Análisis del impacto de las amenazas cibernéticas en la confidencialidad y seguridad de la información relacionada con diseños y producción de camuflados en el Ejército Nacional: estrategias para la protección de información y prevención de amenazas

Mayor Luis Antonio Latorre Jácome

Artículo para optar al título profesional:

Magister en Ciberseguridad y Ciberdefensa

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

DATOS GENERALES		
Nombre del estudiante	**:**	Mayor Luis Antonio Latorre Jácome
Identificación	**:**	91537963
Programa académico	**:**	Maestría en Ciberseguridad y Ciberdefensa
Tutor metodológico	**:**	Jairo Andrés Becerra Cuervo, PhD
Tutor temático	**:**	Jairo Andrés Becerra Cuervo, PhD
Fecha de entrega	**:**	28/09/2025
Extensión	**:**	8.611 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 articulo sea publicado por el Sello Editorial ESDEG en su repositorio institucional y esté disponible bajo una modalidad de acceso abierto.

Tabla de Contenido

Índice de Tablas

Análisis del impacto de las amenazas cibernéticas en la confidencialidad y seguridad de la información relacionada con diseños y producción de camuflados en el Ejército Nacional: estrategias para la protección de información y prevención de amenazas

Analysis of the impact of cyber threats on the confidentiality and security of information related to camouflage designs and production in the National Army: strategies for information protection and threat prevention

Luis Antonio Latorre Jácome[1]
Escuela Superior de Guerra "General Rafael Reyes Prieto"

Resumen: El presente artículo analiza la convergencia entre el tráfico ilícito de prendas de uso privativo del Ejército Nacional de Colombia y las amenazas emergentes en el ámbito de la ciberseguridad. El tráfico de armas, municiones, explosivos y uniformes militares representa una amenaza directa a la seguridad nacional, al fortalecer a grupos armados ilegales y socavar la autoridad de las instituciones del Estado. En este contexto, las redes criminales han adoptado tecnologías digitales para coordinar operaciones ilícitas, acceder a información sensible y evadir controles estatales, lo que eleva la importancia de la ciberseguridad como componente esencial en las estrategias de defensa. A través de un enfoque cualitativo, esta investigación examina los riesgos asociados al uso indebido de uniformes militares, las prácticas de ciberespionaje y las vulnerabilidades en los sistemas de información estatal. Asimismo, se documentan casos recientes de incautación de prendas militares y se resalta la necesidad de estrategias integradas que articulen inteligencia operativa, cooperación interinstitucional y medidas tecnológicas avanzadas. El estudio busca generar recomendaciones para fortalecer la capacidad del Estado en la protección de su soberanía, mediante la implementación de herramientas digitales que permitan rastrear, prevenir y sancionar estas actividades delictivas, contribuyendo así al diseño de políticas de seguridad más eficaces y adaptativas frente a las amenazas híbridas contemporáneas.

Palabras clave: Ciberseguridad, Crimen Organizado, Inteligencia militar, Prendas militares, Tráfico ilícito.

[1] Mayor del Ejército Nacional de Colombia. Estudiante de maestría 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/0009-0009-1801-7218 - Contacto: luis.latorre@esdeg.edu.co.

Abstract: This article analyzes the convergence between the illicit trafficking of clothing exclusively used by the Colombian National Army and emerging threats in the field of cybersecurity. The trafficking of arms, ammunition, explosives, and military uniforms represents a direct threat to national security by strengthening illegal armed groups and undermining the authority of state institutions. In this context, criminal networks have adopted digital technologies to coordinate illicit operations, access sensitive information, and evade state controls, elevating the importance of cybersecurity as an essential component of defense strategies. Using a qualitative approach, this research examines the risks associated with the misuse of military uniforms, cyberespionage practices, and vulnerabilities in state information systems. It also documents recent cases of seizures of military clothing and highlights the need for integrated strategies that articulate operational intelligence, inter-institutional cooperation, and advanced technological measures. The study seeks to generate recommendations to strengthen the State's capacity to protect its sovereignty by implementing digital tools that track, prevent, and punish these criminal activities, thereby contributing to the design of more effective and adaptive security policies in the face of contemporary hybrid threats.

Keywords: Threats, Intelligence, Defense, Organized Armed Groups, Security

Introducción

El tráfico de armas, municiones, explosivos y prendas de uso privativo de las fuerzas militares representa una grave amenaza para la seguridad nacional y la estabilidad del país. Estas actividades ilícitas no solo fortalecen a los grupos armados organizados y a las redes criminales, sino que también debilitan las instituciones encargadas de la defensa y el orden público (Mindefensa, 2023). En este contexto, abordar el análisis de los riesgos asociados a la comercialización ilegal de estos elementos resulta fundamental para diseñar estrategias efectivas de prevención, control y respuesta.

En complemento, es importante también mencionar el concepto de ciberespionaje industrial o corporativo que se refiere al acceso ilegal y carente de ética a información confidencial de una empresa o de una institución con el propósito de obtener una ventaja competitiva. De conformidad a lo anterior, constituye un tipo de ciberataque en el que se sustraen datos delicados o propiedad intelectual para generar beneficios, generalmente a favor de un competidor. Esta práctica normalmente se lleva a cabo de manera encubierta, frecuentemente por empleados o personas con acceso privilegiado a la información que la sustraen en beneficio de otra organización o institución.

Las motivaciones de los delincuentes que llevan a cabo ciberespionaje y sustraen información confidencial y propiedad industrial pueden responder a diversos objetivos, entre los cuales se destacan:

- Obtener considerables beneficios económicos a través de la extorsión a las víctimas o la venta de información sensible a empresas competidoras.

- Favorecer a compañías respaldadas por Estados que patrocinan estos ataques, otorgándoles ventajas estratégicas en el mercado.
- Dificultar el funcionamiento de las organizaciones afectadas, impactando su planificación y estrategia empresarial a mediano y largo plazo.
- Perjudicar la reputación de las empresas al exponer información confidencial, generando desconfianza entre socios, inversionistas y clientes, y evidenciando su vulnerabilidad ante posibles ataques (Tarlogic, 2024).

No obstante, la complejidad del fenómeno requiere un análisis profundo que permita comprender su impacto en la seguridad nacional y su vinculación con el crimen organizado. Estudios recientes han demostrado que la falsificación y comercialización ilegal de uniformes y otros elementos de intendencia no solo facilitan la suplantación de miembros de la Fuerza Pública, sino que también incrementan los riesgos de ataques terroristas y operaciones encubiertas de grupos armados ilegales (Silva y Pérez, 2022).

Además, la protección de la información en estos escenarios se convierte en un elemento clave para garantizar la efectividad de las estrategias de seguridad. La filtración de datos sobre operativos, unidades militares y planes estratégicos puede ser aprovechada por redes criminales para evadir la acción del Estado, comprometiendo la eficacia de las fuerzas de seguridad.

Desde un enfoque académico y práctico, esta investigación permitirá aportar conocimiento sobre los mecanismos empleados en el tráfico de prendas de uso privativo del Ejército Nacional, sus implicaciones para la seguridad y la manera en que la ciberseguridad puede fortalecer la prevención y mitigación de estos riesgos. Asimismo, el estudio contribuirá

a la formulación de recomendaciones para mejorar la capacidad de respuesta del Estado, promoviendo el diseño de estrategias integradas que articulen aspectos normativos, tecnológicos y operativos en la lucha contra el tráfico ilícito.

Un ejemplo de ello son los operativos realizados por tropas de la Sexta División y la Brigada 13, en colaboración con agentes del CTI de la Fiscalía General de la Nación, los cuales permitieron la desarticulación de una red de tráfico de armas con centro de operaciones en Bogotá y actividades en el departamento del Tolima en 2024. Esta operación, que incluyó tres allanamientos en puntos estratégicos, refleja no solo la efectividad de las fuerzas de seguridad, sino también la complejidad de estas redes, que requieren esfuerzos integrales y sostenidos para su desmantelamiento (Semana, 2024).

En el marco de estas acciones, la ciberseguridad y la protección de la información se han convertido en componentes fundamentales. Las redes criminales, cada vez más sofisticadas, recurren a tecnologías digitales para coordinar sus actividades, ocultar sus operaciones y evadir los controles estatales.

