Capítulo 3

La cadena logística del Ejército Nacional de Colombia y ciberseguridad y ciberdefensa: atención a la academia*

DOI: https://doi.org/10.25062/9786287602700.03

Sergio Barrios Torres
Escuela Superior de Guerra "General Rafael Reyes Prieto"

Resumen: Este capítulo examina el interés estratégico del Ejercito Nacional de Colombia por los estudios en que se vincula la relación entre la ciberseguridad, la ciberdefensa y la logística militar; destaca la necesidad imperiosa de ampliar el conocimiento en este ámbito, tanto en la academia como en la actualización de la doctrina militar, para fortalecer la seguridad nacional; señala que las capacidades logísticas en apoyo de las operaciones militares son de gran importancia estratégica; indica posibles rezagos conceptuales y de acción que podrían convertirse en debilidades operativas, y sugiere reflexiones como base para futuras investigaciones y desarrollos doctrinales, con el objetivo de mejorar y proteger la cadena logística militar del EJC desde una perspectiva emergente de ciberseguridad.

Palabras clave: cadena de suministro; cadena logística; ciberdefensa; ciberseguridad; estrategia; logística militar.

* Capítulo de libro resultado del proyecto de investigación *"Tecnologías disruptivas, logística, seguridad y defensa nacional en el ciberespacio"*, del grupo de investigación *"Ciberespacio Tecnología e Innovación"*, de la Escuela Superior de Guerra "General Rafael Reyes Prieto", categorizado C por el Ministerio de Ciencia, Tecnología e Innovación (MinCiencias) y registrado con el código COL0181179. Los puntos de vista y los resultados de este capítulo pertenecen a los autores y no necesariamente reflejan los de las instituciones participantes.

Sergio Barrios Torres
Magíster en Logística Integral, Universidad Militar Nueva Granada, Colombia. Especialista en Seguridad y Defensa Nacional y especialista y diplomado en Comando y Estado Mayor, 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=0000-0001-7207-4605 - Contacto: **sergio.barrios@esdeg.edu.co**

Citación APA: Barrios Torres, S. (2024). La cadena logística del Ejército Nacional de Colombia y ciberseguridad y ciberdefensa: atención a la academia. En M. E. Realpe Díaz, & A. M. González González (Eds.), *Tecnologías disruptivas, logística y seguridad y defensa nacional en el ciberespacio* (pp. 77-110). Sello Editorial ESDEG. https://doi.org/10.25062/9786287602700.03

TECNOLOGÍAS DISRUPTIVAS, LOGÍSTICA Y SEGURIDAD Y DEFENSA NACIONAL EN EL CIBERESPACIO
ISBN impreso: 978-628-7602-69-4
ISBN digital: 978-628-7602-70-0
DOI: https://doi.org/10.25062/9786287602700

Colección Ciberseguridad y Ciberdefensa
Sello Editorial ESDEG
Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia
2024

Introducción

La logística militar es un elemento sensible y del más alto impacto en el sistema de seguridad y defensa del Estado. Esta importancia se interpreta en la intención de la actualización doctrinal del Ejército Nacional de Colombia que la destaca como una función que congrega la aplicación de la estrategia militar y la agrupación de labores y sistemas unidos por un propósito común expresados a manera de objetivos militares y tareas de apoyo a las operaciones militares terrestres y de defensa nacional. En dicha actualización doctrinal, se han destacado las funciones de conducción de la guerra, entre ellas la de sostenimiento, a la cual se atribuye el empleo de sistemas representados en personal, conocimiento, labores e infraestructura que proporciona apoyo y servicios destinados al cumplimiento de objetivos operacionales que proveen al comandante militar de todo nivel el ostentar "libertad de acción, extender el alcance operacional, y prolongación de la resistencia" ante los embates de las amenazas o el enemigo (Fuerzas Militares de Colombia, 2018, p. 66).

Sumado a lo anterior, el concepto de ciberespacio aborda y reúne tanto la ciberseguridad, como la ciberdefensa, de suerte que el ciberespacio es definido como un espacio compuesto y originado con el cual se vinculan el libre flujo de datos ubicado y transmitido por redes informáticas, que se fundó inicialmente para empleo de Fuerzas Militares (FF. MM.) y que posteriormente se trasladó y desarrolló al ámbito de empleo de las sociedades en general, de tal manera que exige interpretar en el mundo globalizado actual, las vulnerabilidades que se representan en los sistemas de información militar y no militar que pueden llegar a filtrar, corromper o destruir datos en beneficio político e igualmente militar, especialmente dando lugar a debilidades o falta de control a través acceder a cierta información o dar cuenta de conocimiento sobre información sensible, motivando incluso intervención,

alcance de certeza de acceso de capacidades y hasta influir en el comportamiento social mediante la tergiversación de narrativas o de la misma información (OTAN, 2020, pp. 1-2).

La importancia conceptual de la ciberdefensa se aprecia en lo expuesto por Sánchez (2020), quien, citando conceptos emanados de la Comisión de Regulación de Comunicaciones CARI, 2009, concibe la ciberseguridad como:

> conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos y usuarios contra los riesgos de seguridad correspondientes en el ciberentorno. (p. 35)

En consecuencia, se destaca el desempeño de lo que es la ciberseguridad, adicionando que esta corresponde a

> […] todas las actividades necesarias para la protección de las redes y sistemas de información, de los usuarios de tales sistemas y de otras personas afectadas por las ciberamenazas, lo anterior, según lo que se ha considerado desde el Parlamento Europeo (2019) y el Consejo de la Unión Europea, bajo la labor de la Agencia de la Unión Europea para la Ciberseguridad. (p.32)

Este capítulo examina el interés estratégico del Ejercito Nacional de Colombia por los estudios en que se vincula la relación entre la ciberseguridad, la ciberdefensa y la logística militar, abarcando, además, la función de conducción de la guerra de sostenimiento, por lo que esta investigación se propone formular razones que den cuenta de la importancia de la promoción del conocimiento, ante la sociedad académica vinculada para aumentar los aspectos temáticos específicos.

En el ciberespacio se han generado transformaciones que impactan directamente en la seguridad de la información, como lo evidencia el incremento de medidas preventivas contra ataques cibernéticos, la asignación de recursos, la adquisición de equipos y el desarrollo de conocimientos especializados, es decir, se observa una mayor dependencia tecnológica que incrementa las amenazas en el ámbito digital. Es fundamental, por lo tanto, que la academia focalice sus esfuerzos en fortalecer mecanismos de ciberdefensa y ciberseguridad, especialmente en lo que respecta a la seguridad de la cadena de logística militar de sostenimiento.

Esto implica ampliar el conocimiento sobre posibles amenazas que puedan comprometer las capacidades, ventajas y desventajas del sistema de apoyo operacional del Ejército Nacional de Colombia, el cual constituye un pilar en la defensa y seguridad del Estado.

Ante esta preocupación, los procesos de planeamiento y conducción de operaciones requieren de adaptabilidad, por lo cual es importante generar estrategias militares de superioridad en tiempo real sobre las diversas amenazas que afecten el desempeño normal del factor logístico militar, a causa de no entender las posibles afectaciones de cadenas de suministro del sector Defensa en Colombia.

Ciberseguridad, ciberdefensa y logística militar del Ejército Nacional de Colombia

Muchas funciones y desempeño de la logística militar dependen hoy del apoyo de redes informáticas y del uso de información y flujos de bienes, cuyo funcionamiento estriba en un entorno complejo que incluye el manejo de capital humano, infraestructuras, sistemas de entrenamiento, sostenimiento de capacidades, sistemas de adquisición y administración de *stocks,* así como de los modos y medios de suministro y abastecimientos de diversas clases, que requieren administrarse por estar ubicados de manera estratégica, adaptados a entornos definidos por capacidades propias y por el ambiente operacional.

Por lo tanto, al realizar las acciones militares de defensa y de seguridad por parte del Ejército Nacional, se ha desarrollado una cadena logística en constante evolución, pasando de acciones de simple adquisición de suministro de bienes y servicios, hasta lograr un mejoramiento productivo, administrativo y operacional táctico como apoyo estratégico. Hoy la logística militar del EJC acuña parte de su desempeño sobre el acceso a las tecnologías de la información. Por lo anterior y no siendo ajena la dependencia tecnológica, se establece una creciente necesidad de resistir ante todo tipo de arremetidas informáticas o de ciberataques que favorecen latentemente la acción de las amenazas o de adversarios sobre la obtención de información sensible representada en activos estratégicos y que permitirían evidenciar las capacidades de apoyo logístico y de sostenimiento propio.

¿Qué tanto puede afectar la falta de desarrollo académico y doctrinal sobre la relación *logística militar, ciberseguridad y ciberseguridad* en apoyo de las operaciones del Ejército Nacional de Colombia? Ante este interrogante, el presente capítulo analiza la necesidad de aumentar el enfoque investigativo y académico en apoyo

a la doctrina que aborde la relación entre la logística militar, la ciberseguridad y la ciberdefensa.

En respuesta a la problemática planteada y al interrogante central, se establece un objetivo general que servirá como eje conductor de la investigación. Este objetivo se alcanzará mediante análisis intermedios específicos para promover un desarrollo óptimo de la propuesta de investigación. Se emprenderá un camino destinado a resaltar la importancia de ampliar el conocimiento académico sobre la relación entre ciberseguridad, ciberdefensa y logística militar, tanto en el ámbito académico, como en el doctrinal y operacional del EJC.

En complemento, se da lugar a alcance de análisis u objetivos intermedios, por lo cual se estima inicialmente: conceptuar y establecer la importancia de la relación ciberdefensa, ciberseguridad y cadena logística del EJC como factor determinante de su cadena de suministro y fortalecer el desempeño de la función de conducción de la guerra (FCG) sostenimiento.

