instituciones claves como la Registraduría y las tendencias crecientes en 2023 reflejan una evolución del ciberconflicto desde sabotajes técnicos hacia operaciones de desinformación e influencia.

Es así que las guerras cibernéticas representan un riesgo directo para la capacidad de planeación, ejecución y control de las operaciones militares. Entre los principales impactos se encuentran.

Guerra Cibernética y Defensa Digital en el Ejército Nacional de Colombia (2021–2023)

El impacto de las guerras cibernéticas en el Ejército Nacional trasciende la dimensión técnica. Se trata de una amenaza a la integridad de la soberanía, la legitimidad institucional y la estabilidad democrática del país. La defensa del ciberespacio se convierte en una condición

esencial para garantizar la continuidad de las funciones del Estado y la protección de la ciudadanía (Deibert, 2020).

Además, la experiencia colombiana refleja la necesidad de cooperación internacional, tanto en el intercambio de inteligencia como en la construcción de capacidades conjuntas con países aliados y socios estratégicos (NATO, 2016).

Tabla 2: Principales tipos de impacto detectado (2021–2023)

TIPO DE IMPACTO	CASOS REPORTADOS	EJEMPLOS CLAVE
Interrupción de sistemas críticos	2	Infraestructura crítica, logística, comunicaciones
Exfiltración de datos sensibles	3	Hackeo a bases militares, redes clasificadas
Manipulación de percepción pública	3	Campañas de desinformación durante elecciones y protestas

Fuente: Fuente: Esici (2022). Centro Cibernético Policial. (2024). Infobae. (2022)

Los principales impactos detectados en el ciberespacio contra Colombia se concentraron en tres dimensiones: la interrupción de sistemas críticos, la exfiltración de datos sensibles y la manipulación de la percepción pública.

Identificación de las vulnerabilidades y amenazas de las infraestructuras críticas asociadas a la seguridad nacional de Colombia y capacidades actuales para librar una guerra cibernética

La creciente digitalización de las infraestructuras críticas y la expansión de las operaciones digitales han convertido a las guerras cibernéticas en uno de los mayores desafíos para la seguridad nacional de Colombia. Estas guerras representan una amenaza que, si bien es global, ha tenido manifestaciones concretas en el país, afectando tanto a entidades públicas como privadas y a las Fuerzas Militares. En este capítulo se describen las vulnerabilidades y amenazas actuales, así como las capacidades de defensa desarrolladas hasta el momento.

Infraestructuras críticas y exposición a ciberataques

Las infraestructuras críticas, que abarcan sectores como energía, salud, telecomunicaciones, transporte y servicios gubernamentales, constituyen pilares esenciales para la estabilidad nacional, pero su alta dependencia tecnológica las hace particularmente vulnerables a ciberataques (CISA, 2021). Aunque Colombia se encuentra entre los pocos países de la región con planes de protección (Berdugo Sierra, 2016), los datos reflejan un panorama alarmante en 2022 se registraron más de 20.000 millones de intentos de ciberataques, con un incremento del 122 % en incidentes de ransomware que afectaron a entidades gubernamentales y de salud (Ministerio de Defensa Nacional, 2023; Ramírez, 2022). A esto se suma el crecimiento del 238 % en ataques contra sistemas industriales y operativos, especialmente en sectores eléctricos y de transporte (Velázquez, 2024).

Un ejemplo crítico fue el ataque de septiembre de 2023 contra IFX Networks, que afectó servicios esenciales de entidades del Estado como el Ministerio de Salud y la Superintendencia de Industria y Comercio. Estos hechos evidencian cómo la sofisticación y persistencia de los atacantes comprometen la disponibilidad, integridad y confidencialidad de los sistemas estratégicos. En este sentido, proteger infraestructuras críticas, como lo reconoce la Ley 1621 de 2013 y la CISA (2021), resulta indispensable para garantizar la seguridad nacional, la economía y el bienestar de los ciudadanos.

En Colombia, el Departamento Nacional de Planeación (2020), p. 62, mediante el documento CONPES 3995, establece la Política Nacional de Confianza y Seguridad Digital, la cual identifica las infraestructuras críticas como prioritarias para la ciberseguridad. Este documento recalca que la dependencia tecnológica de estos sectores los hace más vulnerables a ataques de actores maliciosos.

Riesgo creciente de ciberataques a infraestructuras críticas

Las vulnerabilidades de las infraestructuras críticas se relacionan con varios factores. Por un lado, la creciente interconexión digital mediante la adopción de sistemas SCADA (Supervisory Control and Data Acquisition) y redes industriales (OT, por sus siglas en inglés) incrementa la superficie de ataque (Bodnar, 2021). Estos sistemas, diseñados originalmente para operar en entornos aislados, enfrentan riesgos cuando se integran a redes corporativas o a Internet.

Por otro lado, la falta de inversión en ciberseguridad en sectores como el transporte y la energía ha creado brechas que pueden ser explotadas. Según un estudio de la Organización de Estados Americanos (OEA, 2022), solo el 20 % de las empresas de infraestructura crítica

en América Latina destinan más del 10 % de su presupuesto de TI a la ciberseguridad, cifra considerada insuficiente para las amenazas actuales.

Incidentes recientes y casos relevantes en Colombia

En el contexto colombiano, se han registrado varios incidentes que evidencian la exposición de las infraestructuras críticas. Por ejemplo, en 2023, el ataque de ransomware que afectó a IFX Networks proveedor clave de conectividad para más de 30 entidades gubernamentales, incluyendo el Ministerio de Salud, esto provocó interrupciones en servicios esenciales y expuso la fragilidad de las redes de comunicaciones.

Asimismo, el Centro Cibernético Policial (2024) reportó en su más reciente boletín que sectores como energía y salud han sido los más atacados por amenazas persistentes avanzadas (APT). Estos ataques, generalmente patrocinados por Estados u organizaciones criminales transnacionales, buscan infiltrarse en los sistemas críticos con fines de espionaje, sabotaje o chantaje económico.

Factores que agravan la exposición a ciberataques

La exposición a ciberataques se agrava principalmente por varios factores interrelacionados y de distinta naturaleza. Genera vulnerabilidades críticas que pueden ser explotadas por atacantes. Asimismo, la falta de una cultura de ciberseguridad dentro de las organizaciones, caracterizada por una capacitación insuficiente y la frecuente ocurrencia de errores humanos, incrementa el riesgo de incidentes cibernéticos. La convergencia de las tecnologías de la información (IT) con las tecnologías operativas (OT), como los sistemas industriales y de control, amplía la superficie de ataque al integrar entornos que antes estaban aislados, lo que

facilita a los atacantes acceder a redes críticas. Finalmente. Estos factores requieren una gestión integral y coordinada para mitigar la exposición y fortalecer la defensa cibernética.

Tabla 3: Listado de factores y fuentes

FACTOR	DESCRIPCIÓN BREVE
Obsolescencia tecnológica	Sistemas antiguos sin parches de seguridad
Falta de cultura de ciberseguridad	Poca capacitación y errores humanos frecuentes
Convergencia IT-OT	Mayor exposición por integrar sistemas industriales y redes TI
Interdependencia sectorial	Ataques en un sector afectan otros (energía, agua, transporte)

Fuente: Velázquez (2024), Ramírez (2022), Bodnar (2021), OEA (2022)

Se evidencia que la exposición a ciberataques en Colombia responde a una combinación de factores estructurales y humanos que incrementan de forma significativa las vulnerabilidades críticas. Ya que algunos de los sistemas son antiguos sin parches de seguridad lo cual facilitan la explotación de brechas por parte de atacantes. A esto se suma la escasa capacitación del personal y la incidencia de errores humanos. Por otro lado, se amplía la superficie de ataque al interconectar sistemas industriales y redes de información, generando riesgos adicionales en infraestructuras críticas.