El Plan Ayacucho es una estrategia integral del Ejército Nacional que busca garantizar la seguridad y estabilidad del país, enfrentando múltiples amenazas, entre ellas, el tráfico ilícito de armas, municiones y explosivos. Esta problemática ha sido identificada como un factor clave que alimenta la violencia y dificulta los procesos de consolidación de la paz en el territorio colombiano. En particular, el tráfico de armas no solo fortalece a los grupos armados ilegales y bandas criminales, sino que también fomenta economías ilegales que perpetúan ciclos de conflicto.

En complemento de lo anterior, la institución ha evidenciado la necesidad de una estrategia integral que combine acciones de inteligencia operativa con el uso de tecnologías

avanzadas para la identificación y neutralización de estas redes criminales. Sin embargo, la sofisticación de las amenazas digitales requiere un análisis detallado sobre la manera en que la ciberseguridad puede ser integrada de forma más efectiva en la lucha contra el tráfico ilícito de prendas militares. Estudios recientes destacan que la falta de medidas adecuadas en seguridad digital puede facilitar la infiltración de actores hostiles en sistemas estatales, permitiendo la manipulación o el acceso no autorizado a información clasificada (Gómez y Ramírez, 2021).

Además de las armas y municiones, el tráfico de prendas de uso privativo de las fuerzas militares constituye una amenaza significativa. La utilización ilegal de uniformes e insignias militares facilita la comisión de delitos como secuestros, extorsiones y actos de terrorismo, al permitir que los delincuentes se hagan pasar por miembros de la fuerza pública. Según el artículo 346 del Código Penal Colombiano, "el que sin permiso de autoridad competente importe, fabrique, transporte, almacene, distribuya, compre, venda, suministre, sustraiga, porte o utilice prendas, uniformes, insignias o medios de identificación reales, similares o semejantes a los de uso privativo de la fuerza pública o de los organismos de seguridad del Estado, incurrirá en prisión de cuarenta y ocho (48) a ciento ocho (108) meses y multa de sesenta y seis punto sesenta y seis (66.66) a mil quinientos (1.500) salarios mínimos legales mensuales vigentes" (Código Penal Colombiano, Artículo 346).

Las autoridades han reportado múltiples casos de incautación de material bélico y prendas militares en manos de organizaciones criminales, por ejemplo, en el departamento de Nariño, la Policía Nacional incautó 2.500 cartuchos calibre 5.56 y 25 uniformes pixelados de uso privativo de las fuerzas militares, evitando que estos elementos llegaran a grupos ilegales (PONAL, 2024). Asimismo, en el departamento del Meta, se capturó en flagrancia a

un individuo que transportaba 36 uniformes pixelados y 36 camboyanas sin documentación que acreditara su legalidad o procedencia (PONAL, 2024).

Estos incidentes evidencian la existencia de redes dedicadas al tráfico de prendas militares, las cuales representan riesgos significativos para la seguridad nacional. La apropiación y uso indebido de uniformes oficiales por parte de actores ilegales no solo socava la confianza de la población en las instituciones de seguridad, sino que también pone en riesgo la integridad de las operaciones militares y policiales.

La ciberseguridad juega un papel crucial en la prevención y combate de estas actividades ilícitas. Las organizaciones criminales utilizan plataformas digitales para coordinar el tráfico de armas y uniformes, así como para obtener información sensible que les permita evadir a las autoridades. Por lo tanto, es imperativo que las fuerzas de seguridad implementen medidas robustas de ciberseguridad para proteger sus sistemas de información y comunicaciones.

El tráfico de armas, municiones y prendas de uso privativo de las fuerzas militares constituye una amenaza multifacética que requiere una respuesta integral. La combinación de operaciones de inteligencia, colaboración interinstitucional y fortalecimiento de la ciberseguridad es esencial para contrarrestar estas actividades ilícitas y garantizar la seguridad y estabilidad de Colombia. Ahora bien, es pertinente destacar que desde una perspectiva académica y de seguridad, esta investigación permitirá identificar los riesgos asociados a la convergencia entre el tráfico de prendas militares y la dimensión cibernética, contribuyendo a la formulación de estrategias para la prevención, monitoreo y sanción de estos delitos. Asimismo, se busca generar recomendaciones para el fortalecimiento de las capacidades estatales en ciberseguridad, impulsando el desarrollo de herramientas digitales

que permitan rastrear, identificar y desmantelar redes criminales operando en entornos digitales.

La intersección entre ciberseguridad y tráfico ilícito de prendas de uso privativo del Ejército Nacional representa una problemática de alta relevancia para la seguridad nacional. La evolución de las amenazas digitales exige una respuesta innovadora y adaptativa, en la que el Estado implemente mecanismos avanzados de protección de la información, inteligencia artificial para el rastreo de actividades ilícitas en la web y cooperación internacional en ciberseguridad. Abordar este tema desde una perspectiva integral contribuirá al fortalecimiento de la defensa nacional y a la consolidación de un marco estratégico más efectivo para combatir este fenómeno.

Respecto a lo dicho anteriormente, se plantea la siguiente pregunta de investigación: ¿Cómo se puede orientar el uso de la ciberseguridad en la protección de riesgos asociados a la proliferación de réplicas de camuflados? Para responder a esta pregunta, se propusieron los siguientes objetivos específicos: 1. identificar las principales amenazas cibernéticas relacionadas con la comercialización y distribución de réplicas de camuflados en entornos digitales, 2. evaluar las herramientas y tecnologías de ciberseguridad que pueden emplearse para detectar, prevenir y contrarrestar la falsificación y el tráfico de camuflados, 3. proponer lineamientos estratégicos y normativos para optimizar el uso de la ciberseguridad en la protección contra la proliferación de réplicas de camuflados, con base en experiencias y marcos legales nacionales e internacionales.

Metodología

Esta investigación adopta un enfoque cualitativo, dado que permite comprender fenómenos complejos dentro de su contexto natural y desde las interpretaciones que los propios actores sociales les otorgan (Álvarez et al., 2014). Esta perspectiva es especialmente pertinente para abordar la problemática del tráfico ilícito de prendas de uso privativo de las Fuerzas Militares, en tanto se trata de una actividad delictiva que opera en redes clandestinas, con múltiples dimensiones sociopolíticas, tecnológicas y de seguridad. El enfoque cualitativo permite examinar no solo las estrategias empleadas por los grupos criminales para eludir los controles estatales, sino también las fallas institucionales que permiten su proliferación, así como el papel cada vez más relevante que desempeña la ciberseguridad en la detección, prevención y mitigación de estos riesgos.

El método seleccionado para esta investigación es el descriptivo, el cual posibilita caracterizar detalladamente un fenómeno social sin necesidad de establecer relaciones causales definitivas (Martínez, 2020). A partir de este método se analizarán casos emblemáticos de tráfico de uniformes militares, con el propósito de identificar patrones operativos, canales de distribución, actores implicados y el uso de tecnologías digitales tanto para facilitar el delito como para enfrentarlo. El análisis descriptivo también permitirá exponer los principales desafíos institucionales en materia de inteligencia, control de inventarios militares, cooperación interagencial y capacidades cibernéticas del Estado colombiano.

En consonancia con la naturaleza cualitativa del estudio, se emplearán técnicas de análisis documental como método principal de recolección de información. Se utilizará una

matriz documental diseñada para clasificar las fuentes de información en primarias y secundarias, facilitando así una lectura sistemática y crítica del fenómeno. Las fuentes primarias incluirán documentos oficiales del Ejército Nacional de Colombia, informes de la Fiscalía General de la Nación, reportes de inteligencia de la Policía Nacional y de organismos gubernamentales que hayan participado en operaciones contra estas redes ilícitas.

Asimismo, se consultarán pronunciamientos de entidades internacionales, como la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC) y la INTERPOL, que hayan documentado casos similares en otras regiones. Dentro de estas fuentes primarias, se toma como referencia al Dr. Jairo Becerra y a Ivonne León (2019), quienes resaltan que en la actualidad, las tecnologías de la información y la comunicación (TIC) han generado una transformación profunda en las dinámicas sociales, económicas y políticas. Tanto el sector público como el privado han adoptado herramientas tecnológicas que permiten reducir costos y ofrecer respuestas más ágiles ante las demandas del entorno. Esta transformación, impulsada por la llamada cuarta revolución industrial, no solo ha acelerado los procesos cotidianos, sino que también ha favorecido la transparencia y el acceso eficiente a la información.

