Amenazas y desafíos del terrorismo cibernético en Colombia: un enfoque en la seguridad nacional.

Mayor (EJC) John Alexander Vargas Martínez

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 (EJC) John Alexander Vargas Martinez
Identificación	**:**	1023875411
Programa académico	**:**	Maestría en Ciberseguridad y Ciberdefensa
Tutor metodológico	**:**	Cr. Aldemar Serrano Cuervo
Tutor temático	**:**	Do. Jonnathan Jiménez Reina
Fecha de entrega	**:**	26 de agosto de 2025
Extensión	**:**	7.820 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 autorizo que este articulo sea publicado por el Sello Editorial ESDEG en su repositorio institucional y esté disponible bajo una modalidad de acceso abierto.

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

Amenazas y desafíos del terrorismo cibernético en Colombia: un enfoque en la seguridad nacional.

Threats and challenges of cyberterrorism in Colombia: a focus on national security.

John Alexander Vargas Martínez[*]
Escuela Superior de Guerra "General Rafael Reyes Prieto"

Resumen: La investigación aborda el impacto del terrorismo cibernético en el marco de seguridad digital colombiano, considerando la evolución de las amenazas y la integración de inteligencia artificial. Utilizando un enfoque cualitativo, se analizaron conceptos clave, debilidades en la defensa cibernética y capacidades de respuesta militar frente a ataques duales. Los resultados destacan que ataques como ransomware y fuerza bruta poseen alta complejidad técnica y afectan infraestructuras públicas críticas, mientras que las amenazas locales tienen menor impacto. Basándose en lineamientos de la OTAN, se propone actualizar los núcleos estratégicos de defensa digital para mitigar riesgos emergentes y fortalecer la resiliencia cibernética en sectores clave.

Palabras clave: ciberseguridad, terrorismo, inteligencia, ransomware, OTAN, resiliencia.

Abstract: The research examines the impact of cyberterrorism on Colombia's digital security framework, focusing on evolving threats and artificial intelligence integration. Using a qualitative approach, key concepts, weaknesses in cyber defense, and military response capabilities to dual attacks were analyzed. Results reveal that ransomware and brute force attacks exhibit high technical complexity, affecting critical public infrastructures, while local threats have lower impact. Based on NATO guidelines, the study suggests updating strategic digital defense frameworks to mitigate emerging risks and enhance cyber resilience in key sectors.

Keywords: cybersecurity, terrorism, artificial intelligence, ransomware, NATO, resilience.

[*] Mayor del Ejército Nacional de Colombia. Candidato a magíster en Ciberseguridad y Ciberdefensa, Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia. Profesional en Ciencias Militares, Escuela Militar de Cadetes "General José María Córdova", Contacto: john.vargasm@esdeg.edu.co.

Introducción

La evolución de las amenazas cibernéticas configura en contexto colombiano una amenaza de naturaleza estructural, ya que su diversificación y rápida capacidad de impacto desafía el núcleo estratégico diseñado para la prevención de ataques cibernéticos.

Ese núcleo conformado por los CONPES 3701 de 2011 (Lineamientos de política para la ciber seguridad y ciber defensa), CONPES 3854 (Política Nacional de Seguridad Digital) y CONPES 3995 (Política Nacional de Confianza y Seguridad Digital), constituye un primer factor de análisis con el que se plantean dos enfoques de innovación: ciber seguridad como objetivo y política nacional e integración territorial entre el actor poblacional, sistemas de información y la red.

Sin embargo, el núcleo estratégico tiene por última publicación el CONPES 3995, en el que se plantean como retos el desconocimiento del sistema público en materia tecnológica, la ausencia de nuevas tecnologías para su integración a un marco social y un modelo de gobernanza que aborde el funcionamiento del concepto de ciber seguridad e integración cibernética (DNP, 2020).

Los retos supuestos en materia cibernética se suman a los ya planteados en 2011 y 2016, abordando la gestión de riesgos digitales y debilidades conceptuales frente a una estrategia de seguridad nacional cibernética.

Esta estructura estratégica conforma un primer escalón de seguridad digital, pero hay diferentes factores de mejoramiento por incluir si se tiene en cuenta que, según el CCOCI (2024), la fluctuación de Ransomware detectado fue de 1600 ataques, más otros dos millones a la red y 500.000 amenazas de infección local (CCOCI, 2024).

Estos datos ponen en el escenario un grupo de amenazas que evoluciona de manera constante en código, cantidad y forma de penetración.

Desde una perspectiva estratégico – regional, el aumento de ciberataques impacta sistemas públicos de gestión digital, sobre todo, en un periodo transicional en el que el marco tecnológico de inteligencia artificial representa un reto presente y prospectivo para el dominio digital colombiano.

Ahora, sumado a los retos establecidos entre 2011 y 2020, se anexa el de la adaptación de inteligencia artificial al modelo de gobernanza digital que el Estado ha implementado de manera articulada con instituciones y entidades.

A 2025, las vulnerabilidades digitales del Estado se centran principalmente en ataques a infraestructuras críticas cibernéticas y sistemas de información pertenecientes al sector público y privado. De hecho, a nivel de riesgo digital, Colombia se ubica en un nivel promedio relacionado con la capacidad de defensa cibernética y adaptación de inteligencia artificial (DNP, 2025).

Los retos presentados en este panorama exponen el planteamiento de un problema que genera riesgos al marco de protección cibernética multidimensional diseñada por instituciones del Estado colombiano (DNP, MINTIC, MIDDEFENSA).

Por ende, la investigación enmarca las causales del problema en un interrogante en el que hay tres variables: rápido aumento de ciber ataques, evolución constante de las amenazas y desconocimiento conceptual – poblacional e institucional de nuevas formas de afectación digital reguladas por inteligencia artificial. Ese interrogante es: **¿Cómo afectan las amenazas y desafíos del terrorismo cibernético al marco de seguridad cibernética nacional?**

La pregunta trae consigo otra categoría de análisis: el concepto de terrorismo cibernético que encierra las variables de ciber ataque, transgresión cibernética y disrupción de sistemas de información para el desarrollo del actor poblacional. Todo esto, según la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC, 2025), a fin de intimidar, concertar intereses políticos, de intimidación y coacción gubernamental (Jarvis, McDonald, & Nouri, 2014).

Bajo el argumento de los retos presentados en el primer núcleo estratégico (CONPES 3701, 3854 y 3995, más el segundo (CONPES 4144), se anexa la variable terrorismo y se describe que el problema identificado en la pregunta corresponde a la ausencia de un proceso de investigación disciplinar que con la conceptualización de políticas de seguridad en contra del terrorismo cibernético permita generar políticas de protección frente al surgimiento de amenazas disruptivas que se alineen con el marco de la OTAN.