Necesidad de fortalecimiento y respuesta

El CONPES 3995 (Departamento Nacional de Planeación, 2020) resalta la importancia de fortalecer la resiliencia cibernética del país a través de la colaboración público-privada y la adopción de estándares internacionales como el NIST Cybersecurity Framework y la norma ISO/IEC 27001, lo que constituye un avance hacia la alineación con buenas prácticas

globales. No obstante, persiste una debilidad estructural, la ausencia de un CSIRT nacional consolidado que articule de manera integral la prevención y la respuesta a incidentes en todos los sectores críticos.

Esta falencia se ve agravada por la falta de una Agencia Nacional de Ciberseguridad plenamente operativa, cuya ausencia limita la coordinación interinstitucional y deja a numerosos sectores estratégicos sin una ruta clara de actuación frente a emergencias digitales (Semana, 2023). En consecuencia, Colombia enfrenta un escenario en el que, a pesar de los avances normativos y técnicos, aún carece de una arquitectura institucional robusta que garantice una defensa cibernética integral y sostenible.

Desafíos para el Ejército Nacional de Colombia

Para el Ejército Nacional, la exposición de infraestructuras críticas implica riesgos directos e indirectos. Por un lado, sus propias redes de comando, control, comunicaciones e inteligencia están bajo amenaza constante. Por otro, la dependencia de sectores como energía y telecomunicaciones implica que ataques a estos sectores pueden comprometer la operatividad militar (Ministerio de Defensa Nacional, 2023).

El Ejército, a través del Comando Conjunto Cibernético, ha avanzado en la protección de sus redes y ha realizado ejercicios de ciberdefensa, pero aún enfrenta la necesidad de consolidar sus capacidades de resiliencia y respuesta coordinada con entidades civiles.

Las consecuencias de estos ataques van más allá de la simple pérdida de datos. Incluyen la interrupción de servicios esenciales, la pérdida de confianza de la ciudadanía y la exposición de información sensible, lo que debilita la soberanía digital (Departamento Nacional de Planeación, 2020). Se estima que, para 2025, las pérdidas económicas en

América Latina podrían alcanzar hasta 90 millones de dólares anuales debido a ciberataques (Ramírez, 2022).

Las amenazas cibernéticas han evolucionado desde ataques aislados hacia campañas sofisticadas y persistentes, muchas veces vinculadas a intereses geopolíticos y económicos. De acuerdo con la Organización de Estados Americanos (OEA, 2022), las principales amenazas emergentes son:

Tabla 4: Resumen de amenazas y características principales

AMENAZA	AFECTA PRINCIPALMENTE	NIVEL DE SOFISTICACIÓN
Ransomware a infraestructuras críticas	Salud, energía, transporte	Alto
Amenazas Persistentes Avanzadas (APT)	Redes gubernamentales, militares	Muy alto
Ingeniería social y phishing	Usuarios individuales y corporativos	Medio
Ataques a cadena de suministro	Empresas proveedoras de software	Alto
Uso de IA en ciberataques	Sistemas automatizados y defensas cibernéticas	Muy alto

Fuente: OEA (2022). Centro Cibernético. Ramírez (2022). Velázquez (2024). Bodnar (2021),

Estas amenazas emergentes no sólo afectan la disponibilidad de servicios, sino también la integridad y confidencialidad de la información crítica, comprometiendo directamente la seguridad nacional.

Consecuencias para la seguridad nacional y el Ejército Nacional de Colombia

Las consecuencias de las amenazas cibernéticas trascienden el ámbito digital, generando impactos de gran magnitud en la capacidad del Estado para garantizar la seguridad y el bienestar de sus ciudadanos y estas son:

- ✓ **Interrupción de servicios esenciales**: Los ataques de ransomware a proveedores de telecomunicaciones y salud, como el caso de IFX Networks en 2023, demostraron la capacidad de estos ataques para paralizar servicios críticos del gobierno y del Ejército, afectando la continuidad de operaciones (El Espectador, 2022).
- ✓ **Compromiso de información estratégica**: Los ataques APT han puesto en riesgo información sensible relacionada con operaciones militares, inteligencia y defensa. Según el Ministerio de Defensa Nacional (2023), estos ataques pueden afectar la capacidad de planeamiento estratégico y de respuesta táctica.
- ✓ **Impacto económico**: Las pérdidas asociadas a interrupciones y recuperación de incidentes cibernéticos pueden alcanzar millones de dólares, afectando presupuestos públicos y privados (OEA, 2022).
- ✓ **Desgaste institucional y pérdida de confianza**: La percepción de inseguridad digital y la falta de respuesta efectiva pueden minar la confianza en las instituciones del Estado y en las Fuerzas Armadas (Semana, 2023).
- ✓ **Efectos psicológicos y desinformación**: Además de los daños físicos y económicos, los ataques cibernéticos incluyen campañas de desinformación y manipulación psicológica que buscan polarizar a la sociedad y debilitar la cohesión nacional (Velázquez, 2024).

Capacidades actuales para enfrentar la guerra cibernética

Frente a estas amenazas, Colombia ha desarrollado algunas capacidades relevantes. A nivel gubernamental, el Centro de Operaciones de Seguridad Nacional (SOC), se encarga de la detección y respuesta a ciberamenazas en más de 6 400 entidades públicas (Ministerio TIC,

2025). Este centro utiliza herramientas avanzadas como Mandiant, ThreatQ y Tenable para monitorear incidentes y proteger las redes gubernamentales.

Tabla 5: Capacidades institucionales y tecnológicas

CATEGORÍA	ENTIDAD / INICIATIVA	DESCRIPCIÓN Y FUNCIONES
Capacidades institucionales	Comando Conjunto Cibernético (C3CN)	Creado en 2013 como parte integral de las Fuerzas Militares. Lidera la ciberdefensa militar, protege redes críticas de las Fuerzas Armadas y desarrolla operaciones y planes de contingencia.
	Centro Cibernético Policial (CCP)	Adscrito a la Dirección de Investigación Criminal e INTERPOL de la Policía Nacional. Se enfoca en prevención, detección y respuesta ante delitos cibernéticos que afectan a la ciudadanía e infraestructuras estratégicas.
	Agencia Nacional de Seguridad Digital y Asuntos Espaciales (ANSDAE)	En proceso de consolidación. Busca coordinar la seguridad digital a nivel estatal, unificando esfuerzos civiles, militares y privados.
Capacidades tecnológicas	CSIRT (Centros de Monitoreo y Respuesta a Incidentes)	Detectan tempranamente y mitigan ciberataques. Usan herramientas de análisis de tráfico, inteligencia de amenazas y simulación de escenarios.
Cooperación y alianzas internacionales	OEA – Programa de Ciberseguridad	Proporciona capacitación e intercambio de buenas prácticas en ciberseguridad.
	FIRST (Forum of Incident Response and Security Teams)	Participación de Colombia en foros internacionales para fortalecer respuesta ante incidentes.
	OTAN – Socio Global	Facilita acceso a metodologías avanzadas y ejercicios conjuntos de ciberdefensa.
Formación y talento humano	Fuerzas Militares / Escuela de Comunicaciones del Ejército	Programas de formación en ciberseguridad y ciberdefensa para oficiales y suboficiales.
	Universidad de los Andes / Universidad Nacional de Colombia	Programas académicos especializados en seguridad digital para formar profesionales en ciberdefensa.

Fuente: Ministerio de Defensa Nacional (2023). Centro Cibernético Policial (2024).

La capacitación también ha sido priorizada. Se han desarrollado diplomados y cursos de formación en ciberseguridad para uniformados de las Fuerzas Militares y de la Policía Nacional, incluyendo temáticas como análisis forense, gestión de incidentes y protección en la nube (Ministerio de Defensa Nacional, 2023). Sin embargo, expertos como Ramírez (2022)

advierten que persiste un déficit de talento especializado, así como una falta de cobertura en muchos sectores públicos y privados.