En una segunda instancia, se da lugar a determinar y justiciar la adopción o consideración del abordaje interpuesto por diferentes medios y conceptos, sobre los cuales se sustenta la importancia de orientar a la academia en la investigación y mayor desarrollo del conocimiento puesto sobre la relación entre la cadena logística del EJC y la ciberseguridad, como factor de mejoramiento sobre el desempeño de la cadena de suministro, el desempeño del sistema integrado de gestión logística y, obviamente, la FCG sostenimiento.

Además, y como último propósito intermedio y específico, se pretende formular un análisis que establezca fortalezas, debilidades, oportunidades y amenazas sobre la cadena logística del EJC, su cadena de suministro, a partir del aumento del desarrollo de la investigación y estudio vinculado a la relación ciberseguridad, ciberdefensa y cadena logística del EJC, para obtener una herramienta de apoyo al desempeño de su cadena de suministro.

Métodos

Esta investigación, de enfoque cualitativo, se basa en un área del conocimiento en temas específicos: la logística, la logística militar, la ciberseguridad y la ciberdefensa, por lo que, según Hernández et al. (2014)

> La inmersión inicial en el campo significa sensibilizarse con el ambiente o entorno en el cual se llevará a cabo el estudio, identificar informantes que aporten

> datos y guíen al investigador por el lugar, adentrarse y compenetrarse con la situación de investigación, además de verificar la factibilidad del estudio. (p. 8)

De ahí que el presente análisis implique un proceso inductivo para explorar diferentes perspectivas conceptuales y teóricas. Se recopilan datos, teorías y opiniones diversas para analizar el problema central y responder a la pregunta problema destacada, siguiendo los objetivos intermedios planteados. Además, se consideran la experiencia y las opiniones del autor, así como la contribución conceptos y opiniones relevantes. De esta manera

> postula que la "realidad" se define mediante las interpretaciones de los participantes en la investigación respecto de sus propias realidades. De este modo, convergen varias "realidades", por lo menos la de los participantes, la del investigador y la que se produce en la interacción de todos los actores. (Hernández et al., 2014, pp. 8-9)

A partir de la recolección de datos estructurados en fuentes abiertas, como artículos de investigación y publicaciones especializadas, relacionadas con la logística militar, la ciberseguridad y la ciberdefensa, se formula un enfoque desde la visión del autor especialista en logística militar, que identifica información destacada utilizada como base de exploración que sirve además como antecedente del tema propuesto.

Además, se utilizan dos técnicas adicionales: análisis bibliográfico-documental y análisis histórico-lógico. El análisis bibliográfico consiste en seleccionar y recopilar información de diversas fuentes, como bibliotecas y centros de documentación, para luego analizar y presentar resultados, contribuyendo así a la construcción de conocimiento (Matos, 2020, párr. 8).

Por otro lado, Rodríguez & Pérez (2017) plantean que el análisis histórico-lógico es un método o destreza donde

> lo histórico y lo lógico están estrechamente vinculados. Lo lógico para descubrir la esencia del objeto requiere los datos que le proporciona lo histórico […] lo lógico debe reproducir la esencia y no limitarse a describir los hechos y datos históricos. Estas ideas se resumen en que lo lógico es lo histórico liberado de la forma histórica […] El análisis de la práctica investigativa posibilita afirmar que este método se emplea comúnmente cuando se buscan los antecedentes del problema científico y durante la elaboración de los fundamentos teóricos y metodológicos de la propuesta de solución al problema […] su

> finalidad es la búsqueda de información como parte del momento de la red de indagaciones. (pp.189-190)

Por lo tanto, ante la acumulación y apropiación de datos y gestión documental de obtención de información considerada como relevante se pretende una evaluación a partir de consideraciones de valoración de información basada en principios como los establecidos por (Hitzler & Honer, 2016):

> Las técnicas fundamentales de la recopilación de datos cualitativa consisten en observar los acontecimientos, conseguir documentos […] La observación sirve para obtener impresiones sensoriales, hacer experiencias y registrar fenómenos. Los enfoques de la observación se deberían dar durante el proceso de investigación, formando las teorías, y esto con una tendencia ascendente: las observaciones se precisan y sistematizan en forma de embudo. (p. 63)

De esta manera, se revisaron más de ochenta fuentes, como artículos científicos, documentos académicos y oficiales, que abordan los temas de ciberseguridad, ciberdefensa y logística militar. Se seleccionaron las más relevantes para este documento y se incluyen en la bibliografía.

Se procura hacer una correlación entre la información recolectada y los objetivos trazados, lo cual se enuncia como lo aborda Martínez et al. (2023), un enfoque metodológico donde: "el analista toma un conjunto de decisiones para construir conocimiento ya que, se propone una secuencia sistemática y lógica […] Se aporta solidez en el proceso, en la robustez de la evidencia científica y en las competencias del investigador" (p. 79), lo anterior se orienta al cumplimiento del primer objetivo específico.

Se propone destacar la importancia de desarrollar un enfoque conceptual que explore la relación entre los temas principales. Se emplea un enfoque comparativo para evaluar cómo la ciberseguridad y la ciberdefensa afectan el desempeño de la logística militar y la cadena de suministro del EJC, analizando sus contribuciones científicas y sus similitudes y diferencias de aplicación, "lo que supone una operación mental como lo es observar, analizar e interpretar elementos que posteriormente permiten generar significados y producir conocimiento" (Jiménez, 2021, p. 181).

Se comparan factores de poder con multiplicadores en teorías y prácticas de ciberseguridad. Estas aplicaciones conceptuales y consideraciones generan el

establecimiento del objetivo mediante un enfoque constructivista y un método observacional para recopilar información simple y analizar variables. Esto ayuda al investigador a enriquecer el documento encontrando diferencias e interpretaciones personales (O´leary, 2014, citado por Rodríguez, s.f., pp. 33-35), dando lugar al porqué de proponer mayor aproximación y preocupación de llevar la ciberdefensa sobre la cadena de suministro en el sistema integrado de gestión logística, mediante ampliación doctrinal e investigación.

Consecuentemente, a fin de lograr el tercer asunto por destacar de la presente indagación y análisis, se aborda de una manera reflexiva, mediante un análisis FODA. Lo que permite establecer sobre el eje temático y profundizar en la academia la relación ciberseguridad, ciberdefensa y logística militar, una comprensión sobre debilidades, oportunidades, fortalezas y amenazas, en este caso para las FF. MM. y el conjunto, lo que representa para la estrategia militar y la seguridad y defensa nacional, como aborda Ponce (2007, pp. 114-117), quien estima una evaluación de los factores fuertes y débiles que diagnostican la situación interna de una organización o propósito, muestra de evaluar oportunidades y amenazas. El modelo por emplear se evidencia en la Figura 1.

Figura 1. *Matriz análisis FODA*

ANÁLISIS FODA	**Fortalezas** Anotar elementos propios a destacar	**Debilidades** Anotar elementos que deben revisarse/ mejorarse
Oportunidades Anotar elementos externos que pueden significar oportunidad	**Estrategias SO** Uso de fortalezas para tomar avance de las oportunidades	**Estrategias DO** Superar debilidades para tomar ventaja de las oportunidades
Amenazas Anotar elementos representan una ventaja externa y que pueda afectar intereses	**Estrategias FA** Uso de fortalezas para reducir amenazas	**Estrategias DA** Minimizar debilidades y evitar amenazas

Fuente: elaboración propia con base en AMCES (2023).

Relación logística, ciberseguridad y ciberdefensa

Logística y logística militar

El vaivén, la dinámica y la transformación de los conflictos, la guerra y las amenazas exigen hoy mantener una evolución constante debido al devenir de un mundo en constante movimiento. El ritmo frenético que la evolución de la tecnología influye el impulso de nuevas nociones, ordenamientos, métodos y medios, que se colocan a disposición de la logística a manera de instrumentos en procura del mejor sistema de apoyo a estructuras militares en su encargo estatal de proveer seguridad y defensa.

El origen de la logística integral y empresarial se dio por la preocupación de pulir movimientos de tropa, alojamiento y sostenimiento de estas a gran escala, y aprovisionamiento de pertrechos requeridos en empeños militares. De ahí que el barón de Jomini, al servicio de Napoleón I y del zar de Rusia sobre el siglo XIX, consideró la logística entre las tres estructuras por destacar al arte de la guerra, además de la táctica y la estrategia (Montanyá, 2021), por lo tanto, la logística militar se puede definir como

> parte de la ciencia y arte de la guerra, y como ella, ha sido parte de la historia de la humanidad, con la cual ha evolucionado, y se ha refinado hasta convertirse en una ciencia de aplicación a diferentes procesos de apoyo a las fuerzas operativas. La logística militar se define como "la parte del arte de la guerra que tiene por objeto proporcionar a las Fuerzas Armadas los medios necesarios para satisfacer adecuadamente las exigencias de la guerra". (FAC, 2016, p. 2)

La constante evolución de la logística luego de incorporarse al mundo empresarial impone conceptos novedosos y creación de entidades del orden mundial enfocadas en su estudio como el Council of Supply Chain Management Professionals, CSCMP, (2023) que en la actualidad propone unión de esfuerzos entre profesionales en gestión de la cadena de suministro en el mundo estudiando y aumentando el aumento de educación y desarrollo apropiados en logística.