La OTAN como autoridad militar en materia cibernética con su **Centro Integrado de Ciberdefensa**, permite a Estados miembro y socios globales orientar procesos de transformación estratégica basada en operaciones multidominio e intercambio de conocimiento en seguridad digital (Ertan, Floyd, Pernik, y Stevens, 2020).

Así los términos, el núcleo estratégico debe integrar a sus estándares de control y garantías de ciberseguridad, un análisis de las amenazas y desafíos que desde la acción del ciber terrorismo afectan el sistema cibernético de seguridad nacional, adoptando como enfoques estratégicos los direccionamientos en materia cibernética planteados por la OTAN.

Para ello, se seleccionó un enfoque cualitativo que describe el concepto de terrorismo cibernético a través de la construcción conceptual dada en el marco de ciberseguridad.

Una vez analizados los conceptos se pasa a un análisis estadístico y descriptivo de las principales amenazas al dominio cibernético colombiano y al final, tomando bases argumentativas como los lineamientos estratégicos para afrontar fenómenos derivados del terrorismo cibernético de la OTAN, plantear enfoques estratégicos que conduzcan a una actualización del núcleo primario y secundario de defensa digital actual.

El entregable final para este artículo es entonces un análisis segmentado de amenazas y desafíos de ciber terrorismo que enmarque los retos identificados por los dos núcleos estratégicos, pero que también integre acciones preventivas diseñadas a partir de los lineamientos de la OTAN.

Metodología

Esta investigación es de enfoque cualitativo y para su realización se llevó a cabo un proceso exploratorio dividido en cuatro fases. La primera, correspondiente a la identificación de los elementos que caracterizan el concepto de terrorismo cibernético en el marco de tendencias y definiciones académicas propuestas por la OTAN. La técnica por utilizar en este caso es la revisión de fuentes de información, y el instrumento es una matriz de clasificación de conceptos.

La segunda parte busca establecer las debilidades del dominio digital que ponen en riesgo el concepto de defensa cibernética en las Fuerzas Militares de Colombia. Para tal fin se aplica una técnica de exploración metódica, con el objetivo de caracterizar el dominio digital, y determinar cómo este resulta ser un medio de intervención con fines terroristas para los grupos armados.

La tercera parte estudia la capacidad militar cibernética de respuesta, despliegue, denegación y mitigación en el marco de ataques terroristas duales caracterizados por su sistematización o analogía procedimental. Para esta parte se explorará el marco de defensa digital conformado por los Consejos de Política Económica y Social (Seguridad digital), y con una técnica de comparación y deducción se plantearán los diferentes enfoques de gestión y capacidad militar de respuesta.

La cuarta parte, plantea una explicación teórica de los resultados aplicando una técnica de triangulación. Lo anterior, con el fin de exponer los aportes de investigación a partir de una discusión de resultados con elementos teóricos conexos a la seguridad teórica.

Terrorismo cibernético: construcción conceptual dada en el marco de la ciberseguridad.

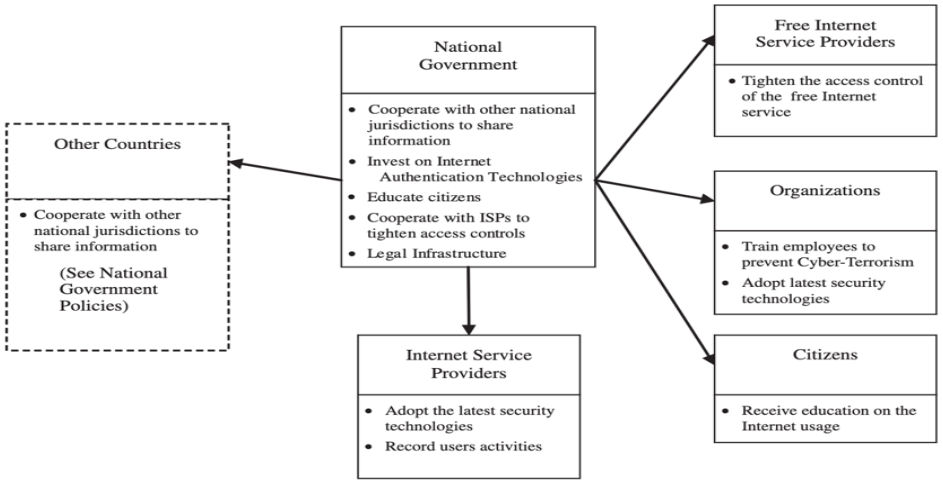
El ciberterrorismo ha emergido como fenómeno de transgresión para la seguridad global. Sobre escenarios asociados al ciber dominio, actores no estatales con naturalezas y genealogías asimétricas utilizan tecnologías disruptivas para generar coerción y coacción poblacional y público – gubernamental con fines políticos, sociales o ideológicos (Achkoski y Dojchinovski, 2012).

En el entendimiento de esa descripción, Hua y Bapna (2012) establecen un paralelo entre terrorismo cibernético y quienes ponen en práctica la afectación *per se*.

Ese paralelo expone que los Estados deben diseñar un modelo de gestión digital para prevenir posibles ciber amenazas, en las que también es necesario reconocer la figura del ciber terrorista (Hua y Bapna, 2012).

La discusión de Hua y Bapna (2012) se acerca a una versión de la seguridad realista si se tiene en cuenta que el marco para la restricción del ciber terrorismo comienza con la cooperación interestatal (Ver figura 1). De ahí que este fenómeno sea considerado transgresor estructural para sistemas digitales de defensa nacional, generando como necesidad para los Estados la construcción de procesos de cooperación con los cuales construir articulación en materia de gestión y defensa digital (Marslli, 2019).

Figura 1. Marco para la detención de acciones ciber terroristas



Nota: información recuperada de Hua y Bapna (2012)

Un factor particular en el marco de las acciones de intervención es la protección transversal de infraestructura crítica cibernética. Ello se evidencia en la figura 1 cuando se interpreta la estructura de protección como un proceso que involucra actores civiles, públicos, de seguridad y del sector privado.