Uno de los pilares fundamentales para la construcción de capacidades de ciberdefensa en Colombia ha sido el fortalecimiento del marco normativo y la formulación de políticas públicas robustas. La Política Nacional de Confianza y Seguridad Digital (CONPES 3995 de 2020) constituye el referente más importante, estableciendo directrices para la gestión del riesgo digital y la protección de las infraestructuras críticas (Departamento Nacional de Planeación, 2020). Este documento establece la necesidad de:

- Fortalecer la gobernanza digital en el sector público y privado.
- Promover la cultura de ciberseguridad en todos los niveles.
- Consolidar la cooperación internacional y alianzas estratégicas para enfrentar amenazas transnacionales.

De manera complementaria, la Estrategia Nacional de Ciberseguridad ha delineado un marco de actuación para el desarrollo de capacidades técnicas y operacionales, impulsando la articulación entre los diferentes actores (Ministerio de Defensa Nacional, 2023).

Se resalta la necesidad de continuar invirtiendo en tecnología, formación y mecanismos de cooperación efectiva, con el fin de garantizar la resiliencia y la defensa integral del Estado colombiano.

Las capacidades actuales de Colombia para enfrentar la guerra cibernética son el resultado de un proceso continuo de maduración y adaptación a un entorno digital cada vez más desafiante. Si bien existen importantes avances en políticas, tecnología e

institucionalidad, las brechas persistentes y las amenazas emergentes exigen un compromiso sostenido para consolidar la soberanía digital y la defensa nacional.

Retos y perspectivas

Aunque Colombia ha avanzado en el fortalecimiento de capacidades como el SOC y el C3N, persisten desafíos críticos, la falta de cobertura al sector privado, la ausencia de un CSIRT nacional (Departamento Nacional de Planeación, 2020) y la incertidumbre sobre la dependencia institucional de la futura Agencia Nacional de Ciberseguridad (Ramírez, 2022). Como advierte Berdugo Sierra (2016), la guerra cibernética no es solo un reto técnico, sino estratégico y político, lo que exige consolidar la gobernanza digital, invertir en talento humano y cooperación internacional para garantizar soberanía y resiliencia frente a amenazas crecientes.

Si bien Colombia ha avanzado en el desarrollo de capacidades de ciberseguridad, las brechas institucionales y tecnológicas evidencian que aún no cuenta con un sistema integral capaz de responder de manera coordinada y efectiva a las amenazas emergentes. Superar estas limitaciones requiere no solo infraestructura y normatividad, sino también una visión estratégica que articule al sector público y privado, fomente la formación de talento especializado y fortalezca la cooperación internacional, garantizando así la soberanía digital y la resiliencia nacional frente a los desafíos de la guerra cibernética.

Evaluación de los efectos tecnológicos y geopolíticos para Colombia en un escenario de guerra cibernética y/o híbrida

La evolución de las TIC ha transformado profundamente la naturaleza de los conflictos contemporáneos, dando lugar a escenarios como la guerra cibernética y la guerra híbrida, donde se diluyen los límites entre lo civil y lo militar (Rid, 2020). Estas dinámicas convierten al ciberespacio en un componente central de la seguridad nacional y en un instrumento estratégico para actores estatales y no estatales que buscan influir en sus adversarios (Cavelty, 2014). La guerra cibernética, al permitir ataques a distancia con alto grado de anonimato, dificulta la atribución y respuesta, mientras compromete infraestructuras críticas, servicios esenciales y la soberanía estatal (Hoffman, 2007). A su vez, la guerra híbrida, mediante tácticas como sabotaje y desinformación, persigue la desestabilización sin un enfrentamiento militar directo (Velázquez, 2024).

En el caso colombiano, estas amenazas adquieren especial relevancia por su contexto geopolítico y su historial de conflictos internos asociados a actores armados ilegales y redes criminales. Las Fuerzas Militares y la Policía Nacional deben enfrentar el doble desafío de proteger tanto el territorio físico como los activos digitales estratégicos, cada vez más vulnerables ante operaciones hostiles (Centro Cibernético Policial, 2024). La interdependencia de sectores como energía, telecomunicaciones y transporte incrementa la posibilidad de efectos en cascada en caso de un ataque sostenido (Bodnar, 2021), lo que resalta la criticidad de garantizar resiliencia en infraestructuras vitales.

La posición de Colombia en el escenario regional, sumada a su alianza con Estados Unidos y la OTAN, convierte su infraestructura digital en un objetivo potencial para actores estatales con intereses estratégicos en la región (OEA, 2022). Esta convergencia de factores tecnológicos y geopolíticos exige un análisis multidimensional que permita anticipar riesgos, fortalecer la capacidad de respuesta y consolidar la resiliencia institucional. Evaluar los impactos tecnológicos, políticos y estratégicos de la guerra cibernética e híbrida es, por tanto, una necesidad crucial para preservar la soberanía y estabilidad del país.

Definición de guerra cibernética y guerra híbrida

La guerra cibernética es un tipo de confrontación que se lleva a cabo en el ciberespacio, empleando medios digitales y redes informáticas como armas para interrumpir, dañar o inutilizar infraestructuras críticas de un adversario, ya sea con fines políticos, económicos o militares (Rid, 2020). Esta forma de conflicto se caracteriza por su bajo costo, su capacidad de anonimato y su potencial para infligir daños significativos sin la necesidad de despliegue físico de tropas, lo que la convierte en una herramienta poderosa dentro de las estrategias de poder de los Estados y grupos no estatales (Cavelty, 2014). En este sentido, la guerra cibernética puede involucrar actividades como el espionaje digital, el robo de propiedad intelectual, la manipulación de sistemas críticos (como redes SCADA) y la alteración de información sensible para minar la confianza en las instituciones (Hoffman, 2007; Centro Cibernético Policial, 2024).

La guerra híbrida es un concepto más amplio que integra diferentes formas de agresión, combinando tácticas convencionales e irregulares con operaciones cibernéticas y psicológicas. Según Velázquez (2024), la guerra híbrida explota la ambigüedad y las zonas

grises, donde las fronteras entre la paz y la guerra se vuelven difusas, permitiendo que los actores maliciosos puedan desestabilizar a sus adversarios sin desencadenar una confrontación directa y abierta. Las tácticas de la guerra híbrida incluyen la desinformación, las campañas de manipulación en redes sociales, el uso de milicias o grupos proxy, y la ejecución de ciberataques coordinados que afectan tanto a objetivos militares como civiles. De acuerdo con la Organización de los Estados Americanos (OEA, 2022), este enfoque busca erosionar la cohesión social y la legitimidad del Estado, debilitando su capacidad de respuesta y generando un entorno de inestabilidad política y social.

En Colombia, la guerra cibernética e híbrida adquiere una relevancia especial debido a la diversidad de amenazas que enfrenta, desde actores criminales con crecientes capacidades digitales hasta posibles injerencias de Estados con intereses geopolíticos en la región (Centro Cibernético Policial, 2024). Comprender estos fenómenos resulta fundamental para anticipar sus efectos y establecer medidas de prevención y respuesta en un escenario cada vez más complejo y dinámico. El país ha avanzado en la digitalización de sectores estratégicos como energía, transporte, telecomunicaciones y defensa, lo que ha modernizado su infraestructura y mejorado la eficiencia en la prestación de servicios. Sin embargo, estos avances también han incrementado la superficie de ataque y, por ende, la vulnerabilidad frente a posibles agresiones cibernéticas (Ramírez, 2022).

El uso de software heredado, la falta de actualización tecnológica y la interconexión creciente entre sectores críticos amplían los riesgos de un ciberataque masivo (Bodnar, 2021). Estos riesgos se agravan en un entorno internacional caracterizado por la competencia entre potencias y el uso del ciberespacio como herramienta de poder (Nye, 2022). Así, un ataque exitoso podría paralizar servicios básicos, afectar la toma de decisiones estratégicas y

debilitar la confianza ciudadana en las instituciones. Esto significa que las vulnerabilidades tecnológicas no solo comprometen la operatividad, sino también la seguridad nacional y la estabilidad política (OEA, 2022).