La actualización doctrinal del Ejercito Nacional de Colombia formula que, si bien la logística militar como concepto no desaparece, sí agrega de manera destacada y evolutiva un actuar orientado en mayor dimensión sobre la aplicación y

desempeño de la logística en el campo militar; tal es el caso de organizaciones como el EJC, donde la logística se considera como

> el planeamiento y ejecución del movimiento y el apoyo de las fuerzas. Implica tanto el arte militar como la ciencia, saber cuándo y cómo aceptar el riesgo, priorizar una mirada de requerimientos y equilibrar recursos limitados, todo requiere arte militar, mientras que la comprensión de las capacidades del equipo incorpora la ciencia militar. (EJC, 2016, p. 8)

Es de enfatizar que la logística militar ha sido ampliamente definida y constituye todo el poder de soporte estructural operacional para dar lugar a lo que puede ser posible en el planeamiento estratégico y táctico de las operaciones militares, hasta el punto de considerar que casi todo es factible por desarrollarse en el campo de la táctica militar, pero solo la logística permite en gran proporción que sea posible hacerlo y hasta donde se llega.

> La actualidad de las áreas de manejo de la logística militar y el soporte que se surte mediante ella acumula responsabilidades basadas en el planeamiento y conducción de operaciones de sostenimiento que involucran producción, logística inversa, adquisición, apoyo general de ingenieros, almacenamiento, servicios en campaña, transporte, entrega, y mantenimiento. (EJC, 2018, p. 28)

Lo que indica que este amplio espectro de integración de funciones y responsabilidades se orienta a suplir necesidades complejas, para lo cual la logística es responsable de la obtención y administración de flujos de información sensible que exigen máxima seguridad tanto de sí, como de sus procesos y procedimientos. Sobre esta información y manejo de sus infraestructuras recae el peso que debe considerarse de uso crítico, por lo que el conocimiento de esta información da lugar a una conducción y manejo amparado bajo el dominio de la ciberseguridad, dadas las condiciones de ventaja que deben destacar y de su celo, ante las amenazas y capacidades que representan o conocimiento que se estima de su funcionamiento, o del denominado sistema integrado de gestión logística, denominación empleada dentro del EJC y sobre el que se especifican los flujos transversales del ejercicio sobre el que fluye su estructura.

Ciberseguridad y cadena de suministro

En cumplimiento de la estructura del presente documento, se establece que existe la realidad de colocación del ciberespacio como el quinto dominio de la seguridad.

Dicha categoría ha traído consigo la necesidad de asegurarlo, intención que se dinamiza ante la exigencia de variadas modalidades de irrupción del mismo ciberespacio. Además, se ha afianzado como concepto de poder y de defensa, a lo que se suma el uso de novedosas tecnologías evidenciando recursos al alcance de diversos actores que hacen parte del sistema internacional a manera de herramienta del equilibrio del poder, por lo tanto

> es una práctica cada vez más necesaria en un mundo cada vez más digitalizado y, por ende, más desprotegido ante los ataques informáticos, tanto internos como externos. Esto lo convierte en una actividad cada vez más atractiva para las organizaciones cibercriminales por los grandes beneficios que reporta. (UNIR, 2022, s.p.)

Así, organizaciones de todo tipo aplican medidas para dar cara y anticipadamente, ante embates, pero sobre todo para fortalecer acciones de detección y corrección que generen confianza y libre desempeño de acciones y actividades propias de la organización. Análogamente, crear un escenario diseñado desde el ámbito militar da cuenta de su relación de la ciberseguridad a partir de combatir riesgos y amenazas diversas, motivadas por enemigos a la paz, el equilibrio de las regiones, la proliferación del terrorismo y varias capacidades de dañar estructuras criminales trasnacionales, que pretenden encausar brechas sobre las capacidades militares de los Estados y alianzas estratégicas. Ante lo anterior

> La alta dependencia tecnológica de nuestra sociedad es una realidad constatable, siendo imprescindible para el buen funcionamiento de los Estados, sus fuerzas y cuerpos de seguridad y sus infraestructuras. Esta dependencia seguirá aumentando en el futuro. Las tecnologías de la información hacen posible casi todo lo que nuestras FAS necesitan: apoyo logístico, mando y control de sus fuerzas, información de inteligencia en tiempo real y un largo etcétera. (Díaz, 2011, p. 220)

El ciberespacio debe ser considerado, entonces, como una dimensión sobre la cual se trasladan los conflictos y las guerras restringiendo los límites de acción de las amenazas, y este uno de los principales motivos que requieren de toda la atención de los estrategas militares, y que pueden ser determinantes ante la intención de doblegar al contendiente o enemigo. Caso contrario la carencia o desestimación del empleo del ciberespacio en contra de las acciones de la fuerzas de defensa y seguridad de los estados, pueden suponer una amenaza significativa

autoconstruida debido a los bajos costos requeridos para causar daños a partir del empleo y uso de hábiles programadores que estén en capacidad de encontrar las más sensibles vulnerabilidades de todos tipo de sistema de defensa, de armas y, sobre todo, de los sistemas destacados para el apoyo logístico, que pueden dar lugar a poner en evidencia ubicaciones estratégicas logísticas, y hasta información relacionada con la disposición de entrenamiento de sostenimiento y las formas de hacerlo.

En su recopilación de elementos y eventos introductorios a un estudio a manera de estado del arte sobre ciberseguridad, Joyanes (2011) destaca la relación entre la ciberseguridad y el sector militar, mencionando, entre otros aspectos, que el ciberespacio y la ciberdefensa obedecen a un campo de batalla, actuando como activo nacional estratégico, que obliga a la toma de decisiones encausadas a defender las redes militares, que incluyen dominios de aire -tierra-mar-espacio y ciberespacio en lo relativo a la guerra, y subordinados a la seguridad nacional (p. 31).

De la misma manera, se hace una aproximación a situaciones consideradas como catastróficas generadas a partir de la carencia de estrategias y mal entendimiento tras ataques cibernéticos, sobre los cuales se relacionan con secretos militares logísticos y nucleares y donde además se encierran accesos a informaciones de logística militar no considerada inicialmente como clasificada, que dan apertura al conocimiento de asuntos sensibles que incluyen sistemas económicos y de adquisición y da lugar al acomodo de términos como el de las ciberarmas, haciendo alusión a equipos utilizados en complemento a las armas convencionales propias de los teatros de operaciones (p. 34), en intentos de controlar ciberataques de alto impacto.

Ciberdefensa y cadena de suministro

Ante lo ya destacado, existe la intención de desarrollar componentes que alerten e intervengan bajo detección anticipada y reactiva de intrusiones aisladas o no a las redes de flujo de información reservadas y prevenir potenciales ataques cibernéticos de organizaciones u otras naciones del orden foráneo.

Así las cosas, el concepto de *ciberdefensa* se establece como una medida ante un ciberataque, por lo tanto y en términos prácticos simples, corresponde a una renuencia sobre una acción deliberada para causar perjuicio o una consecuencia sobre algún considerado adversario orientado a obtener efectos a favor en el ámbito de las operaciones militares propia o particularmente dicho. IBM (s.f.) establece que "los ciberataques son intentos no deseados de robar, exponer,

alterar, inhabilitar o destruir información mediante el acceso no autorizado a los sistemas". Ahora bien, y en apoyo a lo anterior, la Junta Interamericana de Defensa, mediante Ganuza (2020) establece que la ciberdefensa es capacidad organizada y preparada para combatir en el ciberespacio. Comprende actividades defensivas, ofensivas y de inteligencia. (p. 14), y la ciberdefensa militar, como la unidad que aproxima: la ciberdefensa al arte militar del empleo del ciberespacio y a las operaciones militares en el ciberespacio (ciberoperaciones) y propone una taxonomía de los diferentes tipos de ciberoperaciones (p. 8).

Para la Unión Internacional de Comunicaciones (UTI), la ciberseguridad es "el conjunto de herramientas políticas, guías de acción, abordajes de gestión, acciones, mejores prácticas y tecnologías empleados para proteger la disponibilidad integridad y confiabilidad de activos en las infraestructuras interconectadas" (UTI, 2018, p. 13).

La relación entre ciberdefensa y ciberseguridad, de manera específica para el ámbito militar debe entenderse como la primera, en función de actuar mediante entidades estatales, orientadas bajo políticas que interactúan organizadamente para luchar en el ciberespacio, bajo acciones de defensa, acciones operacionales ofensivas dentro de la inteligencia militar. La segunda es, en consecuencia, las medidas formuladas y acogidas dese la estrategia militar operativa y táctica, establecidas y destinadas a la prevención o mitigar hasta la manera mínima posible afectaciones sobre los sistemas de manejo de información sensible y no sensible que permita el conocimiento detallado de los medios militares (equipos, infraestructura, manejo de personal y capacidades) de un nación o Estado empleados para su defensa y seguridad. Todo lo anterior, entendido y relacionado con las acciones provistas desde la logística militar para administrar los recursos de todo orden requerido para adelantar cualquier plan u operación militar empleando una capacidad bélica ostentada.

Logística militar, ciberdefensa y ciberseguridad

Sobre este particular, se otorga alcance a las menciones del Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN (CCDCOE, 2023), que coloca de presente la importancia dentro de la alianza, en torno a

> el ciberespacio como un ámbito de operaciones en el que la OTAN debe defenderse con tanta eficacia como lo hace en el aire, la tierra y el mar […] que arrojan más luz sobre las implicaciones prácticas, una disuasión y defensa

> más amplias [...] la integración en la planificación operativa y las operaciones y misiones de la Alianza [...] organización más eficaz de la ciberdefensa de la OTAN y mejor gestión de recursos, habilidades y capacidades. (s.p.)

De ahí que, así como para organizaciones tan poderosas, y que asumen el aspecto de las amenazas inmersas en el ciberespacio, dan cuenta del entorno del desempeño en operaciones militares, y la influencia de la seguridad en las mismas sumado al gran desafío puesto sobre la amplia gama de actores, intereses, medios y capacidades conjuntas. Es en esta proporción en que se debe asumir la máxima seguridad sobre la información enfilando el interés en el cumplimiento de la misión y ejercer control para cumplir los propósitos deseados.