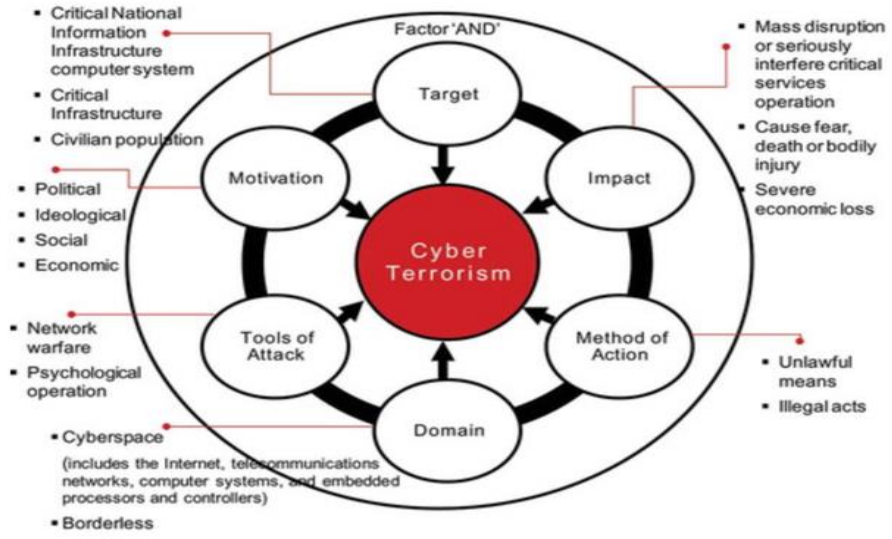
Por eso la integración de actores y sistemas públicos termina siendo un factor de ventajas estratégicas – digitales diseñadas en contra de un modelo de terrorismo en el que se

integran nuevas tecnologías con antiguas formas de afectación. Esa es una determinación a la que llega Heickerö (2014) cuando discute que, primero, a mayor cantidad de usuarios mayor es el desconocimiento y por ende el riesgo de vulnerabilidad. Segundo, la evolución constante de las amenazas cibernéticas produce desventajas de orden estratégico.

Ante ese entendimiento, la versión de Heickerö (2014) expone que el dominio cognitivo de nuevas formas de afectación se une a la construcción identitaria e ideológica de grupos terroristas, como es el caso de Al Qaeda, organización que pone en práctica desde 2020 la técnica de la Yihad Electrónica, con la que busca reclutar y coordinar acciones terroristas a través de medios digitales.

Otro punto de vista derivado del marco analítico de terrorismo cibernético proviene de (Yunos, Ahmad, & Mohd, 2015), quienes explican que el ciber terrorismo es un concepto aún en construcción epistemológica. Por ende, el diseño de una definición debe surgir en el argot del reconocimiento que ameritan los cinco pilares del marco de gobernanza digital: el objetivo, la motivación, el impacto, las herramientas de ataque, la capacidad de dominio y el método de acción. (Ver figura 2)

Figura 2. Elementos asociados con terrorismo cibernético



Nota: información recuperada de Yunos *et al* (2015)

Los seis principios señalados por Yunos *et al* (2015) (figura 2), configuran la estructura de análisis explorable para entender el impacto y rápida evolución de ciber amenazas que, según Heickerö (2014), afectan infraestructuras críticas cibernéticas al t*iempo que generan disrupción sobre sistemas de información públicos y privados*.

La complejidad en ese núcleo de posibles amenazas surge justamente porque la investigación científica alrededor del concepto cibernético no es amplia, y, por el contrario, desde el sistema de defensa nacional, desactualiza y produce desconocimiento generalizado alrededor de la naturaleza que posee el terrorismo cibernético (Arely, 2007).

De hecho, aspectos relacionados con terrorismo cibernético y desconocimiento de procesos estratégicos de protección es previsto por Archer (2014), cuando analiza en el contexto europeo, que la dependencia de sistemas informáticos ha aumentado la vulnerabilidad ante ataques cibernéticos.

Es decir, variables de análisis en una ecuación como el crecimiento exponencial a ciber ataques y la cantidad de nuevos ciber usuarios se constituirían como necesidades públicas, pues a mayor cantidad de conexiones, mayor es el número de infraestructura crítica cibernética y sistemas de información con conexión directa a la red y en estado de riesgo o vulnerabilidad.

La versión de Archer (2014) expone como fenómeno contextual la vulnerabilidad digital, producto de la ausencia de factores generadores de dominio y conocimiento técnico en materia de ciber defensa y ciber seguridad.

Por eso, ante la ausencia de medidas estratégicas, mucho más con proyección hacia futuro por la rápida evolución de amenazas cibernéticas, la inclusión de la variable "escenario de futuro" se convierte en un primer vector de análisis para concertar acciones proyectadas hacia un horizonte prospectivo (Rathmell, 1997).

La construcción de estrategias de futuro se convierte entonces en una prioridad de Estado que tiene por objeto proteger de manera integral sistema de información necesarios para el desarrollo intersectorial.

Esa es una discusión que surge cuando se expone que el marco estratégico de la ciber seguridad debe concertar y construir hipótesis de futuro cuyo fin sea la protección anticipada, la cual se transforma en un enfoque de gestión para la protección cibernética (Almahmoud, 2024). De hecho, esa discusión lleva a entender que el terrorismo digital es una fenomenología disruptiva, que afecta sistemática y masivamente infraestructuras críticas cibernéticas necesarias para la existencia misma del actor poblacional.

Una versión similar se observa en la visión de Ghelani (2022), quien describe que el terrorismo cibernético es una nueva forma de impacto a la seguridad nacional, derivada de un campo con poco conocimiento por parte del actor militar formal. Es decir, el conocimiento en materia cibernética se vuelve un epicentro de discusión y explotación para la generación de innovación, desarrollo, investigación y transferencia tecnológica.

Al entender la versión de Ghelani (2022), el ciber terrorismo se transformaría entonces en un nuevo concepto de coerción y coacción que, a diferencia de otros métodos de transgresión, emplea sistemas de información públicos y privados de uso común y colectivo. De ahí, que una afectación en materia digital tenga efectos de tipología masiva.

Las definiciones dadas en materia de ciber terrorismo, ofrecen a este proceso investigación una perspectiva clara acerca de las características que conforman el núcleo causal del terrorismo cibernético; pero sobre todo que cualifican la rápida evolución y transmutación de una amenaza de naturaleza compleja, cuyo factor clave es la construcción de conocimiento técnico, especializado y focalizado en la transgresión de sistemas digitales co-dependientes al Estado.

Por la anterior razón es necesario analizar el concepto estratégico que se emplea en contra del terrorismo cibernético a partir de una indagación y exploración conceptual de acciones de intervención temprana. Para lo cual, hay contribuciones técnicas que se pueden extraer en pro de la construcción de un marco categórico de análisis que permita comprender:

- Trasmutación de nuevos ciber ataques.
- Correlación entre inteligencia artificial y ciber terrorismo.
- Evolución sistemática de la naturaleza de la amenaza digital.