Las infraestructuras críticas, como las redes SCADA y sistemas de control industrial, son objetivos prioritarios de actores maliciosos (Cavelty, 2014). En Colombia, la digitalización de estos sistemas ha optimizado procesos, pero también ha abierto nuevas puertas a la amenaza cibernética (Centro Cibernético Policial, 2024). Un ciberataque sostenido podría interrumpir servicios eléctricos, de agua, combustibles o transporte, impactando directamente a millones de ciudadanos (Ramírez, 2022). El sector financiero, por su parte, altamente dependiente de plataformas digitales, también es vulnerable a ataques que podrían desestabilizar la economía y disminuir la confianza de inversionistas nacionales e internacionales (Velázquez, 2024).

Estos efectos no serían solo económicos, sino también sociales y políticos. La OEA (2022) advierte que la interrupción prolongada de servicios esenciales tendría un fuerte impacto psicológico, generando caos, incertidumbre y debilitando la cohesión social. Por ello, proteger infraestructuras críticas y construir resiliencia tecnológica se ha convertido en una prioridad estratégica para garantizar la gobernabilidad en situaciones de crisis (MinTIC, 2023).

En escenarios de guerra híbrida, la información es un recurso clave y un blanco constante. Ataques orientados al robo de datos clasificados, protocolos de defensa o planes operativos afectarían la capacidad de reacción del Estado. Según Nye (2022), la manipulación y desinformación constituyen armas eficaces para dividir la cohesión institucional y social. Narrativas falsas o datos alterados podrían afectar decisiones críticas y

sembrar desconfianza entre las entidades de seguridad y defensa, agravando la inestabilidad interna.

A ello se suma la dependencia de Colombia de proveedores internacionales de tecnología, lo que amplía la exposición a vulnerabilidades en la cadena de suministro (Bodnar, 2021). La seguridad de las redes militares y policiales no depende únicamente de sus propios mecanismos de control, sino también de la confiabilidad de los proveedores externos. En este marco, el espionaje cibernético no solo compromete la dimensión operativa, sino que puede minar la moral institucional y la confianza ciudadana en la capacidad del Estado para garantizar la soberanía y el orden interno (Centro Cibernético Policial, 2024).

El ecosistema de ciberseguridad colombiano, aún presenta brechas significativas. La coexistencia de sistemas modernos con plataformas heredadas limita la interoperabilidad y ralentiza la coordinación táctica. En situaciones de conflicto, esta falta de integración tecnológica afecta la velocidad y precisión de la respuesta, elementos críticos en la defensa nacional.

El Comando Conjunto Cibernético (C3CN) y el Centro Cibernético Policial (CCP) se enfrentan a riesgos de saturación ante ataques distribuidos, como los DDoS, que podrían paralizar temporalmente sus operaciones (MinDefensa, 2023). La falta de redundancia tecnológica y de procesos automatizados de respuesta agrava la crisis, obligando a priorizar sectores críticos y dejando vacíos de seguridad que pueden ser explotados por actores hostiles (Bodnar, 2021). Estos vacíos, además de poner en riesgo la defensa digital de la nación, comprometen la coordinación interinstitucional en momentos de crisis.

Ante esta realidad, se vuelve indispensable adoptar estrategias de ciberdefensa proactivas basadas en la detección temprana, la respuesta automatizada y la resiliencia

tecnológica. La inversión en inteligencia artificial, ciberinteligencia y ejercicios de simulación fortalecería las capacidades nacionales, permitiendo enfrentar con mayor eficacia escenarios de guerra cibernética e híbrida. En conclusión, Colombia se encuentra en un punto crítico donde debe consolidar sus capacidades digitales, fortalecer la gobernanza y construir resiliencia para salvaguardar la seguridad nacional frente a amenazas que trascienden lo tecnológico y abarcan lo político, económico y social.

Implicaciones de diferente naturaleza para Colombia ante las actuales guerras cibernéticas y la amenaza potencial de verse inmersa en ellas

La evolución de las tecnologías digitales ha modificado profundamente la naturaleza de los conflictos contemporáneos. La guerra cibernética y la guerra híbrida, que combinan ataques cibernéticos, desinformación y acciones convencionales o irregulares, representan un desafío creciente para la seguridad y la estabilidad de los Estados (Rid, 2020; Hoffman, 2007). Estas formas de confrontación se caracterizan por su capacidad de operar en múltiples dominios físico, virtual y cognitivo, difuminando las fronteras entre tiempos de paz y de guerra (Nye, 2022). En el caso colombiano, estas amenazas adquieren especial relevancia debido a la creciente digitalización de sectores estratégicos y a las tensiones internas y regionales que configuran su entorno geopolítico (Centro Cibernético Policial, 2024).

Además, la utilización de herramientas tecnológicas como el hacking, los ataques de denegación de servicio (DDoS) y el espionaje digital permite a actores maliciosos estatales o no estatales— socavar la infraestructura crítica, influir en la opinión pública y debilitar la cohesión social (Velázquez, 2024). Las consecuencias no se limitan al ámbito tecnológico,

sino que también afectan la gobernabilidad, la estabilidad política y la economía del país (OEA, 2022). Por lo tanto, resulta fundamental examinar estas implicaciones de manera integral para comprender los riesgos reales y potenciales que conllevan las guerras cibernéticas e híbridas para Colombia.

1. Implicaciones tecnológicas

La infraestructura crítica de Colombia ha experimentado un notable proceso de digitalización. Esta modernización ha permitido mejorar la eficiencia de los sistemas y la prestación de servicios esenciales, pero también ha incrementado la superficie de ataque y ha expuesto nuevas vulnerabilidades (Centro Cibernético Policial, 2024). Las redes SCADA (Supervisory Control and Data Acquisition) y otros sistemas de control industrial, fundamentales para la operación de infraestructuras críticas, se han convertido en objetivos prioritarios para los actores maliciosos, ya que su alteración puede generar disrupciones significativas que afectan a la población y a la economía (Cavelty, 2014).

Por otro lado, la dependencia de tecnologías extranjeras para software, hardware y servicios digitales incrementa la exposición de Colombia a restricciones o manipulaciones geopolíticas, lo que podría limitar la capacidad de recuperación y adaptación ante ataques cibernéticos sostenidos (Bodnar, 2021). Además, la falta de inversión en soluciones locales y la carencia de una base industrial tecnológica sólida agravan esta vulnerabilidad, comprometiendo la soberanía tecnológica y reduciendo la resiliencia nacional (Velázquez, 2024).

Asimismo, la saturación de las capacidades de respuesta del Comando Conjunto Cibernético (C3CN) y del Centro Cibernético Policial (CCP) constituye un riesgo tangible,

especialmente en un contexto de guerra cibernética o híbrida. La interoperabilidad limitada entre las diferentes agencias y la coexistencia de tecnologías heredadas en las redes de mando y control de las Fuerzas Militares dificultan una respuesta coordinada y eficaz frente a ataques coordinados y sostenidos (Ramírez, 2022; Ministerio de Defensa Nacional, 2023). Esto podría traducirse en un debilitamiento de la capacidad de contención y mitigación de amenazas, afectando no solo la infraestructura tecnológica, sino también la seguridad nacional en su conjunto.

Implicaciones políticas y de seguridad nacional

La manipulación de la información y la difusión de noticias falsas constituyen una de las principales amenazas en escenarios de guerra cibernética e híbrida, al debilitar la confianza en las instituciones democráticas, fomentar la polarización social (Nye, 2022), y cuestionar la legitimidad de los procesos electorales (Velázquez, 2024). En el caso colombiano, donde la cohesión social es vulnerable, estas estrategias representan un riesgo significativo para la gobernabilidad, mientras que actores armados no estatales y redes criminales con capacidades cibernéticas emergentes añaden un desafío adicional al utilizar entornos digitales para coordinar actividades ilícitas, infiltrar redes estatales o atacar infraestructuras críticas (Ramírez, 2022).