La preparación en ciberdefensa y ciberseguridad militar requiere decisión, con base en los preceptos emanados del concepto nacional de lo que debe ser la ciberdefensa nacional y, por lo tanto, debe apoyarse en otros campos de acción del Estado, como el económico y el de la logística nacional en sustento de la logística militar y de sostenimiento, primero como medio de financiamiento y segundo por ser parte de la estrategia de movilización nacional (integración de los campos del poder del Estado para enfrentar una guerra) en caso de requerirse.

La anterior discusión orienta la necesidad de asociar la ciberdefensa y la ciberseguridad con la logística militar, logrando unión de esfuerzos conceptuales, organizacionales y destacados para aumentar el desempeño de las operaciones de defensa y seguridad. De esta manera, deben fluir las ciberoperaciones militares[1] fundadas en la misión del EJC pensando en causar efectos que aporten a los objetivos de la misión logística de sostenimiento. Así, se correlacionan las ciberoperaciones con un eje articulador a partir de capacidades técnicas, logísticas y administrativas requeridas en beneficio redundante para planeamiento y conducción de operaciones militares partiendo de la premisa de fortalecer la seguridad de redes y sistemas de apoyo, causando sorpresa e iniciativa y obstaculizando intenciones de amenazas y enemigos que intenten dar cuenta de los conocimientos en ventajas logísticas y su soporte propio.

La relación entre logística militar y ciberseguridad se alcanza bajo la siguiente condición: la logística militar asume técnicas que enmarcan la planeación, realización y vigilancia de flujos de todo tipo de suministros y pertrechos, recursos físicos y financieros, además de personal especializado en satisfacer elementos

[1] Las ciber operaciones son operaciones militares que se desarrollan en el ciberespacio con los mismos objetivos que las que se producen en las dimensiones clásicas del teatro de operaciones: adquirir ventaja, conservarla, situar al enemigo en desventaja y explotarla (Real Instituto Elcano, 2014).

esenciales y que soportan necesidades de las operaciones militares. Es esta disciplina considerada entonces como eslabón primordial que garantiza el buen desempeño y fluidez de equipos críticos y comunes, sus suministros y máximo grado de disponibilidad en el instante y terreno apropiado. En la actualidad y en la era digital, la logística militar igualmente se afecta a causa de ciberataques, donde estos estriban en influencia de tecnologías de la información y comunicación (TIC), que le permiten gestión y coordinación de sus medios apropiados, de ahí la importancia de resguardarlos impidiendo que sean vulnerables ante ataques cibernéticos y robo o conocimiento de su información.

Lo anterior conlleva peligrosos efectos para el desarrollo de las operaciones militares, ya que los ciberataques destinados a las redes de información logística y en general a todos sus sistemas podrían obstaculizar o inutilizar los flujos de información y de bienes, con sus respectivos elementos, servicios, suministros, mantenimiento y especial funcionamiento, lo que implicaría una baja de la certeza operativa y la capacidad de alistamiento y respuesta efectiva requerida por la táctica militar operativa.

De ahí que adoptar medidas de ciberseguridad para los sistemas de cadena logística del EJC y su cadena de suministro involucra diseñar medidas a fin de preservar los sistemas de información y comunicación utilizados en los sistemas integrados de gestión logística militar. Lo anterior debe incluir canales de diseño de identificación de riesgos, protocolos de verificación, capacitación del talento humano destacado en logística para lograr una mejora y resiliencia frente a estos posibles efectos cibernéticos.

En síntesis, la logística militar y la ciberseguridad viven interrelacionadas debido a la gradual dependencia de sistemas de información y comunicación y su importancia en las operaciones militares. Añadiendo que, sin sistemas de logística integrales en apoyo a las operaciones, será considerada baja la capacidad de éxito y cumplimiento de la misión.

Diseño de la cadena de suministro del Ejército Nacional de Colombia

Es necesario esbozar cómo está diseñada la cadena de suministro del EJC, lo que permite distinguir su funcionamiento y poner de presente sus intervinientes, flujos y apoyos de relación recursos, planeamiento, adquisición, conducción logística y

máximo canal de distribución. Definida dicha cadena como "la interacción de tres procesos que integran el macroproceso de gestión logística de la Fuerza: planeamiento logístico; adquisición bienes y servicios, y operación logística" (EJC, 2023, s.p.).

Tabla 1. *Diseño de la cadena de suministro del Ejército Nacional de Colombia*

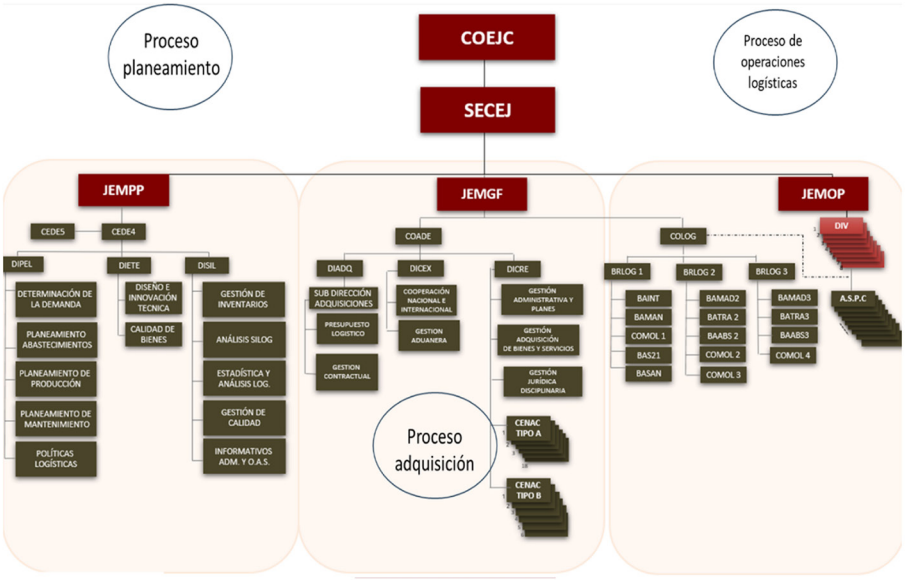
Proceso	Función	Objetivos	Gestión de procesos
Planeamiento logístico	Direccionar la logística mediante la creación de estrategias y su alineamiento en la organización.	Controlar y medir la gestión logística producción, abastecimiento, mantenimiento, servicios técnicos y transporte	Almacenamiento. Auditoría y confrontación de cargos. Contratación unidades ejecutores de presupuesto y centrales administrativas. Control de calidad productos de intendencia. Diseño, investigación y desarrollo productos de intendencia. Entrega. Exportación. Mantenimiento de maquinaria de producción. Mantenimiento de tercer nivel de armamento. Mantenimiento de tercer nivel cascos blindados. Mantenimiento segundo nivel armamento vehículos tácticos y optrónicos unidades móviles de mantenimiento. Mantenimiento tercer nivel optrónicos. Mantenimiento tercer nivel vehículos tácticos. Nacionalización. Planeación de producción. Producción material intendencia. Recepción. Registro y certificado de matrícula de una aeronave. Rehabilitación funcional. Trámite *loa's* y enmiendas. Transportes.
Adquisición de bienes y servicios	Identificación de las necesidades, selección de modalidad de compra, y todas las fases de la administración de la vida útil del bien o servicio, logrando dar sostenibilidad al Ejército.	Adquirir bienes y servicios que requiere la Fuerza mediante procesos, empleando buenas prácticas logísticas, que satisfagan las necesidades permitiendo el sostenimiento, proyección y soporte oportuno de la Fuerza.	
Operación logística	Parte de la cadena de suministro que consiste en calcular, preparar, disponer, organizar, entregar y vigilar el material, los bienes y servicios desde el punto de origen hasta el punto de consumo y satisfacer las necesidades para el funcionamiento de un Ejército y sus operaciones militares.	Garantizar la optimización de la cadena de suministro en las cantidades, el lugar, el tiempo y las condiciones exigidas por los hombres y unidades del Ejército para el sostenimiento de las operaciones miliares y la rehabilitación funcional del personal herido en combate.	Adquisición. Mantenimiento. Producción. Logística inversa. Ingenieros en apoyo general. Almacenamiento. Servicios en campaña. Transporte. Entrega.

***** Según los procesos, función y objetivos del sistema integrado de gestión logística del EJC.

****LOA:** Letter of Offer and Acceptance (Carta de oferta y aceptación).

Fuente: Sistema Integrado de Gestión Logística del EJC (2023).

Figura 2. *Sistema integrado de gestión logística, cadena de suministro del EJC y sus procesos*



Fuente: elaboración propia con base en Sistema Integrado de Gestión Logística del EJC (2023).

La Figura 2 muestra los procesos, funciones y objetivos vistos desde la organización y sus responsables, estableciendo gráficamente los tres momentos esenciales sobre los cuales se genera: planeación, adquisición y puesta en marcha de la logística militar y el sostenimiento propiamente dicho. Desde su diseño estructural, da lugar a formalizar la similitud conceptual establecida a partir de la diferencia entre la cadena de suministro y la cadena de abastecimiento.

Tabla 2. *Diferencias entre cadena de suministro y cadena de abastecimiento*

	Cadena de suministro	**Cadena de abastecimiento**
Alcance	Abarca todas las actividades involucradas en la producción, manejo y distribución de bienes y servicios.	Se enfoca específicamente en el movimiento y almacenamiento de bienes.
Objetivos	Garantizar que los productos correctos estén disponibles en el momento y lugar correctos.	Garantizar la entrega oportuna y eficiente de bienes y servicios a los clientes.
Actividades	Abastecimiento, la fabricación y la distribución.	Transporte, el almacenamiento y la gestión de pedidos.

Fuente: ISIL (2023).