Este proceso de cambio se enmarca en un contexto global donde la información se convierte en el eje central de la transformación productiva. La Tecnología 4.0 integra diferentes niveles, ámbitos y actores en redes altamente complejas que funcionan como sistemas neuronales capaces de procesar y distribuir conocimiento en tiempo real. Según autores como Minsky (1988) y Castells (2006), esta nueva industria requiere estructuras organizativas flexibles, capaces de adaptarse y reorganizarse rápidamente.

Entre las principales características de estas redes destacan la instantaneidad, la interactividad, la virtualidad y la unicidad, lo cual ha dado paso a nuevas formas de organización, ajenas a restricciones físicas o territoriales. La globalización, unida al avance de las TIC, ha impulsado reformas en la administración pública hacia modelos de gobernanza más horizontales, cooperativos e inclusivos, lo que implica una ciudadanía más participativa y comprometida con los principios de equidad (Güedez, 2019)

Finalmente, este nuevo paradigma exige un Estado con la capacidad de articular, coordinar y liderar los esfuerzos sociales hacia objetivos comunes de desarrollo. La gobernanza, entendida como un sistema de toma de decisiones colectivas que involucra a actores estatales y no estatales, no solo redefine las estructuras institucionales, sino que transforma los métodos de producción y difusión del conocimiento (Reyes Beltrán, 2017; Rivera Méndez, 2010).

Por su parte, las fuentes secundarias estarán compuestas por literatura académica especializada en tráfico de bienes militares, ciberseguridad, inteligencia estratégica y crimen organizado. También se incluirán artículos científicos, reportajes periodísticos, estudios de caso y análisis técnicos sobre ciberamenazas emergentes relacionadas con el uso indebido de uniformes militares y su comercialización en plataformas digitales. Esta combinación de técnicas permitirá una comprensión integral del fenómeno, basada en el análisis de información multidimensional y contextualizada. De acuerdo con Campoy y Gomes (2022), el enfoque cualitativo apoyado en fuentes diversas es esencial para entender las motivaciones, estructuras operativas y estrategias de los actores involucrados en actividades ilícitas, lo que a su vez facilita la formulación de respuestas efectivas en términos de política pública, regulación y seguridad nacional.

Resultados

Principales amenazas cibernéticas relacionadas con la comercialización y distribución de réplicas de camuflados en entornos digitales

La industria manufacturera enfrenta diversas amenazas cibernéticas, entre las que se destacan el ransomware, los ataques dirigidos a la cadena de suministro, el phishing, las amenazas internas y las técnicas de ingeniería social. En 2023, este sector concentró el 25 % de los ciberataques a nivel global, lo que lo posiciona como el más afectado por este tipo de delitos (IBM, 2024). Dado su creciente uso del Internet de las Cosas (IoT) para optimizar procesos y aumentar la productividad, resulta fundamental abordar los riesgos asociados a la ciberseguridad (Jaryeong, Kaylee, y Darren, 2025).

Comprender la importancia de la seguridad informática en el entorno industrial, así como conocer las principales amenazas y las acciones necesarias para mitigarlas, es clave para garantizar la continuidad operativa y la protección de los activos digitales.

La seguridad cibernética se ha convertido en un pilar estratégico para las empresas del sector manufacturero. Esto se debe a la automatización progresiva de sus procesos —como las líneas de producción, los sistemas de control o la gestión de inventarios— los cuales dependen cada vez más de tecnologías digitales que, sin protección adecuada, pueden ser vulnerables a ataques.

El aumento de incidentes cibernéticos dirigidos a este sector pone de manifiesto la urgencia de establecer mecanismos de defensa más sólidos. Los delincuentes digitales aprovechan las brechas en los sistemas para interrumpir operaciones, sustraer información

confidencial y generar pérdidas económicas significativas, afectando tanto la calidad como los tiempos de producción (Jaryeong, Kaylee, y Darren, 2025).

Además, la complejidad de las redes industriales, que integran tecnologías de la información (TI) y tecnologías operativas (TO), representa un reto adicional. Mientras las TI gestionan datos, comunicaciones y planificación, las TO controlan equipos de producción, sensores y maquinaria automatizada (Cisco, s. f.). El uso de dispositivos IoT, como sensores inteligentes y cámaras, permite recopilar información en tiempo real para mejorar la eficiencia. No obstante, cada dispositivo conectado representa un posible punto de acceso para ciberataques, ampliando de manera significativa la superficie de riesgo (Zhukabayeva et al., 2025).

En este contexto, se ha documentado que al integrar elementos modernos de TI en arquitecturas OT antiguas, las infraestructuras industriales se vuelven objetivos atractivos para atacantes sofisticados que explotan vulnerabilidades en protocolos obsoletos (Makrakis et al., 2021). La convergencia entre TI y TO, si bien impulsa eficiencia y productividad, requiere de un enfoque robusto en seguridad digital que contemple cifrado, segmentación de redes y detección temprana de anomalías (IBM, 2024).

De hecho, investigaciones recientes sobre ciberseguridad en manufactura inteligente subrayan que los dispositivos IoT industriales, si no se protegen adecuadamente, facilitan la manipulación o el acceso no autorizado a datos sensibles (Masum, 2023; Ugwuanyi & Irvine, 2021). Por eso, fortalecer los sistemas de seguridad digital es indispensable para proteger las operaciones industriales en este contexto tecnológico cada vez más interconectado (Sumit & Vardhan, 2025).

Las amenazas en el entorno digital pueden adoptar múltiples formas y representan serios riesgos para el sector manufacturero. A continuación, se detallan algunos de los peligros más relevantes:

Ransomware

Respecto a esta amenaza, es pertinente resaltar que esta es una de las más graves, toda vez e este tipo de ataque bloquea el acceso a sistemas o datos mediante cifrado y exige un pago a cambio de la clave para restaurarlos. Ahora, en el ámbito manufacturero, los sistemas de control de producción y los módulos de gestión de inventarios suelen ser los blancos más comunes, así las cosas, cuando un ataque de este tipo tiene éxito, puede detener las operaciones, generar retrasos en la cadena logística y causar pérdidas económicas significativas.

Un ejemplo de este caso fue el ataque a una multinacional en el año 2022 cuya actividad principal es la fabricación de neumáticos, fue víctima de un ataque de ransomware, este incidente ocasionó interrupciones en sus operaciones y la empresa se vio obligada a desconectar las redes de todas sus plantas en América del Norte y América Latina, en esta oportunidad los atacantes accedieron a información confidencial, incluidos archivos sensibles de clientes, y amenazaron con hacerlos públicos si no se cumplía con el pago exigido (Jaryeong, Kaylee, y Darren, 2025).

Ataques a la cadena de suministro

Esta es otra amenaza crítica ya que los delincuentes aprovechan las debilidades de los proveedores o aliados comerciales para penetrar los sistemas de una empresa y en lugar

de atacar directamente a la organización o a la institución, se infiltran a través de un tercero con menores niveles de seguridad. Este tipo de incursión puede extender su impacto a lo largo de toda la red de negocios. Un ejemplo conocido es el ataque perpetrado en 2020 contra SolarWinds, proveedor de soluciones de software de gestión TI. Los atacantes introdujeron un código malicioso en su plataforma Orion, utilizada por numerosas empresas y entidades gubernamentales en EE.UU. Este malware permitía el acceso no autorizado a los sistemas de los clientes, lo que derivó en la instalación de programas maliciosos adicionales y un mayor compromiso de seguridad en múltiples redes (Jaryeong, Kaylee, y Darren, 2025).

Amenazas internas

Estas amenazas provienen del personal de la organización, como empleados o contratistas, que, ya sea por descuido o intención maliciosa, pueden comprometer la seguridad de los sistemas, toda vez que un trabajador con acceso innecesario puede cometer errores que vulneren la infraestructura digital o incluso filtrar información estratégica.

En 2023, Tesla fue protagonista de uno de los incidentes de filtración más grandes en su historia. Dos exempleados compartieron información personal de más de 75.000 personas, incluidos datos de empleados, con un medio internacional. Aunque la información no fue publicada, la empresa podría enfrentar sanciones de hasta 3.300 millones de dólares por infringir la normativa europea de protección de datos (GDPR).

Phishing y ataques de ingeniería social

Los fraudes mediante phishing y técnicas de ingeniería social son métodos frecuentes empleados por ciberdelincuentes para manipular a los trabajadores y obtener acceso a datos sensibles. Estos ataques se presentan comúnmente como correos electrónicos falsos, mensajes de texto engañosos, llamadas fraudulentas o sitios web clonados, diseñados para que los usuarios revelen información crítica o realicen acciones que comprometan la seguridad (Jaryeong, Kaylee, y Darren, 2025).