El robo o alteración de información estratégica genera impactos directos en la toma de decisiones militares y gubernamentales, incrementando la incertidumbre y comprometiendo la seguridad operativa y nacional (Centro Cibernético Policial, 2024). Estas vulnerabilidades resaltan la urgencia de fortalecer la gobernanza digital y la ciberseguridad mediante coordinación interinstitucional, marcos normativos actualizados y una ciudadanía

sensibilizada, con el fin de construir una respuesta integral que preserve la estabilidad y la soberanía nacional (Bodnar, 2021).

Implicaciones económicas

Las repercusiones económicas derivadas de un conflicto cibernético o híbrido pueden ser profundas y sostenidas en el tiempo. La interrupción de servicios críticos, como los sistemas eléctricos, las redes de transporte y las telecomunicaciones, puede paralizar la actividad económica en múltiples sectores, afectando tanto a las grandes industrias como a las pequeñas y medianas empresas (Organización de los Estados Americanos (OEA), 2022). Estas disrupciones tienen un impacto directo en la productividad y en la confianza de los inversionistas, lo que puede traducirse en una reducción de la inversión extranjera y un deterioro en la competitividad del país (Cavelty, 2014).

Por otra parte, las pérdidas derivadas de ataques cibernéticos a sistemas financieros o a empresas estratégicas podrían alcanzar cifras millonarias, generando efectos en cascada que afecten al crecimiento económico y al empleo (Velázquez, 2024). Estas afectaciones también pueden tener un costo reputacional significativo para las empresas colombianas, que verían comprometida su posición en los mercados internacionales y su capacidad para atraer socios y clientes (Bodnar, 2021).

Asimismo, la dependencia tecnológica de Colombia respecto a proveedores internacionales de software, hardware y servicios digitales en particular de empresas de Estados Unidos, Europa y Asia representa una vulnerabilidad adicional en este contexto (Ramírez, 2022). En situaciones de tensión geopolítica, estos proveedores podrían imponer restricciones o condicionar el acceso a tecnologías críticas, lo que limitaría la capacidad de

recuperación y adaptación del país ante un conflicto cibernético sostenido (Bodnar, 2021). Esta falta de autonomía tecnológica aumenta la exposición a chantajes o bloqueos económicos que podrían agravar aún más el impacto económico de un ataque cibernético o híbrido (Ministerio de Defensa Nacional, 2023).

Finalmente, el costo de la ciberdefensa y de la recuperación tras un ciberataque suele ser elevado, exigiendo inversiones constantes en infraestructura, talento humano y capacidades de respuesta (Centro Cibernético Policial, 2024). Estas inversiones, aunque necesarias, pueden presionar el gasto público y desplazar recursos que podrían haberse destinado a otras prioridades de desarrollo económico y social (Velázquez, 2024). En consecuencia, las implicaciones económicas de la guerra cibernética e híbrida para Colombia subrayan la urgencia de fortalecer la resiliencia digital y de diversificar las fuentes tecnológicas para proteger la autonomía y la estabilidad económica nacional.

Implicaciones sociales y culturales

Finalmente, las amenazas cibernéticas tienen un impacto directo en la vida cotidiana de los ciudadanos, afectando no solo la seguridad digital, sino también la confianza social y la cohesión comunitaria. La pérdida de confianza en las instituciones encargadas de proteger los datos personales y la infraestructura digital genera un ambiente de incertidumbre y ansiedad en la población (Cavelty, 2014). Esta inseguridad digital puede traducirse en menor participación ciudadana en actividades en línea, debilitando procesos democráticos como la deliberación y la participación política

Por otra parte, la manipulación de información y la difusión de narrativas falsas a través de redes sociales y plataformas digitales constituyen un riesgo significativo para la

cohesión social. Estas campañas de desinformación pueden amplificar tensiones políticas y culturales preexistentes, exacerbando divisiones y polarizando a la sociedad. En el caso de Colombia, donde persisten desafíos relacionados con la desigualdad y la convivencia tras el conflicto armado, la propagación de noticias falsas podría erosionar aún más la confianza interpersonal y la solidaridad social (Nye, 2022).

Además, las amenazas cibernéticas afectan las prácticas culturales y el acceso a la información. La saturación de narrativas falsas o manipuladas no solo crea desconfianza hacia los medios tradicionales y digitales, sino que también limita el derecho a la información veraz y al debate público informado (Hoffman, 2007). Esto, a su vez, impacta la formación de opiniones y el desarrollo de una cultura cívica sólida, que son fundamentales para la democracia y la participación ciudadana.

En suma, las implicaciones sociales y culturales de la guerra cibernética e híbrida en Colombia resaltan la necesidad de fortalecer la alfabetización digital de la población y de promover una cultura de ciberseguridad y resiliencia comunitaria. Estas medidas no solo protegerán a los ciudadanos de amenazas tecnológicas, sino que también contribuirán a consolidar una sociedad más cohesionada y democrática.

Consideraciones finales

En síntesis, la amenaza de verse inmersa en guerras cibernéticas e híbridas plantea a Colombia desafíos interdependientes que exigen una respuesta integral y coordinada en todos los niveles de la sociedad. No se trata únicamente de fortalecer las capacidades tecnológicas de defensa, como la modernización de infraestructuras críticas o la actualización de sistemas de mando y control. Es fundamental también robustecer la cooperación internacional y

regional, aprovechando alianzas estratégicas y compartiendo inteligencia para contrarrestar las amenazas que trascienden las fronteras nacionales (Organización de los Estados Americanos (OEA), 2022).

La ciberresiliencia de las instituciones, constituye un pilar esencial para garantizar la continuidad de los servicios públicos y la protección de los activos estratégicos (Ramírez, 2022). Este esfuerzo debe ir acompañado de políticas que promuevan la reducción de la dependencia tecnológica de proveedores extranjeros, fomentando la innovación y el desarrollo de soluciones tecnológicas propias (Bodnar, 2021). La búsqueda de la soberanía tecnológica, en este sentido, se convierte en un objetivo prioritario para mitigar los riesgos de condicionamientos geopolíticos que pueden surgir en escenarios de conflicto cibernético o híbrido.

De igual forma, la alfabetización digital de la ciudadanía y de los servidores públicos resulta clave para enfrentar las implicaciones sociales y culturales de estas guerras modernas. Una sociedad informada, capaz de identificar la desinformación y consciente de las amenazas cibernéticas, puede contribuir activamente a fortalecer la cohesión social y a reducir la vulnerabilidad frente a ataques de manipulación informativa. En este contexto, la educación y la sensibilización digital deben ser parte integral de las estrategias nacionales de ciberseguridad y defensa.

Finalmente, estos esfuerzos deben enmarcarse en una visión amplia de defensa nacional y de soberanía tecnológica, que reconozca la interdependencia entre la dimensión tecnológica, la seguridad nacional, la estabilidad política y el bienestar social (Nye, 2022). Solo mediante un enfoque que combine la innovación tecnológica, la cooperación internacional y la educación ciudadana será posible enfrentar las múltiples dimensiones de

los conflictos contemporáneos y proteger los intereses nacionales de Colombia en el escenario global.

Análisis encuesta

La investigación incluyó una encuesta aplicada a personal experto en ciberseguridad y ciberdefensa, con el propósito de identificar percepciones y experiencias en el ámbito militar.