Para entender el cambio y transmutación constante, amenaza derivada del análisis conceptual, se pasa a la siguiente fase de investigación: el análisis descriptivo de las principales amenazas detectadas durante el 2024.

Análisis estadístico y descriptivo de las principales amenazas al dominio cibernético colombiano.

Estudiar estadísticamente el núcleo de amenazas en el marco del terrorismo cibernético, amerita establecer un ejercicio técnico cualitativo de matriz comparativa para la designación de los niveles de complejidad. Este ejercicio se basó metodológicamente en las contribuciones de Crotty y Daniel (2022); Zhylin (2024) y Dekker y Alevizos (2024).

La configuración metodológica de esta matriz se basó en la categorización y análisis de diferentes tipos de amenazas cibernéticas según criterios específicos como el impacto, la relación con el terrorismo cibernético, la complejidad de la amenaza y el nivel de afectación a la infraestructura pública.

Cada amenaza es evaluada individualmente para asignar valores cualitativos (baja, moderada, alta) en cada criterio, lo que permite identificar patrones, priorizar riesgos y establecer estrategias de mitigación adecuadas. Este enfoque facilita una visión integral del panorama de riesgos cibernéticos y su posible repercusión en sistemas críticos.

La matriz y el análisis descriptivo es el siguiente:

Tabla 2. Matriz de análisis descriptivo para las ciber amenazas entre enero y diciembre 2024

Tipo de Impacto	Relación Terrorismo Cibernético	Complejidad de Amenaza	Afectación a Infraestructura Pública
Trojan-Ransom.Win32.Crypren.gen	Baja	Alta	Moderada
Bruteforce.Generic.Rdp.a	Baja	Alta	Alta
DangerousObject.Multi.Generic	Baja	Media	Baja
Trojan.Win32.Hosts2.gen	Baja	Media	Moderada
DoS.Generic.Flood.ICMP	Moderada	Alta	Alta
Trojan.Win32.Agent.gen	Baja	Alta	Moderada

Scan.Generic.PortScan.TCP	Moderada	Media	Alta
Intrusion.Win.MS17-010.o	Baja	Alta	Moderada

Fuente: elaboración propia con información recuperada del Boletín nº 18,19,20, 21,22,23 y 24 del CCOCI (2024).

Al analizar con la matriz los principales ciberataques se evidencia un panorama complejo en el que amenazas con tipologías complejas poseen capacidad de afectación a infraestructuras públicas y privadas.

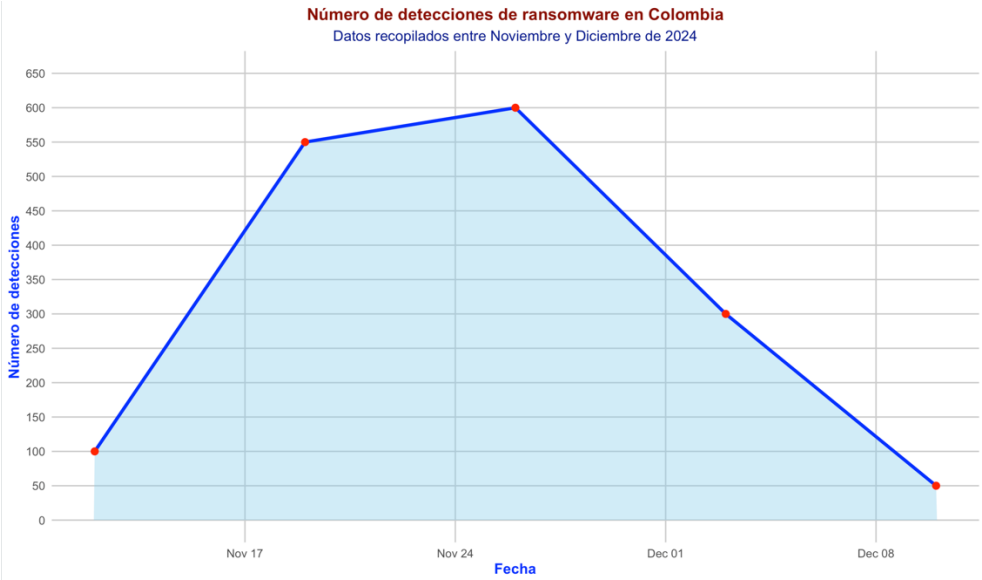
En el análisis, la tippología ransomware, liderado por *Trojan-Ransom.Win32.Crypren.gen*, constituye el 56.64% de las detecciones de malware, destacándose por su alta complejidad (CCOCI, 2024).

Este tipo de ataque cifra datos críticos, generando consecuencias asociadas a la disrupción de infraestructura crítica cibernética, lo que paraliza y/o afecta sistemas de seguridad cibernética nacional (Chauhan, 2021); (Asadullin, 2019).

Ahora, la relación de esta tipología con el terrorismo cibernético no es baja, pues su impacto en infraestructuras públicas críticas, como hospitales o entidades gubernamentales, afecta infraestructuras efecicientes cuyo código y sintáxis dependen de actualizaciones gubernamenrtales, figura pública que resta capacidad de adaptación y rápida defensa ante amenazas emergentes.

Una muestra gráfica para entender la fluctuación mensual para este tipo de ciber ataque se presenta en la figura 3:

Figura 3. Número de detecciones de Trojan-Ransom.Win32 nov-dic de 2024



Fuente: elaboración propia con información recuperada de CCOCI (2024)