Así las cosas, y dando alcance al significado de la FCG sostenimiento, en las operaciones logísticas, la producción sitúa la cadena de suministro por encima de la cadena de abastecimiento. Por lo tanto, es importante resaltar en este punto, la influencia del apoyo tecnológico que permite dar dominio fundado sobre la cadena de suministro y su manejo de información logística en el EJC, lo que implica manejo no solo de la información, sino además la administración de recursos medios y bienes. El Ministerio de Defensa Nacional, MDN, (2023) destaca al Sistema de Información Logística (SILOG) como:

> un sistema informático integrado que agrupa en tiempo real todas las funciones de la administración organizacional, trabaja en la integración de los departamentos logísticos de todas las Fuerzas con el fin de optimizar los bienes y recursos, para hacer más eficiente el abastecimiento de tropas, el mantenimiento de equipos y la compra de insumos […] implementado un sistema de información tipo ERP donde se gestiona en una misma plataforma, todos los procesos logísticos y financieros, convirtiéndose en una herramienta indispensable de soporte para la planeación, el control y fiscalización del sector. (párr.1)

En términos de su función, el SILOG

> desarrolla, integra e implementa los procesos administrativos, logísticos y financieros del sector Defensa en un sistema de información integrado, utilizando mejores prácticas y tecnología moderna para el control y administración óptima de los recursos, encaminados al apoyo efectivo de las operaciones que adelanta la fuerza pública. (párr. 3)

Tabla 3. *Manejo de Información logística SILOG*

Módulo Logístico	**Módulo de Mantenimiento**	**Módulo Financiero**
Debe subir a la plataforma SAP todos los procesos logísticos de las FF. MM., para controlar y verificar, en cada paso, desde el momento de la contratación hasta la llegada de elementos al cliente final.	El módulo de mantenimiento establece procedimientos para el mejoramiento y sostenimiento de las aeronaves de la fuerza pública y el armamento liviano.	Gestión financiera en los movimientos de los módulos Logístico y de Mantenimiento. Igualmente, se procesa la información financiera ingresada en el sistema y se evalúa el cumplimiento de normas contables y fiscales.

• Compras • Gestión de inventarios • Producción • Ventas • Plan de Compras • Calidad	• Aeronáutico • Naval • Terrestre • Biomédico • Armamento • Comunicaciones • Recursos Humanos	• Activos Fijos • Contabilidad • Presupuesto • Costos • Tesorería
Módulo Técnico Tiene como fin proveer el direccionamiento tecnológico, el mantenimiento de las aplicaciones, garantizando la seguridad y disponibilidad de la plataforma sobre la cual se opera el sistema de información. **Módulo de Seguridades y Control de Accesos** Tiene como fin realizar la gestion de los usuarios del Sistema de Informacion Logistica garantizando de esta manera la confidencialidad de la infromacion dando acceso solo al personal autorizado. **Módulo de Formacion para el trabajo** Tiene como misión facilitar el cambio organizacional que implica la implementación del sistema SAP en la fuerza pública. Tiene tres ejes: Capacitación Presencial, Capacitación Semipresencial y Sensibilización.		

Fuente: elaboración propia con base en MDN (2023).

La tabla 3 evidencia la calidad y magnitud de la información acumulada sobre la plataforma SAP, parte integral de la administración de bienes, recursos y *stock* de almacén representados en varias clases de abastecimientos, que incluyen información que da cuanta de las dimensiones de capacidades en áreas varias, y que se encuentran en forma de datos sensibles en la cadena de suministro de toda la organización del sector Defensa, las FF. MM. y el Ejército Nacional de Colombia. Sumado a lo anterior y desde la infraestructura logística del EJC y sus unidades tácticas y técnicas que manejan las operaciones logísticas se complementa la información indicando que actualmente la Fuerza cuanta con 46 unidades (batallones) de Apoyo de Servicios Para el Combate con capacidades individuales que soportan de manera regional en concordancia con la asignación territorios de la divisiones, brigadas y más sobre los comandos conjuntos, constituyéndose en una amplia red que vinculan capacidades sobre las que se generan y se nutren las fases del planeamiento de operaciones militares ofensivas, defensivas y de apoyo de la defensa a la autoridad civil.

Esta organización requiere igualmente que, a su nivel, se dé un manejo de información en aspectos administrativos que involucran, equipos de transporte, cantidades y consumo de combustible, sistemas de mantenimiento de equipos, personal destacado en labores de logística, almacenamiento y *stock* de inventarios de abastecimiento varios, elementos de apoyo de sanidad igualmente de comunicaciones, sumando capacidades de distribución entrega y suministro en cada una

de sus áreas de responsabilidad. Por lo anterior, una vez se establece y formaliza el relacionamiento entre la logística militar, la ciberseguridad y la ciberdefensa que crean un vínculo de manejo de la información que amerita ser orientado bajo la lupa y un mayor interés desde la academia y su generación de doctrina que ampare la seguridad de esta información valiosa.

Ataques cibernéticos a la cadena de suministro del EJC

La logística integral[2] y el ciberespacio[3] pueden ser considerados factores de poder y multiplicadores de eficiencia en el sostenimiento de la logística militar de varias maneras y sobre las cuales se cimenta el proponer amplitud de la academia y la doctrina a fin de fomentar el estudio de la ciberseguridad de la logística militar y de sus sistemas de gestión y de flujo de información:

Seguridad y manejo óptimo de recursos

La logística militar involucra la gestión eficaz de recursos en procura de la adquisición de medios, suministros, mantenimiento de equipos y preparación de personal. Los sistemas cibernéticos y herramientas empleados para el cumplimiento de estas funciones facilitan el seguimiento y rastreo en tiempo real de tales recursos; el correcto funcionamiento de sistemas logísticos da cuenta de tomar decisiones a partir de pronósticos de demanda orientados al sistema logístico militar, lo que admite una alta gestión y administración de los recursos. Además, los sistemas cibernéticos ayudan a anunciar y evadir inconvenientes logísticos, como la inexactitud de provisiones o el sostenimiento de equipos, mejorando así el uso de los recursos.

Dado lo anterior y sobre el sector Defensa en Colombia, es importante destacar la manera en que se ha dado importancia en este aspecto mediante la adopción de la estrategia sectorial establecida como Guía metodológica de planeamiento por capacidades (MDN, 2018)

---

2 Nuevo modelo de organización y gestión mediante el cual todos los procesos y departamentos están coordinados para redirigir los esfuerzos en una misma dirección (Esnova, s.f.).

3 Mundo no físico, sin límites, donde cualquier persona puede estar interconectada únicamente con una conexión a la red de tal manera que pueda interactuar con el mundo entero sin barreras.

> En respuesta a hacer que la estructura de Fuerza para el cumplimiento de su misión constitucional de brindar seguridad y defensa […] La proyección y desarrollo de la Estructura de Fuerza busca garantizar que la Fuerza Pública sea sostenible y eficiente en el presente y futuro. (p. 4)

Sin embargo, entidades u organizaciones como el Ejercito Nacional y, en general, las FF. MM. pueden ser foco de atención de ataques a sus cadenas de suministro, utilizando varios canales. Tal es el caso de utilización de información proveniente de proveedores externos que a su vez sea vulnerable a ataques sobre su información; ante eventos como este, se estima que existan tres ataques principales o clases de eventos:

> 1) amenazas físicas a la cadena de suministro: suelen requerir la cooperación con fabricantes y proveedores; 2) amenazas a la cadena de suministro digital: para reducir el tiempo de desarrollo, los desarrolladores de *software* utilizan una biblioteca común de terceros para realizar una función en su aplicación sobre información y acceso a las herramientas dígales, y 3) comprometer información de correos electrónicos empresariales con información financiera o destacada de negocio vinculante. (Proofpoint, 2023, párr. 7)

Se agrega, a manera de ejemplo, la ocurrencia de situaciones presentadas como la perpetrada al Sistema de Gestión de la Cadena de Suministro en 2018, y un asalto cibernético intensivo encaminado al sistema de gestión de la cadena de suministro manejado por el Departamento de Defensa de EE. UU. , complicando la seguridad de los datos afines a provisores y sus vínculos logísticos, poniendo en peligro las cadenas de suministro de las FF. MM., hecho referenciado como el ciberataque a SolarWinds. (BBC News Mundo, 2020, párr. 1).

Automatización como factor de seguridad del sistema de gestión logística

Los adelantos en tecnologías cibernéticas y automatización de técnicas agilizan y optimizan operaciones logísticas militares de sostenimiento. Ejecutan trabajos administrativos de forma expedita liberando ejecutores humanos, logrando desempeños transcendentales y de manejo más complejo. A manera de ejemplo, se ilustra el empleo de satélites militares en la eficiencia de las operaciones de la cadena de suministro.

> los satélites militares brindan una plataforma para una mayor automatización del proceso de gestión de la logística y la cadena de suministro. Mediante

> el uso de inteligencia artificial, los satélites militares pueden proporcionar un análisis automatizado de datos, lo que permite a los administradores de la cadena de suministro tomar mejores decisiones en una fracción del tiempo […] están revolucionando la logística y la gestión de la cadena de suministro, proporcionando una mejor comunicación, seguimiento de activos y automatización. Al permitir una mejor toma de decisiones. (Frąckiewicz, 2023, pp. 8-10)

Lo anterior formula la orientación a futuro del desarrollo que se establece en la dependencia del uso de tecnologías en apoyo a las cadenas de suministro dentro de la logística militar de sostenimiento, que, si bien requiere de asignación de recursos, permite evidenciar las fortalezas que ameritan mayor atención de la academia en procura de afianzar la aproximación entre la ciberseguridad, la ciberdefensa y la logística militar. A mayor avance y apoyo tecnológico en logística militar, mayor dependencia, mayor atención a la ciberseguridad orientada fortalecer la seguridad de los sistemas logísticos militares.