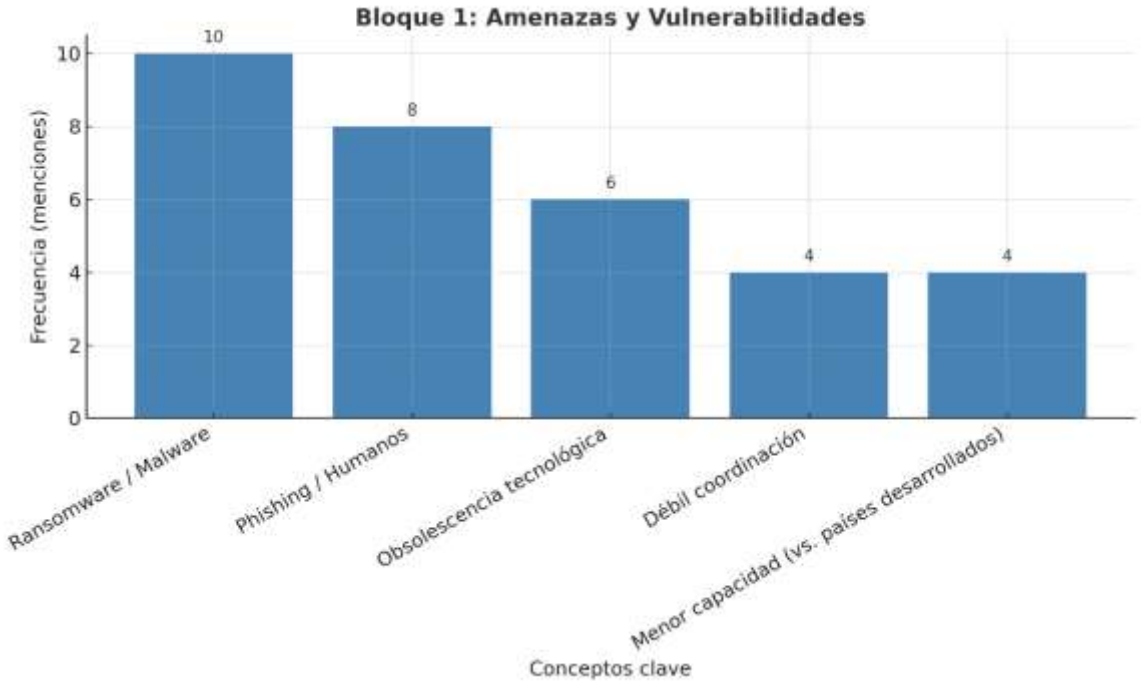
La metodología se basó en la recopilación de respuestas abiertas, donde se analizaron las menciones más frecuentes realizadas por los participantes. Este enfoque permitió priorizar los temas de mayor relevancia y construir un panorama claro de los riesgos y retos que enfrenta la institución.

El cuestionario estuvo organizado en 4 bloques principales:

- Amenazas y vulnerabilidades
- Impactos y casos relevantes
- Perspectiva tecnológica y geopolítica
- Estrategias y propuestas de mejora

De esta forma, los resultados reflejan tanto las preocupaciones inmediatas como las proyecciones estratégicas que deben considerarse en el fortalecimiento de la ciberdefensa nacional.

Bloque 1: Amenazas y Vulnerabilidades

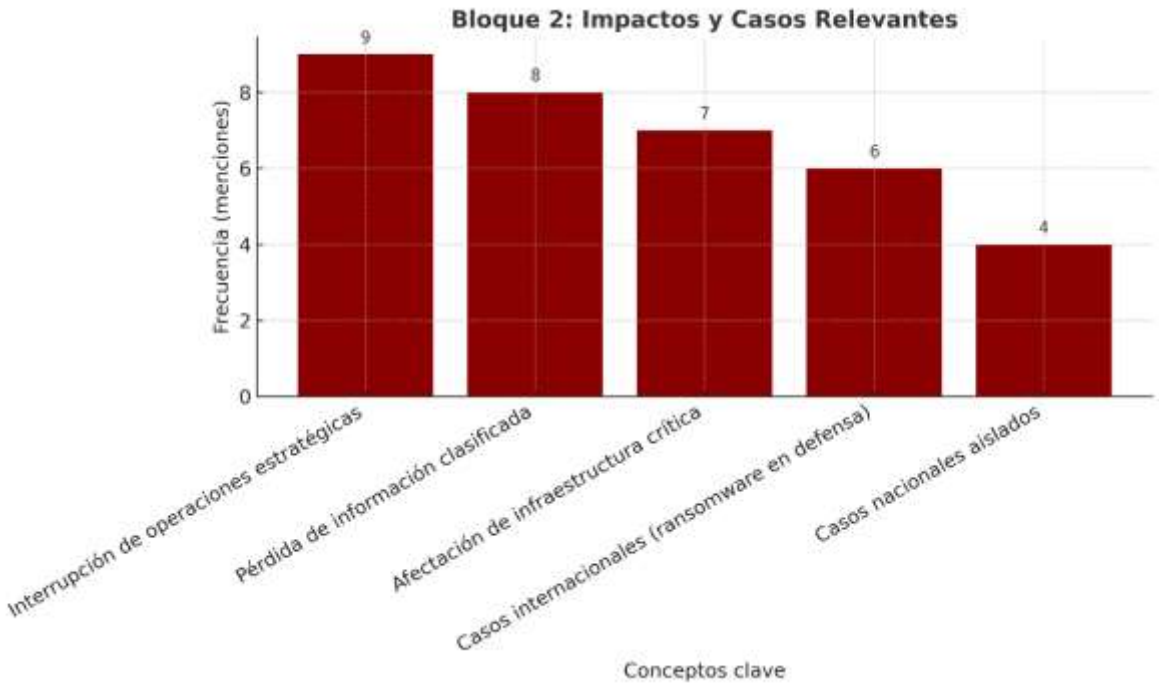


El gráfico muestra los conceptos claves más mencionados por los entrevistados en relación con las amenazas y vulnerabilidades que enfrentan Colombia. Refleja que el riesgo cibernético en Colombia se concentra en tres dimensiones principales:

1. Amenazas externas (ransomware, phishing, espionaje).
2. Vulnerabilidades internas (factores humanos y tecnología obsoleta).
3. Limitaciones estructurales (débil coordinación y menor capacidad tecnológica frente a potencias extranjeras).

Evidenciando la necesidad de fortalecer la capacitación del personal, la modernización tecnológica y la cooperación interinstitucional, pilares fundamentales para una ciberdefensa militar efectiva.

Bloque 2: Impactos y Casos Relevantes

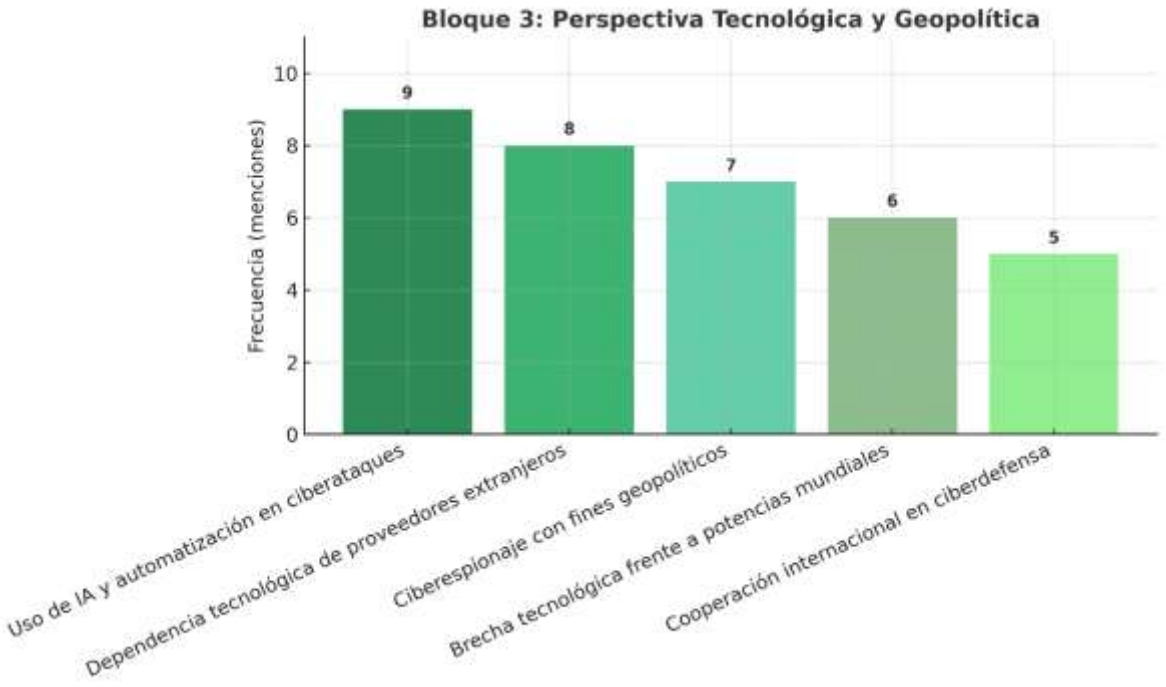


Refleja los impactos más mencionados y los casos relevantes considerados por los entrevistados al evaluar los riesgos de un ciberataque. Coinciden en que los impactos de un ataque cibernético trascienden lo digital y pueden afectar directamente la seguridad nacional.