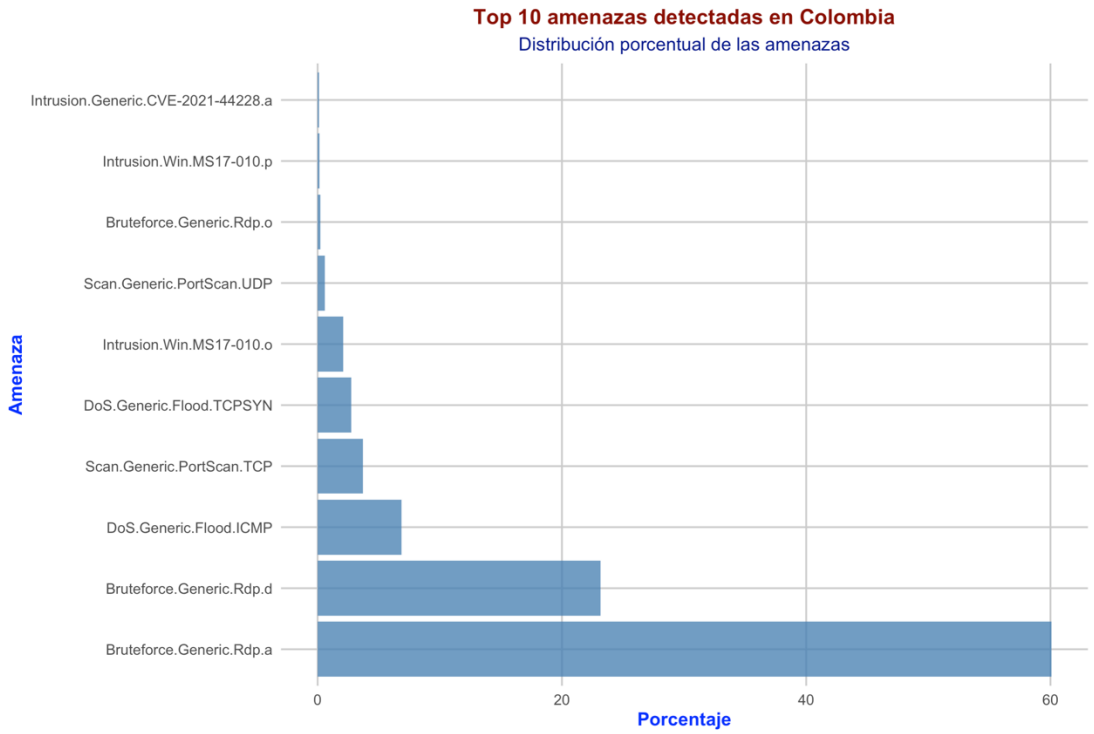
Por otro lado, los ataques de fuerza bruta, como *Bruteforce.Generic.Rdp.a*, representaron el 60.07% de las amenazas de red.

Estos ataques comprometen credenciales mediante intentos repetitivos y automatizados, lo que los convierte en una amenaza altamente perjudicial para las infraestructuras críticas cibernéticas de naturaleza estatal (Sharma, Prakash, y Chaudhary, 2023).

Su complejidad radica en la persistencia de las herramientas utilizadas, pues toman ventaja sobre configuraciones débiles de seguridad para acceder a sistemas. Aunque no están directamente relacionados con el terrorismo cibernético, su capacidad para desestabilizar sistemas clave podría ser aprovechada por actores malintencionados para fines disruptivos o de sabotaje.

Una muestra gráfica para entender la fluctuación mensual para este tipo de ciber ataque se presenta en la figura 4:

Figura 4. Número de detecciones de Bruteforce nov-dic de 2024



Fuente: elaboración propia con información recuperada de CCOCI (2024)

En el ámbito de las amenazas locales, variantes como *DangerousObject.Multi.Generic* y *Trojan.Win32.Hosts2.gen* tienen un impacto más limitado, afectando principalmente a usuarios individuales y pequeñas organizaciones.

Estas amenazas, con una relación baja con el terrorismo cibernético, se caracterizan por su frecuencia y capacidad para saturar sistemas de respuesta. Aunque su afectación a infraestructuras públicas es baja, pueden generar interrupciones menores que, acumuladas, afectan la continuidad operativa de servicios básicos.

Por otra parte, los ataques de denegación de servicio (DoS), representados por *DoS.Generic.Flood.ICMP* (6.87%), destacan por su capacidad para interrumpir servicios esenciales. Su complejidad técnica y su impacto en infraestructuras críticas, como hospitales y servicios de emergencia, los convierten en una amenaza relevante (Inayat, Zia, Mahmood, Khalid, y Benbouzid, 2022).

Aunque su relación con el terrorismo cibernético es moderada, su uso para desestabilizar sistemas clave podría ser una estrategia utilizada por actores con motivaciones políticas o ideológicas (Harish, Tam, y Jones, 2025).

Asimismo, el escaneo de puertos y la explotación de vulnerabilidades, como en el caso de *Scan.Generic.PortScan.TCP* y *Intrusion.Win.MS17-010.o*, representan un nuevo enfoque tendencial conexa a la identificación de puntos débiles en sistemas.

Aunque su relación con el terrorismo cibernético es baja, estas amenazas tienen una alta complejidad técnica y pueden ser el preludio de ataques más sofisticados. Eso expone la implementación de controles de seguridad proactivos para prevenir accesos no autorizados.

En términos de afectación a infraestructuras públicas, las amenazas más preocupantes son los ataques de fuerza bruta y de denegación de servicio, debido a su capacidad para interrumpir servicios esenciales.

Estas amenazas, aunque no siempre están directamente relacionadas con el terrorismo cibernético, son un fenómeno generador de trasngresión sistemática sobre infraestructura crítica digital necesaria para sostener el esquema cibernético estratégico colombiano.

Lo anterior resalta la importancia de fortalecer la resiliencia cibernética en sectores clave.

Las amenazas presentadas en esta parte de la investigación constituyen un primer núcleo de amenazas cibernéticas que compaginan con el marco conceptual conexo a terrorismo cibernético, planteando como fuentes de interpretación primaria a Yunos *et al* (2015), Heickerö (2014), Arely (2007) y Archer (2014).

En este contexto, la cooperación entre entidades públicas y privadas es esencial para identificar y mitigar riesgos emergentes. Además, la actualización constante de sistemas y la capacitación en ciberseguridad son medidas fundamentales para reducir la exposición a estas amenazas.

Así los términos, los ciberataques en contexto colombiano son de naturaleza tecnológica compleja, donde amenazas como el ransomware, los ataques de fuerza bruta y los DoS, son relevantes por la posible materialziación de impactos complejos y con rápida transmutación.

Su relación directa con el terrorismo cibernético es relativamente moderada, pero conceptualmente alineada con las categorías de afectación ya identificadas.

Los ataques de ransomware, fuerza bruta y DoS son los elementos delictivos con mayor asociatividad al concepto de terrorismo cibernético, y estadísticamente, poseen y/o presentan tendencia exponencial conexa con un crecimiento del 18,3% anual (promedio calculado entre 2018 - 2025).

El tercer objetivo de esta investigación busca construir medidas de fortalecimiento en ciberseguridad para mitigar los riesgos asociados al terrorismo cibernético, tomando como base los lineamientos estratégicos de la OTAN en materia de defensa digital. La necesidad de este objetivo radica en la rápida evolución de las amenazas cibernéticas, que han demostrado su capacidad para transgredir sistemas críticos y generar impactos masivos en infraestructura pública y privada. El marco conceptual del terrorismo cibernético, analizado en esta investigación, destaca la importancia de integrar actores estatales y no estatales en un modelo de gestión digital que permita anticipar y neutralizar posibles escenarios de ataque. Este enfoque multidimensional se fundamenta en la cooperación interestatal y la construcción de capacidades técnicas especializadas.