Sistemas de comunicación y coordinación logística

La logística militar requiere herramientas que provean en muchos y destacados casos comunicación vertiginosa entre estructuras y niveles de mando. Los sistemas logísticos apoyados en tecnologías de la información deben asegurar la toma de decisiones mediante canales seguros, logrando eficacia y máxima precisión de situación respecto de materiales y suministros propios de la cadena de suministro del sistema de gestión logística militar otorgando rapidez en la respuesta logística de sostenimiento de operaciones militares.

La cadena de suministro no ha sido ajena al impacto de las tecnologías, influyendo positivamente en su funcionamiento; este aporte también se formaliza en la administración de la logística militar, siempre con el horizonte de analizar información oportuna y detallada propendiendo por calidad de apoyo logístico, influyendo en asuntos tales como reducción de costos, reducción de tiempos de espera y mejorando la administración en asuntos de flujos de abastecimientos de diversas clases. Simchi-Levi (citado por Correa, 2008) relaciona los objetivos de las tecnologías en la administración de las cadenas de suministro:

> 1) proporcionar información disponible y visible; 2) tener en un solo punto el acceso a los datos; 3) facilitar la toma de decisiones basadas en el hecho que se tiene información de toda la cadena de suministro, y 4) permitir la colaboración entre los actores de la cadena de suministro. (p. 40)

Lo anterior permite referenciar la importancia de procesos que den cuanta del mejoramiento adaptativo establecido a partir de implementación de métodos y modelos de administración de la información en procura de evidenciar con ellos la formalización de sus deficiencias posibles o de las amenazas o riesgos del manejo de dicha información a favor de la implementación de la ciberdefensa en la logística militar y las maneras estratégicas de hacer las cosas en su sistema integral de funcionamiento.

Estrategias de seguridad y protección del sistema integrado de la logística militar

El ciberespacio libra un papel decisivo en la seguridad y amparo de la logística militar. Los sistemas de ciberseguridad consiguen revelar y advertir de ciberataques, al sistema logístico militar resguardando así los procedimientos y la información considerada crítica de la logística militar. Conjuntamente, los métodos cibernéticos de seguridad logran robustecer la seguridad en la cadena de suministro, certificando la legitimidad y la realidad de los bienes, y materiales empleados para el funcionamiento del sistema de logística y funcionamiento de las FF. MM.

Pero más allá de la estrategia para lograr objetivos militares en sí, puede llegar a ser más importante la anticipación. Por lo tanto, la preparación anticipada para este caso en particular y para atender correctamente las amenazas centradas y dirigidas contra el sistema de gestión logística deberá estructurarse como parte inicial de la estrategia un apresto adelantado: por cuenta de este precepto, se adhiere al mismo lo que afirma Esbry (2021), dando cuenta de la importancia de la estrategia y aplicable a destacar una estrategia para dar protección a la información logística

> […] considerar que las características de los conflictos de nuestra era confirman la vigencia del arte de la guerra como principios filosóficos, que van desde lo estratégico a lo táctico, abarcando también áreas de la conducción integral de la guerra como lo económico, la educación, lo político, lo diplomático, la industria, etc. (p. 42)

Lo anterior invocando lo considerado por la obra de Sun Tzu, que apreciaba la importancia de vivir capacitados, dentro de su corriente filosófica centrada en "ganar la guerra antes". De esta manera, es básico que en el EJC se estudie y fructifique convenientemente esta correlación para perfeccionar sus estructuras y operaciones logísticas de sostenimiento para conservar su capacidad operativa ante cualquier amenaza y escenario posible, especialmente las relacionadas con ciberataques, fundamentalmente, los que afectan y puedan estar orientados al debilitamiento del aparato logístico de soporte operacional.

Dicho lo anterior, existen varias teorías, hipótesis o prácticas de manejo, que logran crear un marco de análisis entre la logística militar, hoy FCG sostenimiento, y la relación con la ciberseguridad, que podrían ser base de la formación de literatura y doctrina en logística militar.

Teoría de bienes y tecnología de doble uso[4]

Sostiene que la tecnología y los sistemas desarrollados en terminaciones civiles logran ser manejados para propósitos militares. En este contexto, los métodos de gestión de la cadena de suministro empleados en el ámbito comercial, junto con la tecnología asociada, pueden aplicarse igualmente para alcanzar objetivos y logros militares. Esta realidad subraya la creciente urgencia de salvaguardar estos sistemas contra posibles amenazas cibernéticas.

Sobre este hilo, los métodos empleados en gestión de la cadena de suministro utilizados comercialmente y la tecnología dispuesta en estos también pueden ser manejados para objetivos y logros militares, lo que acrecienta la necesidad de proteger estos sistemas de posibles amenazas cibernéticas. Esta relación se afina bajo la concepción de Buzan (1998):

> los aspectos sobre los que va a incidir esa revolución tecnológica están íntimamente relacionados con el desarrollo de la tecnología del sector civil. El empleo de técnicas de doble uso en el campo de las comunicaciones, los móviles, o la inteligencia, resaltan el carácter unitario de la Revolución Industrial. Se puede así indicar, que toda sociedad industrializada mantiene también un potencial militar, gracias a los conocimientos, recursos materiales, humanos, y financieros, desarrollados. De ahí también, la dificultad de separar las aplicaciones civiles de la tecnología de su empleo para uso militar. (p. 156)

El riesgo compartido en ciberseguridad[5]

Esta práctica señala que las entidades o estructuras empresariales y militares, junto con sus proveedores intervienen en el riesgo de un posible ataque cibernético. En este contexto, se espera que las empresas que proveen servicios de logística militares o generan el canal para su desarrollo tomen medidas para responder por

[4] Producto o un servicio 'que puede destinarse tanto a usos civiles como militares', es decir que generalmente se destina a un uso civil, por ejemplo, en la industria, pero que también puede servir para desarrollar armas o material militar, o viceversa, uso civil en empleo militar (Francia diplomacia, 2014).

[5] Lo que las empresas necesitan es una nueva manera de ver el riesgo y una forma más colaborativa de identificar y abordar los riesgos a los que se enfrentan (PWC, 2024).

la seguridad cibernética de sus técnicas y procedimientos internos, a fin de impedir posibles impactos nocivos en la capacidad de la Fuerza afectando su enfoque de diseño para empleo en provisión de defensa.

Este aspecto se ejemplifica en dos vías. Una vía es la orientación del empleo de los ejércitos y de cómo aportan a su ciberdefensa asumiendo posturas de apoyo tecnológico y su importancia con las cadenas de suministro y su respetivo valor dentro de la estrategia militar. La otra vía es la postura de las empresas proveedoras de tecnología no solo informática, sino la industria proveedora de sistema de armas y equipos de uso crítico. Entonces, se tiene la postura de Fernández (2016), quien relata cómo cada día la tecnología transforma la guerra y la accion de los ejércitos y su logística:

> La guerra es una lógica de transformación que, en ocasiones revierte la situación y lo que era una fortaleza se transforma en una debilidad. Lo que se acrecienta ante fallos, averías y la existencia de vulnerabilidades, que además requieren de una cadena logística compleja. (p. 8)

La segunda vía o postura se identifica con Seguridad en America (2021) que propone no solo comentar sobre la importancia de la ciberseguridad, sino que aduce la importancia de pasar de la teoría a la acción:

> En este dinamismo que vivimos y digitalización, no podemos ignorar hacia donde nos están llevando las tendencias, dentro del marco de seguridad debemos siempre cuidar el balance entre: personas, procesos/procedimientos (bajo marco legal) y la tecnología que cada vez cumple roles más trascendentales en el día a día, apoyándonos a incrementar nuestra eficiencia operacional. (párr. 7)

Lo anterior debe involucrar desde las acciones políticas y posturas de los Estados hasta la menor intervención de actores, pasando por la responsabilidad de interviniente de quienes administran la seguridad de la información militar y la seguridad que debe impartirse en las cadenas de suministro del ejército.

Teoría del control[6]

Sostiene que, en un entorno militar, es forzoso poseer un control amplio sobre toda la cadena de suministro y sus sistemas relacionados. Esto circunscribe la

[6] La teoría de control se ocupa del "sistema de control" de los "sistemas dinámicos" en los procesos y máquinas de ingeniería. El objetivo es desarrollar un modelo o algoritmo que gobierne la aplicación de las entradas del sistema para conducirlo a un estado deseado, minimizando cualquier retardo, sobreimpulso o error de estado estacionario (William, 1996).

proporción de medidas en seguridad cibernética en indivisos semblantes de esa misma cadena de suministro, a partir de la adquisición de materias primas, servicios, bienes destinados a producción y posteriormente llevados al almacenamiento hasta que se involucren en procesos u operaciones de sostenimiento de entrega en áreas de requerimiento o de combate.

> Deben gestionarse las actividades misionales y operativas propias de la entidad y definirse, de manera paralela, controles que ayuden a proteger el activo más valioso: la información. Una organización que desee ser cada día más competitiva debe tener como pilar la protección de la información, evitando su exposición ante personas malintencionadas o posibles ciberataques. (ManageEngine blog, 2022, párr. 1)

Teoría de la resiliencia o ciberresiliencia[7]

Se centra en la capacidad de una organización para recuperarse rápidamente de un ataque cibernético. En este contexto, las empresas de logística militares deben implementar medidas de seguridad cibernética para minimizar los riesgos de un posible ataque y para garantizar una rápida recuperación en caso de que ocurra un incidente.