Un caso relevante tuvo lugar en 2019, cuando Toyota Boshoku Corporation, filial de Toyota, fue víctima de un ataque de tipo BEC (compromiso de correo electrónico corporativo). Los atacantes se hicieron pasar por un socio comercial confiable y lograron persuadir a un empleado para que autorizara una transferencia bancaria fraudulenta, lo que resultó en una pérdida de 37 millones de dólares en pocas horas.

Las amenazas a la seguridad de la industria manufacturera no solo se limitan al ámbito digital. Aunque ataques como el ransomware, el phishing, la ingeniería social y las vulnerabilidades en la cadena de suministro representan riesgos crecientes para este sector, también existen amenazas físicas que, al igual que las cibernéticas, comprometen la integridad operativa, la confidencialidad de la información y la seguridad nacional (Revista Cambio, 2024).

Ahora, para el caso de Colombia, un claro ejemplo de esto es el reciente operativo liderado por la Fiscalía General de la Nación y el Ejército Nacional, en el cual fue desarticulada una red clandestina dedicada a la fabricación y comercialización de uniformes falsificados de uso exclusivo de las Fuerzas Militares. Este caso pone de manifiesto cómo la

infiltración de actores maliciosos dentro de procesos de manufactura incluso desde estructuras informales o ilegales puede representar un riesgo paralelo al de los ciberataques. La fabricación y distribución de uniformes militares falsos, además de vulnerar derechos de propiedad industrial, expone al país a escenarios de suplantación de identidad, infiltración en organismos de seguridad y actividades delictivas con apariencia de legalidad.

Ambos fenómenos la cibercriminalidad y la falsificación de productos estratégicos revelan una misma necesidad: fortalecer los sistemas de protección, tanto físicos como digitales, en entornos de manufactura. La conexión entre las tecnologías de la información (TI) y las tecnologías operativas (TO), especialmente a través del Internet de las Cosas (IoT), incrementa los puntos vulnerables. Así como los dispositivos conectados pueden ser explotados para interrumpir operaciones y extraer datos sensibles, también los procesos productivos no regulados pueden dar paso a la creación de artículos críticos que son utilizados con fines ilícitos (Revista Cambio, 2024).

Esto sugiere que la seguridad en la industria manufacturera debe abordarse de manera integral, incluyendo tanto la protección frente a ataques digitales como la supervisión estricta de las cadenas de suministro físico y la verificación de legitimidad en los productos fabricados. En un contexto donde las fronteras entre lo cibernético y lo físico se difuminan, la fabricación ilegal de elementos militares y los ciberataques a sistemas de manufactura deben ser entendidos como expresiones de una misma amenaza multidimensional.

Comercialización ilegal de prendas militares

La comercialización ilegal de uniformes y accesorios militares en Colombia no solo constituye un delito contra los derechos de propiedad industrial, sino que se encuentra en una

zona crítica donde confluyen la seguridad nacional, la economía informal, el crimen organizado y, más recientemente, las amenazas cibernéticas. Este fenómeno ha cobrado mayor relevancia ante los constantes decomisos de prendas falsificadas que imitan a las utilizadas por el Ejército, la Policía y la Fuerza Aérea, elementos que, en manos equivocadas, pueden facilitar delitos de suplantación, extorsión, secuestro y ataques armados (Revista Cambio, 2024).

Instrumentalización por Grupos Armados Ilegales

Diversos reportes de inteligencia han evidenciado que estas prendas falsas son empleadas por grupos como las disidencias de las FARC y estructuras criminales del ELN para camuflar sus acciones e infiltrar territorios donde operan fuerzas legítimas del Estado. Como lo documentó El Tiempo en enero de 2024, más de 50 uniformes similares a los del Ejército Nacional fueron decomisados en Caquetá, en poder de un supuesto colaborador del grupo armado "Carolina Ramírez" del Estado Mayor Central (EMC) (El Tiempo, 2024).

Esta práctica plantea un riesgo directo para las comunidades, pues cualquier grupo que logre hacerse pasar por miembros del Ejército o la Policía puede operar con mayor facilidad, generar confusión entre los ciudadanos y obstaculizar las labores de inteligencia de las autoridades legítimas.

Conexión con Cadenas de Suministro y Plataformas Digitales

La comercialización de estos uniformes no ocurre únicamente en tiendas físicas o talleres clandestinos, sino que ha migrado hacia plataformas digitales y redes sociales. A través de mercados electrónicos no regulados, como Facebook Marketplace o sitios web poco controlados, se ofrecen prendas tácticas con emblemas oficiales, muchas veces sin

verificación de origen. Estos canales son también susceptibles de ser utilizados por redes criminales para lavar dinero o financiar actividades ilegales, aprovechando las lagunas jurídicas y la débil trazabilidad del comercio electrónico informal.

Esta digitalización del mercado negro expone tanto a usuarios como a productores legales a ciberataques, suplantación de marca y sabotajes informáticos. Como lo advierte la firma de ciberseguridad Kaspersky, las industrias manufactureras y de moda son particularmente vulnerables debido a sus altos volúmenes de transacciones, su uso de proveedores externos y sus sistemas interconectados sin la debida protección (Kaspersky, 2023).

En complemento de lo anterior, hay que decir que la vulnerabilidad de las industrias manufactureras y de moda a ciberataques, suplantación de marca y sabotajes informáticos, debido a la digitalización del mercado negro y la interconexión de sus sistemas, se basa en diversos informes y análisis de Kaspersky.

La creciente sofisticación de estos ataques se atribuye al uso extendido de tecnologías industriales conectadas y a la integración en cadenas de suministro globales, lo que genera vulnerabilidades críticas si uno de los eslabones no cuenta con medidas de ciberseguridad adecuadas. María Isabel Manjarrez, investigadora de seguridad en Kaspersky, explicó que la atracción hacia la manufactura se debe a sus sistemas de tecnología industrial y a la conectividad de sus cadenas de suministro, que las convierten en un blanco atractivo.

Además, Kaspersky ha destacado que la rápida automatización y digitalización en los sectores de logística y transporte están introduciendo nuevos desafíos, incluyendo la combinación de delitos cibernéticos y tradicionales, como el robo de vehículos y mercancías, la piratería marítima y el contrabando. Estos ciberataques no dirigidos podrían tener

consecuencias físicas, especialmente en vehículos fluviales, marítimos y camiones (Kaspersky, 2023).

Estos hallazgos subrayan la necesidad urgente de que las industrias manufactureras y de moda refuercen sus medidas de ciberseguridad, especialmente considerando la creciente digitalización y la interconexión de sus sistemas, que las hacen particularmente vulnerables a diversas amenazas cibernéticas.

Impacto sobre la Confianza Pública y las Instituciones

La proliferación de uniformes militares falsos mina la credibilidad de las instituciones del Estado. Si un civil es víctima de un delito cometido por una persona que porta prendas oficiales —aunque sean falsificadas—, se produce un efecto de deslegitimación que impacta la percepción ciudadana de las fuerzas armadas. Según el Observatorio de Seguridad y Defensa del Centro de Estudios Estratégicos de Colombia, la confianza en las instituciones se erosiona cuando los símbolos del Estado (como uniformes e insignias) son usados en contextos criminales, generando un "efecto espejo" donde lo ilegal imita lo legal, confundiéndolos frente a la ciudadanía.

Desafío para la Propiedad Intelectual y la Industria Legal

Empresas colombianas que legalmente producen uniformes para el Estado deben cumplir altos estándares de calidad, trazabilidad y seguridad en sus procesos. La existencia de un mercado paralelo que produce réplicas sin autorización no solo vulnera sus derechos comerciales, sino que representa una competencia desleal que afecta el empleo y la economía formal del país. De acuerdo con datos de la Cámara Colombiana de la Confección y Afines, cerca del 30% de los productos militares que circulan en ferias y tiendas no están certificados,

lo que implica un vacío normativo y fiscal que debe ser atendido con políticas públicas más efectivas.