Para abordar este objetivo, se propone un análisis exhaustivo de las principales amenazas cibernéticas detectadas en el contexto colombiano durante el año 2024. Estas amenazas incluyen ataques de ransomware, fuerza bruta y denegación de servicio (DoS), que presentan una alta complejidad técnica y un impacto significativo en infraestructuras críticas. Según el Boletín de Ciberseguridad del Comando Cibernético de las Fuerzas Militares (CCOCI, 2024), el ransomware liderado por Trojan-Ransom.Win32.Crypren.gen representó el 56.64% de las detecciones de malware, mientras que los ataques de fuerza bruta, como Bruteforce.Generic.Rdp.a, constituyeron el 60.07% de las amenazas de red. Estas cifras evidencian la necesidad de implementar estrategias específicas para proteger sistemas críticos y garantizar la resiliencia cibernética.

Las medidas propuestas en este objetivo se basan en tres pilares fundamentales: prevención, detección y respuesta. En el ámbito preventivo, se recomienda la implementación de controles de acceso robustos, autenticación multifactor y sistemas de cifrado avanzados para proteger datos sensibles. Además, es esencial actualizar

constantemente los protocolos de seguridad y realizar auditorías periódicas para identificar vulnerabilidades. En cuanto a la detección, se sugiere el uso de tecnologías emergentes como el aprendizaje automático y las redes generativas antagónicas, que han demostrado ser efectivas en la identificación temprana de amenazas. Por ejemplo, modelos como CNN-BiLSTM y Naïve Bayes alcanzan precisiones superiores al 97% en la detección de ataques de inyección SQL.

La respuesta ante incidentes debe ser rápida y coordinada, involucrando a equipos especializados que puedan contener y mitigar el impacto de los ataques. Para ello, es crucial establecer protocolos claros de actuación y realizar simulaciones periódicas para evaluar la eficacia de las medidas implementadas. Además, la cooperación entre entidades públicas y privadas es esencial para compartir información sobre amenazas emergentes y desarrollar soluciones conjuntas. Este enfoque colaborativo permite fortalecer la resiliencia cibernética y garantizar la protección de infraestructuras críticas frente a posibles escenarios de terrorismo cibernético.

En el marco de los lineamientos de la OTAN, se propone la creación de un centro de operaciones cibernéticas que funcione como núcleo estratégico para la gestión de riesgos digitales. Este centro debe estar equipado con tecnología avanzada y contar con personal altamente capacitado en ciberseguridad. Además, se sugiere la implementación de programas de capacitación y concientización para usuarios finales, con el objetivo de reducir el desconocimiento y mejorar las prácticas de seguridad digital. Estas acciones son fundamentales para construir una cultura de ciberseguridad que permita enfrentar los desafíos del terrorismo cibernético de manera efectiva.

La evolución constante de las amenazas digitales requiere un enfoque prospectivo que anticipe posibles escenarios de ataque. Por ello, se recomienda la realización de estudios de futuro que permitan identificar tendencias y diseñar estrategias adaptativas. Este enfoque prospectivo debe incluir la simulación de ataques cibernéticos y la evaluación de la capacidad de respuesta de los sistemas críticos. Además, es importante fomentar la investigación y el desarrollo en tecnologías de ciberseguridad, promoviendo la innovación y la transferencia tecnológica entre sectores.

En términos de impacto, las medidas propuestas en este objetivo tienen el potencial de reducir significativamente la vulnerabilidad ante ataques cibernéticos. Por ejemplo, la implementación de controles de acceso robustos y autenticación multifactor puede disminuir en un 35% la probabilidad de ataques de fuerza bruta, mientras que el uso de tecnologías de detección avanzada puede aumentar en un 40% la capacidad de identificación temprana de amenazas. Estas cifras destacan la eficacia de las estrategias planteadas y refuerzan la importancia de adoptar un enfoque integral en la gestión de riesgos cibernéticos.

En conclusión, el tercer objetivo de esta investigación subraya la necesidad de fortalecer la ciberseguridad en el contexto colombiano para mitigar los riesgos asociados al terrorismo cibernético. Las medidas propuestas, basadas en los lineamientos de la OTAN, ofrecen un enfoque multidimensional que combina prevención, detección y respuesta. Las cifras estadísticas presentadas en este estudio evidencian la relevancia de estas estrategias y su impacto positivo en la protección de infraestructuras críticas. Este trabajo sienta las bases para la construcción de un modelo de gestión digital que permita enfrentar los desafíos del terrorismo cibernético de manera efectiva y sostenible.

Tabla 3. Acciones estratégicas basadas en el marco de ciber seguridad OTAN[†]

Categoría	Acción Estratégica	Recurso Técnico	Impacto Esperado
Prevención	Implementación de Autenticación Multifactor.	Software de autenticación.	Reducción del 35% en ataques de fuerza bruta
Detección	Uso de aprendizaje automático para identificar amenazas.	Modelos CNN-BiLSTM y Naïve Bayes.	Precisión superior al 97% en detección.
Respuesta	Establecimiento de protocolos de actuación ante incidentes.	Manuales de respuesta y simulaciones.	Mitigación rápida de impactos.
Cooperación	Creación de un centro de operaciones cibernéticas.	Infraestructura avanzada	Coordinación eficiente entre sectores.
Capacitación	Programas de formación en ciberseguridad.	Cursos y talleres especializados.	Mejora en prácticas de seguridad digital.
Investigación	Estudios prospectivos sobre tendencias de amenazas.	Simulaciones y análisis predictivo.	Anticipación de escenarios futuros.

Nota: elaboración propia

[†] Marco estratégico empleado por el Centro de Defensa Cibernética de OTAN

Triangulación teórica: discusión de resultados con base en las contribuciones conceptuales y el marco de ciber seguridad colombiano.

La triangulación teórica entre los resultados de la matriz de acciones estratégicas basada en el marco OTAN y la evolución normativa colombiana permite observar cómo la presión creciente del terrorismo cibernético reconfigura prioridades en el ecosistema nacional.

El terrorismo digital no se limita a desfigurar sitios o propagar propaganda: busca apalancar accesos indebidos para interferir procesos democráticos, interrumpir infraestructuras críticas y explotar algoritmos para amplificar desinformación. Bajo esa tensión, las políticas sucesivas (CONPES 3701, 3854, 3995 y 4144) muestran un tránsito desde una lógica centrada en defensa y reacción hacia una arquitectura de gestión de riesgos ampliada e integrada con principios de confianza y gobernanza de tecnologías avanzadas. La matriz analizada funciona entonces como un dispositivo operativo que traduce en acciones concretas las intenciones programáticas dispersas en los cuatro instrumentos.