1. La interrupción operativa y la pérdida de información clasificada son las amenazas más graves.
2. La referencia a casos internacionales muestra que Colombia debe aprender de experiencias externas para anticipar riesgos.
3. Aunque los casos nacionales son menores en escala, revelan la falta de preparación y protocolos robustos de defensa.

Este bloque evidencia la necesidad de protocolos de continuidad operativa, planes de contingencia y cooperación internacional para enfrentar escenarios de alto impacto.

Bloque 3: Perspectiva Tecnológica y Geopolítica



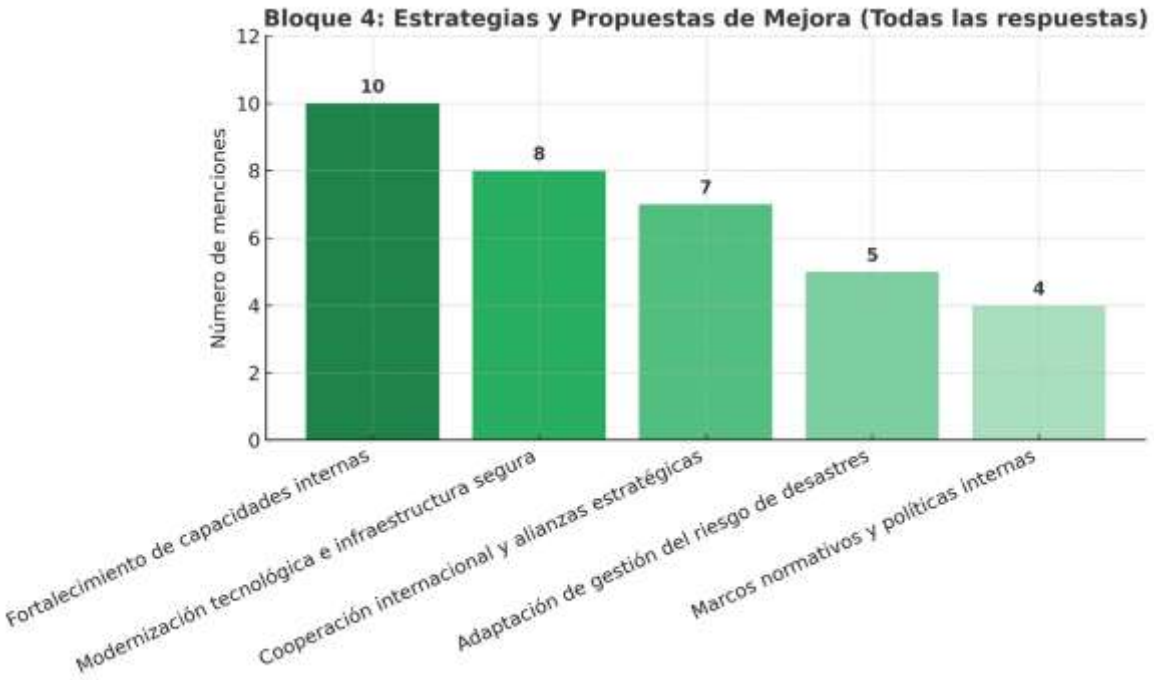
Este bloque recoge la visión de los entrevistados sobre cómo la tecnología y el entorno internacional inciden en la ciberseguridad de Colombia.

Los resultados muestran que el principal reto de Colombia no es solo responder a amenazas emergentes como la IA aplicada al cibercrimen, sino también reducir la brecha tecnológica y la dependencia externa.

1. El país enfrenta un escenario en el que los ataques con motivaciones geopolíticas podrían aumentar.

2. Para equilibrar esta asimetría, la cooperación internacional y la inversión en capacidades nacionales son fundamentales.

Bloque 4: Estrategias y propuestas de mejora



De muestran que la estrategia de ciberdefensa en Colombia debe ser integral, fortalecer sus capacidades internas y reducir su dependencia tecnológica externa, mientras avanza hacia una ciberdefensa colaborativa con actores internacionales y privados.

1. Talento humano como primera línea de defensa.
2. Apoyada en la modernización tecnológica para cerrar brechas de seguridad.
3. Sustentada en la cooperación internacional y alianzas multisectoriales.

Estas propuestas apuntan a un modelo integral donde la formación del talento humano, la modernización tecnológica y la cooperación estratégica se convierten en pilares para proteger la seguridad nacional.

Conclusiones

- La guerra cibernética constituye una amenaza real y creciente para la seguridad nacional de Colombia, pues no solo expone la fragilidad de sus infraestructuras críticas, sino que también impacta de manera profunda las dimensiones política, económica, social y cultural del país. Al tratarse de una confrontación asimétrica, invisible y de difícil atribución, este fenómeno coloca a la nación en un escenario de conflicto híbrido donde la soberanía y la estabilidad democrática pueden verse comprometidas sin un conflicto militar convencional. En este contexto, Colombia se convierte en un objetivo estratégico tanto para actores estatales como no estatales que buscan obtener ventajas y ejercer influencia, lo que evidencia la urgencia de fortalecer las capacidades de ciberdefensa y la resiliencia institucional frente a un desafío cada vez más complejo.
- El riesgo cibernético se presenta como una amenaza estratégica y dinámica de gran relevancia para la continuidad y eficacia de las operaciones militares, dada su naturaleza transversal, volátil y en constante evolución. Por ello, es fundamental adoptar un enfoque integral y proactivo que abarque todo el ciclo de gestión del riesgo, desde la identificación hasta la mejora continua, en lugar de limitarse solo a

la respuesta reactiva ante incidentes. En este sentido, la incorporación de un marco metodológico adaptado a la misión militar, como la gestión del riesgo de desastres, permite abordar las amenazas cibernéticas con una lógica coherente, facilitando su integración doctrinaria y cultural. Esta alineación fortalece la capacidad organizacional para responder eficazmente a incidentes cibernéticos de alto impacto, mejorando la resiliencia y la seguridad operacional.

- La creciente digitalización de las infraestructuras críticas en Colombia, en sectores esenciales como energía, salud, telecomunicaciones, transporte y sistemas gubernamentales, ha incrementado significativamente la exposición del país a ciberataques sofisticados y persistentes que ponen en riesgo la seguridad nacional. Evidenciando cómo estas amenazas afectan la continuidad operativa de múltiples entidades públicas y privadas, destacando la vulnerabilidad derivada de la obsolescencia tecnológica y la insuficiente inversión en ciberseguridad. A pesar de los avances institucionales, persisten desafíos importantes en la coordinación interinstitucional, la formación de talento especializado y la inclusión efectiva del sector privado en la estrategia nacional. Para garantizar la soberanía digital y la estabilidad socioeconómica.
- La importancia de la resiliencia cibernética constituye un valor esencial en el diseño de plataformas de ciberdefensa, al representar la capacidad organizacional de anticipar, resistir y recuperarse de incidentes cibernéticos, asegurando así la continuidad operativa y la protección de la misión en entornos adversos. no solo abarca el fortalecimiento de controles técnicos, sino también la consolidación de

procesos de entrenamiento y capacitación del personal, elementos críticos para mantener la eficacia en la respuesta ante amenazas complejas. La gestión del riesgo cibernético debe entenderse como un proceso continuo y dinámico, que promueve la actualización constante de amenazas y vulnerabilidades, y la incorporación de lecciones aprendidas para adaptarse a las realidades tecnológicas y geopolíticas cambiantes. el éxito de una estrategia de resiliencia cibernética radica en su capacidad integradora y adaptativa, alineando tecnología, procesos y cultura organizacional para sostener una defensa robusta en un escenario cibernético en constante evolución.