Herramientas y tecnologías de ciberseguridad que pueden emplearse para detectar, prevenir y contrarrestar la falsificación y el tráfico de camuflados

El uso de productos falsificados puede generar consecuencias graves, especialmente cuando están involucrados en sectores estratégicos como las infraestructuras críticas como el ámbito militar. Entre los impactos más significativos se encuentran las enormes pérdidas económicas estimadas en miles de millones de dólares anuales solo en países como el Reino Unido (por dar un ejemplo), así como serios riesgos operativos derivados de fallos en armamento y vehículos militares, provocados por piezas no originales.

Frente a esta amenaza, se vuelve indispensable desarrollar estrategias sólidas que ayuden a prevenir la falsificación y aseguren la integridad de las cadenas de suministro, sin embargo, es de resaltar que uno de los factores que ha intensificado este problema es la globalización, la cual ha incentivado la subcontratación como mecanismo de reducción de costos. Lo anterior da lugar a redes de suministro más complejas y fragmentadas, donde múltiples actores participan en diferentes niveles de producción y distribución (Aniello, Halak, Chai, Dhall, Wilczynski, 2019).

Este nuevo panorama presenta tres desafíos fundamentales:

1. **Falta de visibilidad**: La creciente complejidad de las relaciones entre compradores y proveedores dificulta la supervisión de las primeras etapas del proceso, lo cual impide verificar la autenticidad de los componentes adquiridos.

2. **Déficit de trazabilidad**: Los datos sobre el recorrido de los productos se encuentran fragmentados entre distintas empresas, dificultando el seguimiento de los artículos hasta su origen y limitando la posibilidad de realizar investigaciones precisas en caso de irregularidades.
3. **Ausencia de mecanismos de rendición de cuentas**: La opacidad del sistema facilita el comportamiento fraudulento, ya que no existen herramientas efectivas para exigir responsabilidad a cada eslabón de la cadena por su participación en la fabricación o distribución.

En este contexto, la implementación de soluciones tecnológicas avanzadas para la detección, trazabilidad y autenticación de productos se vuelve clave para enfrentar de forma efectiva el fenómeno de la falsificación, destacando que la mayoría de los artículos falsificados no cumplen con los estándares de seguridad ni con los requisitos normativos establecidos, lo cual ocasiona múltiples costos indirectos como ya se mencionó anteriormente.

Existen numerosas tecnologías diseñadas para prevenir la falsificación, utilizadas en productos diversos como documentos legales, billetes, medicamentos, entre otros. Aunque no es el objetivo de este apartado detallar todas estas técnicas, es importante mencionar que muchas de ellas incluyen el uso de etiquetas especiales, sellos o modificaciones directas sobre el producto. También se emplean métodos que requieren dispositivos o condiciones específicas para su lectura, como la iluminación ultravioleta. Si bien estos mecanismos suelen ser precisos, también implican mayores costos de fabricación y monitoreo, no pueden implementarse retroactivamente en productos ya existentes y presentan limitaciones adicionales (García, Mellouli, Rehman, Cypheme, 2024).

Además, es fundamental señalar que los ingresos obtenidos a través de la comercialización de falsificaciones frecuentemente se destinan a financiar otras actividades ilícitas como el narcotráfico o la trata de personas, lo cual amplifica su impacto negativo a nivel económico, social y humano.

La propuesta consiste en aplicar redes neuronales profundas[1] para clasificar imágenes tomadas con teléfonos inteligentes, enfocándose en detectar logotipos o emblemas (como el cocodrilo de una marca). El sistema emplea transferencia de aprendizaje con un modelo EfficientDet-D0[2] para localizar el logo, y utiliza una Red de Transformadores Espaciales (STN)[3] para alinear las imágenes, mejorando la capacidad del modelo ante rotaciones o escalas. Aunque puede incluir datos contextuales (ubicación, entorno, historial), el rendimiento aquí se evalúa solo con imágenes. Esta solución supera los métodos manuales por su precisión, bajo costo y escalabilidad, toda vez que se basa en modelos de inteligencia artificial o redes neuronales profundas, puede alcanzar niveles de precisión mucho más altos al analizar grandes cantidades de datos con criterios consistentes. Esto significa que la detección de falsificaciones o anomalías es más confiable y menos propensa a errores subjetivos (Goodfellow, Bengio & Courville, 2016).

El comercio de productos falsificados se ha convertido en una amenaza creciente para la economía global, la salud pública y la seguridad del consumidor. Este fenómeno afecta no

[1] Es un modelo computacional inspirado en el cerebro humano, compuesto por múltiples capas de neuronas artificiales. Su objetivo es aprender representaciones jerárquicas de los datos de entrada (Goodfellow, Bengio & Courville, 2016).
[2]Se trata de una arquitectura de detección de objetos optimizada para lograr un balance entre precisión y eficiencia computacional. Utiliza como base EfficientNet (una red optimizada para clasificación de imágenes) y lo combina con un BiFPN (Bidirectional Feature Pyramid Network), que permite fusionar información de múltiples resoluciones de manera eficaz. El sufijo D0 indica la versión más ligera de la familia, ideal para dispositivos con recursos limitados, como teléfonos inteligentes (Tan, Pang & Le, 2020).
[3] Es un módulo diferenciable introducido por Jaderberg et al. (2015), que puede insertarse dentro de una CNN para otorgarle invariancia espacial. Esto significa que el modelo puede manejar variaciones en rotación, traslación o escalado de la imagen de entrada, ajustando automáticamente las características para facilitar su clasificación.

solo a las grandes marcas que pierden ingresos y reputación, sino también de manera más crítica al consumidor final, que muchas veces es víctima de estafas al adquirir productos supuestamente originales, pero de calidad inferior o incluso peligrosos.

Estudios recientes han revelado que aproximadamente el 3,3 % del comercio mundial involucra productos falsificados, una cifra alarmante que sigue aumentando con el auge del comercio electrónico y la distribución informal (OECD/EUIPO. (2019). Esta problemática no se limita a sectores como la moda o la tecnología, sino que alcanza industrias sensibles como la farmacéutica. Según datos de la Organización Mundial de la Salud (OMS), en 2017 los medicamentos falsificados representaban cerca del 15 % del mercado global, lo cual tiene consecuencias directas sobre la salud y la vida de millones de personas.

Además de los riesgos sanitarios y económicos, el tráfico de productos falsificados contribuye a la economía ilegal, ya que las ganancias obtenidas rara vez son reguladas o supervisadas por organismos oficiales. Estos recursos suelen alimentar otras formas de delincuencia organizada, incluyendo el lavado de activos, la trata de personas o el financiamiento del terrorismo. Así, el impacto de este mercado ilícito se extiende más allá del consumidor afectado, convirtiéndose en un problema estructural que socava la gobernanza, la legalidad y el desarrollo sostenible.

En este contexto, herramientas como *SpotTheFake*[4], una plataforma que integra redes neuronales profundas para la detección automatizada de productos falsificados a partir de imágenes, se presentan como una alternativa innovadora, precisa y escalable frente a los

[4] Es un sistema que emplea redes neuronales profundas (CNN, Convolutional Neural Networks) para analizar fotografías tomadas con teléfonos inteligentes y determinar si un producto es auténtico o falsificado. El objetivo es brindar un mecanismo ágil, económico y escalable para combatir la falsificación en mercados físicos y digitales (SpotTheFake Project, 2019).

métodos tradicionales de verificación manual. Este tipo de tecnología no solo mejora la eficiencia del control, sino que representa un avance importante en la lucha contra el comercio ilícito en un mundo cada vez más digitalizado (García, Mellouli, Rehman, Cypheme, 2024).