> A nivel mundial, nos hemos visto afectados por un hecho sin precedentes, que no anticipamos y que tuvimos muy poco tiempo de maniobra para mantenernos a salvo, readaptar formas de trabajo y reajustar nuestros hábitos de consumo [...] Ante este panorama, muchas empresas deben preguntarse ¿cuál es mi capacidad y tiempo de recuperación para que mi operación logística se restablezca ante una eventualidad? La respuesta es: resiliencia. Se trata de un concepto que nuestra cadena de suministro debe tener en su ADN para salir avante de la contingencia. (SAP, 2020, párr. 1-2)

En resumen, estas teorías, hipótesis o prácticas de manejo destacan la importancia de la seguridad cibernética, de la ciberseguridad en la cadena logística militar del EJC, su cadena de suministro y su sistema integrado de gestión de logística, así como de la necesidad de implementar medidas para protegerlos ante posibles vulnerabilidades, que tendrían consecuencias considerables en redundante

[7] La ciberresiliencia o resiliencia cibernética describe la capacidad de un sistema u organización para resistir o recuperarse ante ataques o incidentes cibernéticos. De este modo, una organización ciberresiliente trabaja en pos de proteger sus activos digitales y la continuidad de sus sistemas frente a ciberataques o desastres tecnológicos (S2 Grupo, 2023).

deterioro de las operaciones militares. Por lo tanto, a partir de este anterior cúmulo de conceptos, se edifica la gestión documental de formación de doctrina que involucre el diseño de mayor cantidad de manuales de referencia, de campaña y de técnicas y procedimientos que involucren el desempeño de la táctica que proponga la protección de las cadenas de suministro en el EJC.

Matriz FODA. Ciberdefensa de la cadena de suministro del EJC

La Tabla 3 presenta la matriz FODA que analiza la importancia de aumentar el estudio de la ciberseguridad en la logística militar.

Tabla 4. *Matriz FODA*

	FORTALEZAS	**DEBILIDADES**
ANALISIS FODA	• Mayor seguridad en la gestión de información y datos militares. • Disminución del riesgo de ciberataques y vulnerabilidades en la cadena de suministro. • Compromiso con la modernización y la mejora continua de las capacidades militares.	o Limitaciones presupuestarias para la implementación de medidas de ciberseguridad a gran escala. • Falta de personal capacitado y recursos tecnológicos para implementar medidas de ciberseguridad. • Resistencia al cambio por parte de algunos miembros del personal o proveedores que no estén familiarizados con medidas de ciberseguridad en la logística militar.
OPORTUNIDADES	**ESTRATEGIAS FO**	**ESTRATEGIAS DO**
o Mejorar la eficiencia de la cadena de suministro mediante la implementación de medidas de ciberseguridad. • Aumentar la capacidad de respuesta ante posibles ciberataques, con lo que se mejora la resiliencia. • Reducir, potencialmente, los costos relacionados con la recuperación ante ciberataques gracias a la prevención.	1. Aprovechamiento de recursos: utilizar las plataformas de manejo de información y de recursos y bienes del sistema integrado de gestión logística, pero generar directrices de innovación y ajuste de procesos. 2. Alianzas estratégicas: establecer alianzas con otras organizaciones de la academia y de la empresa dando lugar al aumento de medidas que apoyen la ciberseguridad en la cadena de suministro. 3. Diversificación: usar las fortalezas internas para diversificar las medidas involucrando la mayor cantidad de intervinientes en la cadena de suministro, desde proveedores hasta quienes responden por el manejo de recursos de todo tipo. 4. Expansión geográfica: utilizar las fortalezas internas para ampliar la experiencia de manejo de ciberataques, ubicar personal experto y difundir criterios, procedimientos y estrategias. Propender por generación de equipos interdisciplinares para dar apertura a la investigación y doctrina, a partir de la recolección de información.	1. Desarrollar alianzas estratégicas: utilizar las oportunidades externas para desarrollar alianzas con otras empresas o sectores que puedan ayudar a superar las debilidades internas. 2. Mejorar la capacitación y formación del talento humano que administra la cadena de suministro, mediante directrices de mejoramiento en la capacitación y formación del personal, superando la deficiencia y carencia de habilidades técnicas específicas. Todo orientado desde la academia y la actualización doctrinal. 3. Innovación y desarrollo de nuevos productos o servicios: usar las oportunidades externas para impulsar la innovación y el desarrollo de nuevos programas y estudios que permitan actualizar la doctrina y aumentar el desarrollo académico orientado a evitar los ciberataques a la cadena de suministro de la logística del EJC. 4. Mejorar los procesos internos: aprovechar las oportunidades externas para mejorar los procesos internos de la logística del EJC, a fin de superar las debilidades y mejorar la eficiencia del manejo de la información de la cadena de suministro del sistema integrado de gestión logística.

AMENAZAS	ESTRATEGIA FA	ESTRATEGIA DA
• Falta de apoyo político o recursos disponibles para la implementación de medidas de ciberseguridad. • Incremento en ciberataques y amenazas cibernéticas. • Requerimientos gubernamentales o de la industria que no se ajusten a las capacidades técnicas actuales.	1. Mejorar la calidad y eficiencia: utilizar las fortalezas internas para mejorar la calidad y eficiencia de los procesos de producción y operaciones logísticas que presenten vulnerabilidades en el manejo de la información de la cadena de suministro. 2. Desarrollar nuevas habilidades y competencias: utilizar las fortalezas internas para desarrollar nuevas habilidades y competencias que permitan hacer frente a las amenazas. 3. Buscar nuevos espacios académicos en los centros y estructuras de formación y capacitación. 4. Establecer alianzas estratégicas: utilizar las fortalezas internas para establecer alianzas con otras Fuerzas compartiendo experiencias con las cadenas de suministro que integran la cadena de abastecimiento de las FF. MM.	1. Aumentar la competitividad de la Fuerza y su sistema integrado de gestión logística y de su cadena de suministro mediante la generación de propuestas estratégicas llevada a los actores políticos en busca de apoyo de fortalecimiento ante ciberataques sobre la logística militar. 2. Aumentar la capacidad de adaptación desarrollando nuevas habilidades digitales a partir del desarrollo de la investigación para enfrentar la creciente proliferación de amenazas. 3. Utilizar la academia, la investigación e innovación desde la generación de grupos interdisciplinares que aporten y promuevan los recursos destinados para aumentar las propuestas doctrinales en manejo de ciberataques a la cadena de suministro del EJC.

Fuente: elaboración propia.

De manera general, el resultado de la matriz FODA sugiere que hay beneficios importantes en aumentar el estudio de la ciberseguridad en la logística militar, como aumentar la eficiencia de la cadena de suministro y mejorar la capacidad de respuesta ante posibles ciberataques. Sin embargo, puede que surjan obstáculos como limitaciones financieras y falta de personal capacitado y recursos tecnológicos. Al abordar estos desafíos, el EJC puede avanzar en la mejora de las capacidades operativas y la preparación para enfrentar amenazas, tanto tradicionales como emergentes, sobrevinientes sobre la cadena de logística de la Fuerza, su cadena de suministro y su sistema integrado de gestión logística en la FCG sostenimiento.

Conclusiones

La ciberseguridad y la ciberdefensa son componentes fundamentales para garantizar la integridad y confidencialidad de la información estratégica de la cadena logística del EJC y, en consecuencia, de su sistema integrado de gestión logística. El desarrollo de estudios que relacionen la ciberseguridad, la ciberdefensa y la logística militar permitirá fortalecer las capacidades de la institución para proteger y asegurar los sistemas y redes de información que involucran sistema de adquisición, manejo administrativo, *stocks,* mantenimiento de equipos, capacidades del sistema y la FCG sostenimiento materializada en sus unidades y formas de hacer las cosas.

La ciberseguridad y la ciberdefensa son cruciales para evitar ataques cibernéticos que podrían causar daños significativos en términos de infraestructura, operaciones militares y las que involucren a la seguridad nacional, en general, desde la obtención de información que permita establecer capacidades de funcionamiento del EJC.

Es importante que la academia estructurada desde las organizaciones encargadas de la doctrina y el sistema educativo de la fuerza encargada del entrenamiento y la administración de recursos de logística y sostenimiento, generen el panorama de las necesidades de impacto sobre las cuales se edifiquen los constructos para aumentar un conocimiento especializado y avanzado en el campo de la ciberseguridad, la ciberdefensa y orientado al fortalecimiento de la logística militar aplicada en el EJC, con el fin de formar profesionales altamente capacitados e integrales en estas áreas.

La integración de la ciberseguridad y la ciberdefensa en la logística militar y en la doctrina contribuirá a mejorar la gestión de los recursos y la toma de decisiones, permitiendo una mayor eficiencia operativa y logística.

La falta de estudios relacionados con la ciberseguridad, la ciberdefensa y la logística militar y el sistema integrado de gestión logística del EJC limita el desarrollo de estrategias y tácticas adecuadas para enfrentar los desafíos y amenazas cibernéticas en el ámbito de la cadena de suministro de la Fuerza.

La formación en ciberseguridad y ciberdefensa dentro de la academia militar proporciona habilidades y conocimientos necesarios para prevenir y mitigar los riesgos cibernéticos en el entorno de su cadena de suministro, de ahí la importancia destacada en la intervención de la academia ante este reto.

Un rumbo compuesto de la ciberseguridad, la ciberdefensa y la logística militar con su respectiva cadena de suministro accederá a una alta relación y asistencia entre los semejantes figurantes implicados en el amparo de los sistemas militares.

El adelanto de estos saberes proporcionará la adaptación y modernidad de las tácticas y metodologías manejadas en la ciberseguridad y la ciberdefensa, para hacer frente a hechos, amenazas y vulnerabilidades que nacen asiduamente.

La importancia de que la academia desarrolle estos estudios reside en la necesidad de formar líderes militares competentes para tomar decisiones instruidas y valiosas en el ámbito de la ciberseguridad y la ciberdefensa, en aras de proteger los intereses nacionales y garantizar la seguridad de la cadena de suministro del sistema integrado de gestión logística del Ejercito Nacional de Colombia.