- El fortalecimiento de la cultura de ciberseguridad es crucial para el éxito de cualquier plataforma de defensa digital, ya que no solo depende de la tecnología, sino de la activa participación, sensibilización y disciplina de todos los integrantes de la institución. La formación constante y la creación de una cultura organizacional que valore la protección de la información como un activo estratégico son fundamentales para respaldar la seguridad de los sistemas y procesos. esta cultura contribuye decisivamente a la seguridad nacional, especialmente en un contexto donde el ciberespacio se ha convertido en un dominio clave de confrontación y defensa. La implementación efectiva de la plataforma no solo protege los sistemas de información militares, sino que también refuerza la soberanía tecnológica y la autonomía institucional, fortaleciendo la capacidad para responder a amenazas híbridas y dinámicas.

Referencias

Álvarez, D., & Castillo, J. (2021). Ciberseguridad y defensa nacional: Retos y oportunidades para Colombia. Universidad de los Andes.

Bendiek, A. (2018). European cyber security policy. Springer.

Bodnar, J. (2021). Cyber warfare and technological dependencies: Risks for small and middle-power states. Journal of Strategic Studies, 44(5), 811–829.

Bodnar, M. (2021). Cyber-physical systems and SCADA security. Springer.

Cavelty, M. D. (2014). Cybersecurity and threat politics: US efforts to secure the information age. Routledge.

Centro Cibernético Policial. (2024). Boletín de amenazas cibernéticas 2024. https://www.policia.gov.co/

Centro Cibernético Policial. (2024). Informe anual de ciberseguridad en Colombia. Policía Nacional de Colombia.

CISA. (2021). What is critical infrastructure? Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/topics/critical-infrastructure

Clarke, R. A., & Knake, R. K. (2012). Cyber war: The next threat to national security and what to do about it. Ecco.

Deibert, R. (2020). Reset: Reclaiming the internet for civil society. House of Anansi Press.

Departamento Nacional de Planeación. (2020). Política Nacional de Confianza y Seguridad Digital (CONPES 3995).

https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf

El Espectador. (2022, mayo 30). Registraduría confirma ataque cibernético durante las elecciones. https://www.elespectador.com/

García, P., & Moreno, L. (2023). Ciberseguridad y defensa en América Latina: Retos emergentes. Revista de Estudios Internacionales, 38(1), 45–60.

Giles, K. (2016). Russia's 'new' tools for confronting the West: Continuity and innovation in Moscow's exercise of power. Chatham House.

Healey, J. (Ed.). (2013). A fierce domain: Conflict in cyberspace, 1986 to 2012. Cyber Conflict Studies Association.

Hoffman, F. G. (2007). Conflict in the 21st century: The rise of hybrid wars. Potomac Institute for Policy Studies. https://potomacinstitute.org

Jasper, S. (2020). Russian cyber operations: Coding the boundaries of conflict. Georgetown University Press.

Kello, L. (2017). The virtual weapon and international order. Yale University Press.

Lewis, J. (2014). Cybersecurity and cyberwar: What everyone needs to know. Oxford University Press.

Libicki, M. (2007). Conquest in cyberspace: National security and information warfare. Cambridge University Press.

Libicki, M. C. (2009). Cyberdeterrence and cyberwar. RAND Corporation.

Mandiant. (2023). M-Trends 2023: Insights into today's threat landscape. https://www.mandiant.com/resources/m-trends

Méndez, C. (2020). Desafíos de la ciberseguridad en Colombia: Una perspectiva crítica. Revista de Estudios Políticos, 45(2), 35–52. https://doi.org/10.18566/rep.v45n2.a03

Ministerio de Defensa Nacional. (2023). Balance de capacidades del Comando Conjunto Cibernético (C3CN). Gobierno de Colombia.

Ministerio de Defensa Nacional. (2023). Informe de gestión en ciberseguridad y ciberdefensa. Bogotá, Colombia.

MinTIC. (2022). Política Nacional de Seguridad Digital. Ministerio de Tecnologías de la Información y las Comunicaciones. https://www.mintic.gov.co/portal/inicio/Politica-Nacional-de-Seguridad-Digital/

NATO. (2016). Warsaw Summit Communiqué. https://www.nato.int/

Nye, J. S. (2010). Cyber power. Harvard Kennedy School, Belfer Center for Science and International Affairs.

Nye, J. S. (2022). The future of power. PublicAffairs.

Observatorio Colombiano de Ciberseguridad. (2023). Informe anual de ciberseguridad. https://observatoriociberseguridad.gov.co/

Organización de los Estados Americanos. (2021). Estado de la ciberseguridad en Colombia. https://www.oas.org/

OEA. (2022). Ciberseguridad en América Latina y el Caribe: Avances y desafíos. Organización de los Estados Americanos.

Puyosa, I. (2022). Ciberconflictos y desinformación: Retos para la gobernanza democrática en América Latina. FLACSO.

Ramírez, J. (2022). Panorama de la ciberseguridad en Colombia. Revista de Estudios Estratégicos, 18(2), 45–60. https://doi.org/10.31012/rees.v18i2.2022

Ramírez, L. (2022). Ciberseguridad y defensa digital en Colombia: Estado actual y retos futuros. Universidad Nacional de Colombia.

Rid, T. (2013). Cyber war will not take place. Oxford University Press.

Rid, T. (2020). Active measures: The secret history of disinformation and political warfare. Farrar, Straus and Giroux.

Schmitt, M. N. (Ed.). (2013). Tallinn manual on the international law applicable to cyber warfare. Cambridge University Press.

Schmidt, M. (2013). Estonia's 2007 cyber attacks: Motivations and implications. Journal of Cybersecurity, 2(3), 155–164.

Semana. (2023, febrero 15). La Fuerza Pública denuncia ciberataques y campañas de desinformación. https://www.semana.com/

Singer, P. W., & Friedman, A. (2014). Cybersecurity and cyberwar: What everyone needs to know. Oxford University Press.

Velázquez, L. (2024). Incremento alarmante de ciberataques en Colombia. Panorama en ciberseguridad. https://www.panorama-ciberseguridad.com/

Velázquez, M. (2024). Amenazas cibernéticas y la seguridad nacional en Colombia. Pontificia Universidad Javeriana.

Weimann, G. (2015). Terrorism in cyberspace: The next generation. Columbia University Press.

Zetter, K. (2014). Countdown to zero day: Stuxnet and the launch of the world's first digital weapon. Crown.

Bodnar, C. (2021). Ciberseguridad en sistemas de control industrial: Riesgos y estrategias de mitigación. Revista Latinoamericana de Seguridad Informática, 15(2), 45–62.

Cavelty, M. D. (2014). Cybersecurity and the vulnerability of nations. Routledge.

Centro Cibernético Policial. (2024). Informe de ciberseguridad en Colombia 2023–2024. Policía Nacional de Colombia.

Hoffman, F. G. (2007). Conflict in the 21st century: The rise of hybrid wars. Potomac Institute for Policy Studies.

Ministerio de Tecnologías de la Información y las Comunicaciones. (2023). Avances de la transformación digital en Colombia. MinTIC.

Nye, J. S. (2022). Soft power and cyber power in international relations. Harvard Kennedy School.

Organización de los Estados Americanos (OEA). (2022). Ciberseguridad en América Latina y el Caribe: Riesgos, progreso y el camino a seguir. OEA.

Rid, T. (2020). Cyber war will not take place. Oxford University Press.

Velázquez, M. (2024). Infraestructura crítica y obsolescencia tecnológica en Latinoamérica. Bogotá: Editorial Universidad Nacional.