Tabla 1 Herramientas y tecnologías de ciberseguridad aplicadas a la detección y prevención de falsificación de camuflados

Herramienta / Tecnología	**Descripción**	**Aplicaciones en la prevención de falsificación**	**Ventajas**	**Limitaciones**
Blockchain	Registro distribuido e inmutable que enlaza bloques de información criptográficamente (Tapscott & Tapscott, 2016).	Asegura la **trazabilidad digital** de cada prenda o insumo desde su origen hasta su destino.	Transparencia, inmutabilidad, confianza sin intermediarios.	Requiere infraestructura tecnológica robusta y estandarización interinstitucional.
Funciones Físicamente Inconables (PUF)	Identificadores únicos derivados de las propiedades físicas irrepetibles de los chips electrónicos (Maes, 2013).	Autenticación de etiquetas y dispositivos electrónicos en prendas militares.	Difíciles de clonar, bajos costos de integración en hardware.	Poca aplicabilidad en productos ya fabricados; requiere diseño previo en el proceso de producción.
Sistemas de Ciberintelige ncia	Procesos y técnicas que analizan datos de redes, big data y OSINT para identificar amenazas (Rid, 2013).	Detección de redes ilegales de falsificación en entornos digitales y monitoreo de mercados clandestinos.	Permite anticipar amenazas, identificar actores maliciosos y fortalecer la seguridad nacional.	Alto costo de implementación; requiere especialistas en análisis de datos y ciberseguridad.
Redes Neuronales Profundas (IA)	Algoritmos de aprendizaje automático que analizan imágenes y patrones	Clasificación automática de imágenes capturadas con smartphones	Alta precisión, bajo costo operativo, escalabilidad.	Necesita bases de datos amplias para entrenar modelos y

	complejos (Goodfellow, Bengio & Courville, 2016).	para validar autenticidad de logos y uniformes (ej. SpotTheFake).		constante actualización.
Etiquetas y sellos de seguridad	Marcas visibles o invisibles aplicadas directamente sobre el producto (García, Mellouli, Rehman & Cypheme, 2024).	Verificación manual o con dispositivos especializados de prendas militares auténticas.	Método tradicional, relativamente fácil de implementar.	Costos adicionales, no aplicable a productos ya fabricados, riesgo de ser replicados.

Nota: Elaboración propia

Ahora bien, ya centrando la atención especialmente en lo que representa para el Ejército Nacional, hay que decir que la falsificación de uniformes y prendas de uso exclusivo de las Fuerzas Militares no solo vulnera el marco legal vigente (artículo 346 del Código Penal), sino que también representa un riesgo operativo, logístico y reputacional para las instituciones de seguridad del Estado. La utilización de estos elementos por actores armados ilegales, estructuras criminales o individuos con fines de suplantación institucional genera escenarios de riesgo que demandan una respuesta integral. En este contexto, el Ejército Nacional ha desarrollado diversas estrategias para prevenir y controlar este fenómeno, tanto desde una perspectiva interna como mediante acciones de inteligencia externa.

Control logístico interno en la producción de uniformes

Según información publicada por la Revista Semana (2017), el Batallón de Intendencia No. 1 "Las Juanas" implementa mecanismos de trazabilidad y seguridad logística en la producción de uniformes oficiales. Cada rollo de tela entregado para confección está numerado y codificado, permitiendo su seguimiento dentro del sistema logístico. Además, todo excedente textil es destruido mediante pulverización, lo que impide su uso en contextos

no autorizados. Estas prácticas fortalecen el control interno, minimizan el riesgo de fuga de insumos y garantizan la autenticidad del material utilizado por los miembros activos del Ejército Nacional.

Operaciones de inteligencia contra redes ilegales de falsificación

Para 2024 se realizaron una serie de operativos conjuntos entre el Ejército Nacional, la Policía Nacional y la Fiscalía General de la Nación, orientados a la identificación y desmantelamiento de talleres ilegales de confección de uniformes militares. Estas operaciones, realizadas en departamentos como Tolima y Cundinamarca, permitieron la incautación de maquinaria industrial, prendas falsificadas, insignias oficiales y material balístico. Los operativos también resultaron en capturas e imputaciones por delitos contra la fe pública y la seguridad. La eficacia de estas intervenciones se sustenta en labores de contrainteligencia, vigilancia territorial y judicialización de los responsables.

Tabla 2. Comparativo estrategias de prevención y control

Criterio	**Control logístico interno**	**Operaciones de inteligencia**
Enfoque principal	Prevención del desvío interno de materiales	Detección y desarticulación de redes ilegales
Ubicación de aplicación	Instalaciones militares (Batallón de Intendencia)	Zonas urbanas y rurales (Bogotá, Tolima, Cundinamarca)
Herramientas utilizadas	Codificación de telas, trazabilidad, destrucción de excedentes	Inteligencia militar, vigilancia, operativos judiciales
Actores involucrados	Ejército Nacional	Ejército, Policía Nacional, Fiscalía, CTI
Resultado esperado	Evitar fuga de materiales desde la producción oficial	Neutralizar estructuras de falsificación y distribución ilícita
Naturaleza de la estrategia	Preventiva y logística	Reactiva y operativa

Nota: Elaboración propia con datos de Semana (2024).

La comparación entre ambos enfoques revela una estrategia dual por parte del Estado, mientras que el control logístico busca prevenir el desvío interno de materiales, las operaciones de inteligencia actúan sobre redes externas que ya han violado el marco legal. La eficacia de esta doble vía reside en la complementariedad entre prevención y reacción. No obstante, se identifica como oportunidad de mejora la necesidad de incorporar tecnologías emergentes, tales como blockchain para trazabilidad digital que es una tecnología de registro distribuido que permite almacenar información de manera descentralizada, inmutable y transparente, esta tecnología funciona como una cadena de bloques en la que cada bloque contiene datos validados y enlazados criptográficamente con el anterior, lo que hace extremadamente difícil alterar la información sin que se detecte (Tapscott & Tapscott, 2016), funciones físicamente inclonables (PUF)[5] para autenticación de etiquetas, y sistemas de ciberinteligencia, entendidos como es el conjunto de procesos, técnicas y herramientas destinadas a recolectar, analizar y transformar datos de múltiples fuentes digitales en información útil para anticipar, detectar y neutralizar amenazas en el ciberespacio. Estos sistemas combinan monitoreo de redes, análisis de big data, machine learning y fuentes abiertas (OSINT) para identificar patrones de ataques, actores maliciosos y vulnerabilidades. En el ámbito militar y de seguridad nacional, la ciberinteligencia resulta esencial para proteger infraestructuras críticas, detectar campañas de desinformación y prevenir

[5] Funciones Físicamente Inconables (PUF, Physical Unclonable Functions) son mecanismos de seguridad basados en las propiedades físicas únicas e irrepetibles de cada componente electrónico. Estas funciones aprovechan pequeñas variaciones de fabricación en los circuitos para generar respuestas únicas a estímulos eléctricos, lo que equivale a una "huella digital" del dispositivo. Los PUF se utilizan para autenticación de hardware, protección de identidades digitales y generación segura de claves criptográficas, ya que son prácticamente imposibles de duplicar o falsificar, incluso con acceso directo al dispositivo (Maes, 2013).

ciberataques dirigidos (Rid, 2013) y que se usan para monitoreo de canales de distribución ilícita, especialmente en entornos digitales.

Lineamientos estratégicos y normativos para optimizar el uso de la ciberseguridad en la protección contra la proliferación de réplicas de camuflados, con base en experiencias y marcos legales nacionales e internacionales

La proliferación de réplicas de camuflados del Ejército Nacional en el mercado ilegal, tanto físico como digital, representa una amenaza directa a la seguridad nacional. Este fenómeno facilita la suplantación de miembros de la Fuerza Pública, pone en riesgo a la población civil y compromete operaciones militares. Frente a este desafío, la implementación de lineamientos estratégicos y normativos en materia de ciberseguridad se convierte en una necesidad prioritaria para garantizar la protección de los diseños originales, así como la trazabilidad y control de su distribución.

a. Contexto normativo nacional e internacional

En Colombia, la Ley 1581 de 2012 sobre protección de datos personales, la Ley 1273 de 2009 sobre delitos informáticos y el Decreto 1078 de 2015 sobre gobernanza digital establecen un marco normativo fundamental para el tratamiento seguro de información en entornos digitales. Sin embargo, estas normas no abordan de forma específica la protección de información clasificada como estratégica o de seguridad nacional, como es el caso de los patrones de camuflaje militar. Por tanto, se requiere una actualización del marco legal que considere la protección de este tipo de información como un asunto de ciberdefensa.

A nivel internacional, organismos como la OTAN han establecido buenas prácticas en materia de ciberseguridad militar. En sus manuales estratégicos se promueve el desarrollo

de capacidades de detección temprana, protocolos de cifrado robusto, y sistemas de respuesta rápida ante incidentes de seguridad digital (OTAN, 2020). Asimismo, países como Israel y Estados Unidos han creado normativas específicas para proteger la propiedad intelectual de desarrollos militares mediante esquemas de clasificación y control de acceso digitales, respaldados por tecnología blockchain y sistemas de inteligencia artificial (Dobbins et al., 2015).

b. Estrategias para la implementación de lineamientos estratégicos

1. Clasificación y segmentación de información crítica

Los diseños de camuflados deben gestionarse como activos de alta sensibilidad, comparables a la información de inteligencia. Una clasificación estricta permite establecer niveles jerárquicos de acceso, de modo que solo personal autorizado pueda consultar, editar o distribuir los archivos. La segmentación se complementa con controles de autenticación multifactor (MFA), que reducen la probabilidad de accesos indebidos, y con un monitoreo continuo de la actividad de usuarios internos, detectando patrones sospechosos. Esta medida responde a la creciente amenaza de insiders, responsables de filtraciones intencionadas o accidentales en contextos militares y corporativos.