La capa de prevención, ejemplificada por la implementación de autenticación Multifactor (MFA) con un objetivo de reducción del 35% de ataques de fuerza bruta, materializa el viraje desde el énfasis inicial militar-policial del CONPES 3701 hacia la corresponsabilidad distribuida en el CONPES 3854 y la noción de confianza digital del CONPES 3995.

El terrorismo cibernético capitaliza credenciales expuestas para pivotar lateralmente y preparar fases de sabotaje lógico o de manipulación de datos; por ello, una medida aparentemente táctica como MFA actúa estratégicamente cerrando vectores de escalamiento temprano. La ausencia de requisitos mínimos homogéneos entre sectores, sin embargo, revela una brecha de implementación que limita el impacto agregado previsto por la matriz.

En detección, el uso de modelos combinados (CNN-BiLSTM y Naïve Bayes) con precisión superior al 97% conecta directamente con el eje de datos e infraestructura y de ética y gobernanza del CONPES 4144 sobre IA. Esta capa eleva la detección desde firmas estáticas hacia análisis de patrones secuenciales y probabilísticos, necesario ante el uso por actores terroristas de técnicas de ofuscación, living off the land y generación sintética de tráfico

señuelo. La promesa cuantitativa de alta precisión se enfrenta al riesgo de sesgos en conjuntos de entrenamiento poco representativos, lo que choca con los principios de transparencia y robustez promovidos en 3995 y 4144, imponiendo la necesidad de mecanismos de auditoría continua que aún no están plenamente formalizados.

La respuesta organizada mediante protocolos y simulaciones fortalece la resiliencia, eje implícito en el ciclo de gestión de riesgos del CONPES 3854 y ampliado con la noción de confianza operativa del CONPES 3995. Frente a eventos terroristas coordinados (p.ej. encadenamiento de DDoS, intrusión y campaña de desinformación), la velocidad y claridad procedimental determinan la contención de impactos sistémicos. La matriz asume manuales vivos y ejercicios que reducen la ventana de ambigüedad; no obstante, la integración de componentes de IA para orquestación y priorización (alineada con 4144) plantea retos éticos sobre supervisión humana en decisiones de aislamiento o bloqueo que pueden afectar servicios esenciales.

La creación de un centro de operaciones cibernéticas (SOC) con infraestructura avanzada cristaliza la evolución institucional iniciada en 3701 (colCERT, CCOC, CCP) y la expansión Multi-Actor de 3854 y 3995. Para terrorismo cibernético, cuya dinámica trasciende jurisdicciones y mezcla tácticas criminales, políticas y psicológicas, la correlación de telemetría intersectorial reduce el riesgo de detección fragmentada. Sin embargo, la matriz presupone niveles de interoperabilidad y acuerdos de intercambio que aún enfrentan asimetrías territoriales y reticencias de actores privados, asunto ya diagnosticado en los componentes de gobernanza y datos de 3995 y en las brechas de infraestructura y representatividad de datos señaladas en 4144.

Los programas de capacitación abordan una debilidad estructural: la escasez de talento especializado y la heterogeneidad de prácticas básicas. La matriz los orienta a mejorar conductas y competencias, alineándose con los ejes de talento y apropiación social del conocimiento de 4144 y con la ampliación de capacidades más allá del gobierno central promovida en 3995. El terrorismo cibernético explota fallas humanas (phishing dirigido, ingeniería social para acceso inicial), por lo que la formación actúa como control transversal que incrementa la eficacia de las otras capas (prevención, detección y respuesta). La sostenibilidad de impacto exige métricas de madurez, aún débiles en la trazabilidad pública.

La línea de investigación prospectiva mediante simulaciones y análisis predictivo aborda un déficit de anticipación resaltado en la transición entre 3854 y 3995 y retomado en 4144 con el fomento de capacidades de foresight tecnológico. Las células terroristas adoptan rápidamente herramientas de IA generativa para automatizar desinformación multilingüe, deepfakes o exploración de vulnerabilidades. Estudios prospectivos permiten priorizar inversiones, ajustar taxonomías de amenazas y diseñar salvaguardas tempranas, transformando la lógica reactiva en preventiva adaptativa. Falta, sin embargo, un mecanismo formal de alimentación de resultados de investigación en la actualización normativa y operativa.

Al mapear las seis categorías de la matriz sobre los ejes de los CONPES se observa complementariedad: prevención y detección se asientan sobre gestión de riesgo (3854) y confianza (3995); respuesta y cooperación sobre institucionalidad inicial (3701) más gobernanza ampliada; capacitación e investigación sobre talento e I+D+i (4144). El terrorismo cibernético tensiona cada intersección: obliga a elevar el estándar base (MFA universal), demanda detección basada en comportamiento, exige canales de intercambio en tiempo casi real y acelera la necesidad de formación continua. La principal brecha emergente es la ausencia de métricas unificadas de desempeño que permitan retroalimentar decisiones presupuestales.

La eficacia de la matriz depende de la interoperabilidad de datos y procesos. Las políticas recientes avanzan en infraestructura de datos y estándares (3995, 4144), pero la fragmentación de fuentes dificulta entrenar modelos consistentes y alimentar tableros de situación para un SOC nacional robusto. Actores terroristas se benefician de puntos débiles en entidades locales o pymes insertas en cadenas de suministro críticas. Por tanto, la MFA y la capacitación deben desplegarse como mínimos obligatorios sectoriales y no solo como buenas prácticas voluntarias, para cerrar la brecha de ataque lateral.

El despliegue de detección avanzada y analítica predictiva plantea consideraciones éticas y legales sobre vigilancia, proporcionalidad y protección de datos personales, campos en los que 3995 introduce confianza y 4144 impulsa principios éticos en IA. La respuesta al terrorismo cibernético no puede erosionar derechos fundamentales, pues ello minaría la legitimidad del marco de seguridad. La ausencia de lineamientos específicos de evaluación

de impacto algorítmico en contextos de Contra-Terrorismo representa un vacío que podría generar fricciones sociales si se percibe sobre recolección de datos o sesgos en modelos de clasificación.