Referencias

Buzan, B. (1998). Introducción a los estudios estratégicos: Tecnología militar y relaciones internacionales. *Cuadernos de Estrategia,* (99), 155-1166. https://dialnet.unirioja.es/servlet/articulo?codigo=4553585

Centro de Doctrina Conjunta [CEDOC] (Ed). (2018). *Manual Fundamental Conjunto MFC 1.0 Doctrina Conjunta.* Sello Editorial ESDEG. https://doi.org/10.25062/MFC10

Corera, G. (2020, 20 de diciembre). SolarWinds: 5 ataques informáticos de Rusia que transformaron la ciberseguridad en Estados Unidos. https://www.bbc.com/mundo/noticias-internacional-55381892

Correa Espinal, A., & Gómez Montoya, R. A. (2008). *Tecnologías de la información en la cadena de suministro. Dyna, 76*(157), 37-48. http://www.scielo.org.co/pdf/dyna/v76n157/a04v76n157.pdf

Council of Supply Chain Management Professionals [CSCMP]. (2023, 20 de octubre). Council of Supply Chain Management Professionals. https://cscmp.org/

Díaz del Río Durán, J. (2011). La ciberseguridad en el ámbito militar. *Cuadernos de Estrategia,* (149), 215-256. https://dialnet.unirioja.es/servlet/articulo?codigo=3837348

Ejército Nacional de Colombia. (2016). *MFRE 4-0 Sostenimiento.* Imprenta Ejército. https://www.cedoe.mil.co/enio/recurso_user/doc_contenido_pagina_web/800130633_4/458784/mfre_4_0_sostenimiento.pdf

Ejército Nacional de Colombia. (2018). *Manual de campaña.* Imprenta Ejército.

Ejército Nacional de Colombia. (2023, 3 de enero). Sistema Integrado de Gestión Logística. https://www.ejercito.mil.co/sistema-integrado-de-gestion-logistica/

Esbry, G. (2021). Pensamiento estratégico de Sun Tzu: Su legado a través de la historia. *Revista Visión Conjunta,* (25), 39-42. http://www.cefadigital.edu.ar/bitstream/1847939/2013/1/ESGCFFAA-revista%20Visi%C3%B3n%20Conjunta-25.pdf

Fernández-Montesinos, F. (2016, 30 de noviembre). Los militares y la tecnología [Documento de análisis, n.º, 72]. https://www.ieee.es/Galerias/fichero/docs_analisis/2016/DIEEEA72-2016_Militares_Tecnologia_FAFM.pdf

Frąckiewicz, M. (2023). El impacto de los satélites militares en la logística militar y las cadenas de suministro. https://ts2.space/es/el-impacto-de-los-satelites-militares-en-la-logistica-militar-y-las-cadenas-de-suministro/

Fuerza Aérea Colombiana [FAC]. (2016). *Manual de doctrina logística -MALOG-.* Imprenta y Publicaciones Fuerzas Militares República de Colombia. https://www.fac.mil.co/sites/default/files/linktransparencia/Planeacion/Manuales/manuales2022/malog_2016.pdf

Fundación Universitaria Internacional de la Rioja [UNIR]. (2022). ¿Qué es la ciberseguridad? Objetivos e importancia en la actualidad. https://colombia.unir.net/actualidad-unir/que-es-ciberseguridad/#:~:text=La%20ciberseguridad%20o%20seguridad%20inform%C3%A1tica,programas%2C%20de%20posibles%20ataques%20digitales.

Ganuza , N. (2020). *Guía de ciberdefensa: Orientaciones para el diseño, planeamiento, implantación y desarrollo de una ciberdefensa militar.* Junta Interamericana de Defensa. https://www.iadfoundation.org/wp-content/uploads/2020/08/Ciberdefensa10.pdf

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, P. (2014). *Metodología de la investigación* (6.a ed.). Mc Graw-Hill. https://academia.utp.edu.co/grupobasico-clinicayaplicadas/files/2013/06/Metodolog%C3%ADa-de-la-Investigaci%C3%B3n.pdf

Hitzler, R., & Honer, A. (2016). Los métodos cualitativos. En H. Sánchez (ed.), *Análisis para el estudio y la enseñanza de la ciência política: La metodologia de la ciencia política* (pp. 59-68). Universidad Nacional Autónoma de México. https://archivos.juridicas.unam.mx/www/bjv/libros/13/6180/6.pdf

IBM. (s. f.). ¿Qué es un ciberataque? https://www.ibm.com/es-es/topics/cyber-attack

ISIL. (2023). Diferencias entre la cadena de suministro y la de abastecimiento. https://isil.pe/blog/logistica/diferencias-suministro-abastecimiento/#:~:text=Actividades%3A%20la%20cadena%20de%20suministro,y%20la%20gesti%C3%B3n%20de%20pedidos.

Jiménez Jiménez, I. (2021). Elementos que identifican los métodos comparados. *Collectivus, Revista de Ciencias Sociales, 8*(2), 167-192. https://doi.org/10.15648/Collectivus.vol8num2.2021.3134

Joyanes Aguilar, L. (2010). Introducción: Estado del arte de la ciberseguridad. En Ministerio de Defensa (Ed.), C*iberseguridad: Retos y amenazas a la seguridad nacional en el ciberespacio* (págs. 13-46). Imprenta del Ministerio de Defensa de España. https://www.ieee.es/Galerias/fichero/cuadernos/CE_149_Ciberseguridad.pdf

Lifeder. (2020). Investigación bibliográfica: Definición, tipos, técnicas. https://www.lifeder.com/investigacion-bibliografica/#:~:text=La%20investigaci%C3%B3n%20bibliogr%C3%A1fica%20o%20documental,selecci%C3%B3n%20de%20fuentes%20de%20informaci%C3%B3n

MangeEngine. (2022, 21 de julio). ¿En qué consiste un control en ciberseguridad? https://blogs.manageengine.com/espanol/2022/07/21/que-es-control-en-ciberseguridad.html

Martínez Corona, J. I., Palacios Almón, G. E., & Oliva Garza, D. B. (2023). *Guía para la revisión y el análisis documental: propuesta desde el enfoque investigativo.* Ra Ximhai: Revista Científica de Sociedad, Cultura y Desarrollo Sostenible, 19(1), 67-83. https://dialnet.unirioja.es/servlet/articulo?codigo=8851658

Ministerio de Defensa Nacional [Mindefensa]. (2018). *Guía metodológica de planeamiento por capacidades*. Ministerio de Defensa Nacional. http://capacitas.mindefensa.gov.co/storage/biblioteca/Guia_Metodologica_de_Planeacion_por_Capacidades.pdf

Ministerio de Defensa Nacional [Mindefensa]. (2023). *Sistema de Información Logística SILOG*. Ministerio de Defensa Nacional. https://www.mindefensa.gov.co/irj/portal/Mindefensa/contenido?NavigationTarget=navurl://9f049c2f279e9248da04add30057f515

Montanyá, O. (2021, 4 de enero). La logística: de la guerra al arte. https://micromegas.bsm.upf.edu/2021/01/04/la-logistica-de-la-guerra-al-arte/

NATO Cooperative Cyber Defence Centre of Excellence [CCDCOE]. (2023, 19 de octubre). *NATO recognises cyberspace as a 'Domain of Operations' at warsaw summit.* https://ccdcoe.org/incyder-articles/nato-recognises-cyberspace-as-a-domain-of-operations-at-warsaw-summit/

Organización del Tratado del Atlántico Norte [OTAN]. (2020). *Allied Joint doctrine for cyberspace operations.* NATO Standardization Office. https://assets.publishing.service.gov.uk/media/5f086ec4d3bf7f2bef137675/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf

Parlamento Europeo, & Consejo de la Unión Europea. (2019). *Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo* de 17 de abril de 2019. relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) n.º 526/2013 («Reglamento sobre la Ciberseguridad»). https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32019R0881&from=FR

Ponce Talacon, H. (2007). La matriz FODA: Alternativa de diagnóstico y determinación de estrategias de intervención en diversas organizaciones. *Enseñanza e Investigación en Psicología, 12*(1), 113-130. https://www.redalyc.org/pdf/292/29212108.pdf

Proofpoint. (2023). Ataque a la cadena de suministro (Supply Chain Attack). https://www.proofpoint.com/es/threat-reference/supply-chain-attack

Rodríguez Gómez , D. (s. f.). Elección de la metodología de investigación. En *El proyecto de investigación* (pp. 33-35). Universitat Oberta de Catalunya. https://openaccess.uoc.edu/bitstream/10609/147625/3/ElProyectoDeInvestigacion.pdf

Rodríguez Jiménez, A., & Pérez Jacinto, A. O. (2017) *Métodos científicos de indagación y de construcción del conocimiento. Revista Escuela de Administración de Negocios,* (82), 175-195. https://journal.universidadean.edu.co/index.php/Revista/article/view/1647

Sánchez Acevedo, M. E. (2020). La ciberseguridad y la ciberdefensa, la necesidad de generar estrategias de investigación sobre las temáticas que afectan la seguridad y defensa del Estado. En E. S. Guerra & G. E. Medina-Ochoa (Eds.), *La seguridad en el ciberespacio: Un desafío para Colombia* (pp. 34-38). Editorial ESDEG. https://doi.org/10.25062/9789584288929.01

SAP. (2020, 6 de abril). Construyendo la cadena de suministro resiliente en tiempos de contingencia. https://news.sap.com/latinamerica/2020/04/construyendo-la-cadena-de-suministro-resiliente-en-tiempos-de-contingencia/

Seguridad en América. (2021, 13 de junio). Ciberseguridad, menos teoría y más acción. https://www.seguridadenamerica.com.mx/noticias/articulos/27840/ciberseguridad-menos-teorIa-y-mAs-acciOn

Unión Internacional de Comunicaciones (UTI). (2018). *Guía para la elaboración de una estrategia nacional de ciberseguridad:* Participación estratéginca en la ciberseguridad. Unión Internacional de Telecomunicaciones. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-S.pdf