2. Cifrado y respaldo seguro de diseños originales

El cifrado de extremo a extremo garantiza que los archivos de patrones de camuflaje se mantengan inaccesibles incluso si son interceptados. La implementación de algoritmos robustos como AES-256 o RSA es indispensable para cumplir con estándares internacionales de seguridad. Asimismo, los repositorios digitales seguros deben contar con respaldo automático, redundancia geográfica y registros de auditoría, lo que no solo protege la integridad de los archivos, sino que asegura la disponibilidad de información crítica ante

ataques de ransomware o fallos técnicos. Esto otorga resiliencia digital en un escenario donde la pérdida de un diseño puede comprometer la operatividad de las fuerzas armadas.

3. Sistemas de trazabilidad y blockchain

El uso de blockchain en la gestión de camuflados garantiza la inmutabilidad de registros, la verificación descentralizada y la transparencia en la cadena de suministro. Cada bloque registraría transacciones específicas: creación del diseño, autorización de confección, transporte y distribución. De esta forma, cualquier intento de alteración o falsificación quedaría registrado de manera visible. En entornos militares, la trazabilidad digital permite identificar rápidamente desviaciones o filtraciones, al mismo tiempo que fortalece la confianza interinstitucional en los procesos logísticos.

4. Vigilancia digital y ciberinteligencia

El establecimiento de unidades especializadas de ciberinteligencia militar permitiría monitorear de forma sistemática plataformas digitales, marketplaces y foros clandestinos, donde se promocionan réplicas de camuflados. A través de técnicas de OSINT (Open Source Intelligence), análisis de big data y machine learning, es posible identificar patrones de venta ilegal, geolocalizar actores maliciosos y coordinar operaciones de interdicción. Este enfoque proactivo complementa los mecanismos tradicionales de vigilancia física y facilita la detección temprana de focos de producción y comercialización ilícita.

5. Colaboración con actores internacionales

El tráfico de réplicas militares constituye un delito transnacional, por lo que la cooperación internacional es esencial. El Ejército Nacional debe articularse con organismos como INTERPOL, la OTAN y la OEA, compartiendo información sobre redes ilícitas, tipologías de falsificación y tecnologías de autenticación. Los convenios bilaterales

permitirían operaciones conjuntas de incautación y judicialización más allá de las fronteras nacionales. Además, la cooperación facilita el acceso a buenas prácticas globales en ciberdefensa y al uso compartido de herramientas tecnológicas de última generación.

Formación y sensibilización institucional

La ciberseguridad no depende únicamente de la tecnología, sino también de la cultura organizacional. Es crucial capacitar al personal militar involucrado en el diseño, confección y custodia de camuflados en:

- Riesgos digitales, como phishing, malware o ingeniería social.
- Buenas prácticas éticas y normativas, vinculadas a la seguridad nacional.
- Simulaciones de incidentes reales, que fortalezcan la capacidad de respuesta.

Además, se recomienda implementar campañas internas de sensibilización que promuevan la denuncia anónima de irregularidades y refuercen la responsabilidad digital como un valor central en la misión institucional (González & Torres, 2021).

Propuestas normativas específicas

- Normativa exclusiva para camuflados: Los patrones deberían recibir una clasificación similar a la información de inteligencia, restringiendo legalmente su acceso y reproducción.
- Registro digital obligatorio: Todo nuevo diseño debe inscribirse en una base de datos nacional encriptada, con control de versiones y auditorías periódicas.
- Sanciones agravadas: La filtración, venta o reproducción no autorizada debería tipificarse como delito agravado, aplicable tanto a servidores públicos como a actores externos, garantizando sanciones proporcionales al daño ocasionado.

Lecciones aprendidas y experiencias comparadas

- Corea del Sur: Ha implementado plataformas militares cerradas, accesibles solo desde redes internas seguras, lo que reduce las posibilidades de filtración de información sensible.
- Chile: Aplica protocolos de control de calidad que incluyen marcas ocultas en los tejidos de uniformes, las cuales permiten verificar la autenticidad incluso en zonas de combate.

Estas experiencias muestran que la combinación de infraestructura tecnológica, protocolos normativos y medidas operativas permite construir un marco integral para la protección de información y recursos militares sensibles. En Colombia, adaptar estas experiencias a las condiciones locales y a la infraestructura actual del Ejército permitiría dar un paso sólido hacia la consolidación de una defensa digital más robusta y coherente con los retos contemporáneos.

Conclusiones

El análisis realizado permite comprender que las amenazas cibernéticas no solo afectan la infraestructura tecnológica del Ejército Nacional, sino que comprometen aspectos fundamentales como la integridad de los diseños de camuflados, la seguridad operacional y la imagen institucional. El primer objetivo permitió identificar cómo la falsificación y comercialización digital de uniformes militares se ha convertido en una práctica extendida, facilitada por la debilidad de los controles digitales y por la falta de normativas especializadas.

El segundo objetivo abordó las herramientas tecnológicas disponibles para la detección y mitigación de estas amenazas. Se evidenció la utilidad de tecnologías como blockchain, inteligencia artificial y sistemas de monitoreo automatizados, pero también se identificó la necesidad de contar con talento humano capacitado y con procesos claros que permitan su integración efectiva en el contexto militar.

Finalmente, el desarrollo del tercer objetivo demuestra que no basta con tener recursos técnicos o herramientas digitales; es necesario contar con un marco normativo coherente, específico y actualizado que respalde toda la estrategia de ciberseguridad. La protección de los diseños de camuflados debe entenderse como una prioridad de seguridad nacional, no solo por su valor estratégico, sino por las implicaciones que tiene su uso indebido en la suplantación, el engaño y la desestabilización de las operaciones legítimas del Ejército.

En conjunto, los hallazgos de los tres objetivos sugieren la necesidad de una política integral de ciberseguridad militar que contemple tanto la prevención tecnológica como la regulación normativa y la formación del personal. Solo así será posible enfrentar de manera eficaz las amenazas digitales que atentan contra la confidencialidad y seguridad de la información sensible del Ejército Nacional.

Referencias

Álvarez, J., Gómez, M., y Restrepo, L. (2014). Diseños cualitativos en investigación social. Universidad Nacional de Colombia.

Aniello, L., Halak, B., Chai, K., Dhall, R., y Wilczynski, A. (2019). Towards a supply chain management system for counterfeit mitigation using Blockchain and PUF. https://arxiv.org/pdf/1908.09585

Bargent, J. (2015). *Colombia's criminal groups and the business of camouflage*. Insight Crime. https://insightcrime.org

Becerra, J., y León, I. (2019). La seguridad digital en el entorno de la Fuerza Pública: Diagnósticos y amenazas desde la gestión del riesgo. Bogotá: ESDEGUE Libros.

Campoy, R., y Gomes, C. (2022). Métodos cualitativos en investigación social: Teoría y práctica. Editorial UOC.

Castells, M. (2006). *La era de la información: economía, sociedad y cultura. Volumen I: La sociedad red*. Madrid: Alianza Editorial.

Centro Cibernético Policial. (2022). Informe anual de cibercrimen en Colombia. Policía Nacional de Colombia.

Cisco. (s. f.). IT/OT Convergence in Critical Infrastructure and Industrials. Cisco. https://www.cisco.com/c/en/us/solutions/collateral/industries/manufacturing/itot-convergence-wp.html

Corte Constitucional de Colombia. (2016). Sentencia C-748 de 2016. https://www.corteconstitucional.gov.co/relatoria/2016/C-748-16.htm

Departamento de Defensa de los Estados Unidos. (2006). National Military Strategy for Cyberspace Operations. https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf

DNP - Departamento Nacional de Planeación. (2022). Política nacional de seguridad digital. https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/CONPES%204044.pdf

Dobbins, J., McGinn, J. G., Crane, K., Jones, S. G., Lal, R., Rathmell, A., y Swanger, R. D. (2015). America's role in nation-building: From Germany to Iraq. RAND Corporation. https://www.jstor.org/stable/10.7249/mr1753rc

Ejército Nacional de Colombia. (2023). *Plan Ayacucho*. Bogotá: Ejército Nacional de Colombia. https://www.ejercito.mil.co/plan-ayacucho-efectividad-operacional/

El Tiempo. (2024, enero). *Decomisan más de 50 uniformes del Ejército en Caquetá destinados a disidencias de las Farc*. El Tiempo. https://www.eltiempo.com

Fernández, L. (2021). La ciberdefensa en Colombia: Un enfoque estratégico. Revista Seguridad y Defensa, 9(1), 34–45.

García, H., Mellouli, D., Rehman, A., y Cypheme, L. (2024). Deep neural network-based detection of counterfeit products from smartphone images. https://arxiv.org/pdf/2410.05969

Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep learning*. MIT Press.

Gómez, D. (2020). Propiedad intelectual y su protección ante delitos informáticos. Revista Jurídica Digital, 5(2), 77–93.

Gómez, C., & Ramírez, J. (2021). Seguridad digital y riesgos de la información en sistemas estatales. Revista Colombiana de Seguridad Informática, 12(2), 45–62.

Granadillo, J. (2013). Ciberseguridad y defensa nacional: un enfoque integral. Caracas: Instituto de Altos Estudios de Seguridad.

Güedez, J. J. (2019). Implicaciones de la gobernanza en el gobierno electrónico: Actores e interacciones. Revista Compendium. https://www.redalyc.org/journal/880/88062542004/

IBM. (2024). IT and OT cybersecurity: A holistic approach. IBM Insights. https://www.ibm.com/think/insights/it-and-ot-cybersecurity-integration

IBM Security. (2024). IBM X-Force Threat Intelligence Index 2024 (p. 8). IBM Corporation. Disponible en: https://newsletter.radensa.ru/wp-content/uploads/2024/03/IBM-XForce-Threat-Intelligence-Index-2024.pdf

Jaderberg, M., Simonyan, K., Zisserman, A., & Kavukcuoglu, K. (2015). Spatial transformer networks. Advances in Neural Information Processing Systems, 28.

Jaryeong, K., Kaylee, P., y Darren, G. (2025). Principales amenazas cibernéticas que ha de afrontar la industria manufacturera y cómo mitigarlas. Obtenido de Keeper: https://www.keepersecurity.com/blog/es/2025/02/06/top-cyber-threats-facing-manufacturing-and-how-to-mitigate-them/

Kaspersky. (2023). Los ataques al sector industrial van en aumento: un resumen anual de Kaspersky. Obtenido de https://www.kaspersky.com/about/press-releases/industrial-sector-attacks-on-the-rise-an-annual-overview-by-kaspersky

Martínez, A. (2020). *Metodología de la investigación cualitativa y cuantitativa*. Ciudad de México: Editorial Trillas.

Makrakis, G., Kolias, C., Kambourakis, G., Rieger, C., & Benjamin, J. (2021). Vulnerabilities and Attacks Against Industrial Control Systems and Critical Infrastructures. arXiv. https://arxiv.org/abs/2109.03945

Ministerio de Defensa Nacional. (2021). Plan estratégico de ciberseguridad del sector defensa. Bogotá: MDN.

Mindefensa. (2023). *Informe sobre tráfico de armas, municiones y explosivos en Colombia*. Bogotá: Ministerio de Defensa Nacional.

Minsky, M. (1988). *The society of mind*. New York: Simon & Schuster. https://www.jstor.org/stable/20708493

Miron, M. (2019). La guerra irregular, insurgencias y cómo contrarrestarlas. Revista Científica General José María Córdova, 17(27), 457–480. https://doi.org/10.21830/19006586.497

Naciones Unidas. (2020). Ciberseguridad y protección de activos estratégicos: Recomendaciones para América Latina. Nueva York: Oficina de Asuntos de Desarme.

OCDE. (2022). Cybersecurity policy making at a turning point: Analysing a new generation of national cybersecurity strategies for the Internet economy. https://www.oecd.org/sti/cybersecurity.htm

OECD/EUIPO. (2019). *Trends in Trade in Counterfeit and Pirated Goods* (versión PDF). https://www.eusemiconductors.eu/sites/default/files/uploads/201903_EUIPO-OECD_TrendsCF-PiratedGoods.pdf

Organización Mundial de la Salud. (2017). Informe sobre medicamentos falsificados. https://www.who.int/

Organización de Estados Americanos – OEA. (2019). Fortalecimiento de capacidades nacionales en ciberseguridad en América Latina. Washington, D.C.: OEA.

OTAN. (2020). *NATO cyber defence policy*. Brussels: North Atlantic Treaty Organization. https://www.nato.int

Pérez, J. (2023). Seguridad de la información en la industria textil de defensa: Retos ante la digitalización. Revista Colombiana de Defensa y Tecnología, 15(2), 109–125.

Policía Nacional de Colombia (PONAL). (2024). *Informe de incautaciones de armas y uniformes militares en Colombia*. Bogotá: Dirección de Investigación Criminal e INTERPOL.

RedSeguridad.com. (2022). *Ciberespionaje corporativo: modalidades y riesgos*. Red Seguridad. https://www.redseguridad.com

Reyes Beltrán, J. (2017). Gobernanza, participación y redes en la política pública colombiana. Bogotá: Ediciones Uniandes.

Revista Cambio. (2024). Incautan dos toneladas de uniformes y elementos militares que no tenían permisos. Obtenido de Revista Cambio: https://cambiocolombia.com/pais/contrabando-incautan-dos-toneladas-de-uniformes-elementos-fuerza-publica-por-venta-sin

Revista Semana. (2017). Así se controla la confección de los uniformes del Ejército para evitar que caigan en manos equivocadas. https://www.semana.com/nacion/articulo/asi-se-controla-la-confeccion-de-los-uniformes-del-ejercito-para-evitar-que-caigan-en-manos-equivocadas/542706/

Revista Semana. (2024). Desmantelan red que falsificaba uniformes del Ejército: la peligrosa amenaza que enfrentan las Fuerzas Militares. https://www.semana.com/nacion/articulo/desmantelan-red-que-falsificaba-uniformes-del-ejercito-la-peligrosa-amenaza-que-enfrentan-las-fuerzas-militares/202451/

Rivera Méndez, J. (2010). El Estado en la era digital. Departamento Nacional de Planeación (DNP). https://colaboracion.dnp.gov.co/CDT/Desarrollo%20Social/Estado_digital_RiveraMendez.pdf

Roa, C. (2022). Lineamientos jurídicos para la protección de diseños militares en el entorno digital. Revista de Derecho Militar, 28(3), 203–218.

Rojas, F., & López, A. (2023). *Ciberseguridad y soberanía nacional: Retos para América Latina*. Revista Iberoamericana de Seguridad Digital, 8(1), 77–94.

Serban, A., Ilas, G., y Cosmin, G. (2020). SpotTheFake: An initial report on a new CNN-enhanced platform for counterfeit goods detection. https://arxiv.org/pdf/2002.06735

Silva, P., & Pérez, L. (2022). *Falsificación de uniformes y riesgos de seguridad en Colombia*. Revista de Estudios en Seguridad y Defensa, 14(3), 101–120.

Suárez, A., y Mendoza, R. (2021). Ciberinteligencia y seguridad nacional: análisis del contexto colombiano. Revista de Estudios Estratégicos, 12(1), 66–84.

SolarWinds. (2020). Orion Platform Security Advisory. https://www.solarwinds.com/trust-center/security-advisories

SpotTheFake Project. (2019). *SpotTheFake: An early report on an enhanced CNN platform for counterfeit product detection*. arXiv preprint arXiv:1908.09585.

Tan, M., Pang, R., & Le, Q. V. (2020). EfficientDet: Scalable and efficient object detection. *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, 10781–10790.

Tarlogic. (2024). *Ciberespionaje: motivaciones y riesgos*. Tarlogic Security. https://www.tarlogic.com

Tesla. (2023). Data breach disclosure. https://www.tesla.com/legal/privacy

Toyota Boshoku Corporation. (2019). Official statement on phishing attack. https://www.toyota-boshoku.com/global/

Zhukabayeva, T., et al. (2025). *Cybersecurity Solutions for Industrial Internet of Things*. PMC / MDPI. https://pmc.ncbi.nlm.nih.gov/articles/PMC11723252