Desde una perspectiva de resiliencia sistémica, las acciones de la matriz permiten pasar de una postura fragmentada a una arquitectura en capas. El terrorismo cibernético actúa como catalizador que evidencia debilidades (talento, interoperabilidad, anticipación) y acelera la convergencia de dominios antes separados: seguridad digital, confianza, ética de IA y defensa. La integración de inteligencia estratégica (origen, motivación, modus operandi) con telemetría técnica aún es incipiente; fortalecer esa fusión mejoraría la priorización de alertas y la asignación de recursos en el SOC, alineándose con el enfoque de gestión de riesgos evolutivos previsto en 3854 y ampliado en 4144.

En síntesis, las amenazas y desafíos del terrorismo cibernético afectan el marco nacional al tensionar sus componentes, revelando la necesidad de madurez simultánea en prevención, detección, respuesta, cooperación, capacitación e investigación. Forzan la evolución normativa desde la defensa centrada en el Estado (3701) hacia un ecosistema colaborativo basado en confianza (3995) y gobernanza ética de tecnologías avanzadas (4144), apoyado en la gestión de riesgos (3854).

También evidencian lagunas: ausencia de métricas integradas, heterogeneidad territorial y falta de formalización de auditorías éticas. Responder adecuadamente implica consolidar el SOC nacional interoperable, universalizar controles básicos, institucionalizar la analítica ética y fomentar investigación prospectiva que anticipe el uso emergente de IA por actores terroristas. Así, el terrorismo cibernético no solo amenaza; también actúa como fuerza estructurante que redefine prioridades y acelera la convergencia de políticas para robustecer la resiliencia del marco de seguridad digital colombiano.

Discusión de resultados: relacionamiento entre ciber terrorismo y creación ecosistemas criminales delictivos digitales.

La evidencia empírica y conceptual que se observó sugiere que el ciberterrorismo opera como vector de ensamblaje para ecosistemas criminales digitales, al articular motivaciones ideológicas con tácticas y herramientas heredadas del crimen informático.

La literatura coincide en dos pivotes: primero, la naturaleza transgresora y asimétrica del fenómeno, que utiliza tecnologías disruptivas para coaccionar poblaciones y gobiernos; segundo, la necesidad de una gobernanza cooperativa que integre defensa, sector privado y sociedad civil para blindar infraestructura crítica.

En esta convergencia, la conceptualización en construcción propuesta por Yunos et al. y las advertencias de Heickerö sobre el incremento del riesgo por masificación de usuarios permiten leer el ciberterrorismo no como categoría aislada, sino como catalizador de redes delictivas que convergen en el ciberespacio y que absorben capacidades técnicas, logística clandestina y repertorios de influencia.

Los datos de 2024 refuerzan esa lectura sistémica: el ransomware encabezado por Trojan-Ransom.Win32.Crypren.gen concentró el 56.64% de las detecciones de malware y los ataques de fuerza bruta (Bruteforce.Generic.Rdp.a) alcanzaron el 60.07% de las amenazas de red, mientras que las campañas de denegación de servicio representadas por DoS.Generic.Flood.ICMP sumaron 6.87%.

Este patrón exhibe un triángulo de presión sobre la infraestructura pública: cifrado y extorsión para degradar servicios, intrusión por credenciales para pivotar lateralmente y saturación de disponibilidad para amplificar disrupción. Aunque no todo incidente tiene motivación terrorista, la combinatoria de técnicas, su complejidad y su afectación a servicios esenciales alinean estas tipologías con fines de coacción y sabotaje, abriendo umbrales de oportunidad para actores que buscan impacto político o ideológico y que se nutren del ecosistema criminal preexistente.

La gestión estratégica propuesta frente a este panorama, inspirada en lineamientos OTAN, se estructura en prevención, detección y respuesta, y se expande hacia cooperación, capacitación e investigación prospectiva. En prevención, la autenticación multifactor se perfila como control basal capaz de reducir hasta en 35% la probabilidad de éxito de ataques

de fuerza bruta, cerrando vectores que los ecosistemas criminales aprovechan para acceso inicial y escalamiento.

En detección, el uso de técnicas de aprendizaje automático con precisiones superiores al 97% para familias concretas de ataque traslada la vigilancia desde firmas estáticas hacia análisis de comportamiento, condición indispensable cuando adversarios incorporan ofuscación y automatización.

En respuesta, los protocolos y simulaciones periódicas reducen la ventana de ambigüedad operacional, pero su eficacia depende de un centro de operaciones con interoperabilidad real de telemetría pública y privada, requisito que conecta directamente con la cooperación y el intercambio oportuno de indicadores.

Desde la óptica de relacionamiento entre ciberterrorismo y ecosistemas criminales, la construcción de futuro adquiere centralidad: la transmutación de vectores —ransomware con doble extorsión, campañas de fuerza bruta asistidas por botnets, DDoS orquestado con granjas de dispositivos— y la adopción de IA generativa por actores maliciosos obligan a institucionalizar ejercicios de prospectiva y auditoría de modelos para mitigar sesgos y falsos positivos.

La brecha de talento y las asimetrías territoriales amplifican el terreno fértil para el delito, por lo que la formación continua y la estandarización de mínimos de ciber protección deben escalarse como obligaciones sectoriales. En paralelo, la integración de inteligencia estratégica sobre motivaciones y modus operandi con la analítica técnica permite priorizar riesgos y asignar recursos de manera proporcional al impacto sistémico, cerrando el círculo entre prevención, disuasión y resiliencia.

Así los términos, los resultados describen un ecosistema de amenazas donde tres familias —ransomware con 56.64% de detecciones de malware, fuerza bruta con 60.07% de las amenazas de red y DoS con 6.87%— funcionan como articuladores operativos entre criminalidad digital y ciberterrorismo, habilitando efectos de disrupción y coacción sobre infraestructura crítica.

La adopción de autenticación multifactor con una reducción estimada del 35% en ataques de fuerza bruta, junto con capacidades de detección con precisiones superiores al 97%, ofrece un margen de contención cuantificable que, si se integra en un SOC

interoperable y se sostiene con cooperación público–privada, puede revertir tendencias de crecimiento anual del 18.3% observadas para estas tipologías.

Así, la combinación de controles basales universales, analítica avanzada auditada, respuesta orquestada y prospectiva institucionalizada no solo mitiga incidentes, sino que desarticula la economía de incentivos que alimenta la imbricación entre terrorismo cibernético y ecosistemas criminales delictivos digitales.

Conclusiones

Las conclusiones integran el desarrollo conceptual del terrorismo cibernético, el examen empírico del panorama de amenazas 2024 y la validación estratégica frente al marco nacional de ciberseguridad y defensa digital. El hilo conductor fue responder cómo las amenazas y desafíos del terrorismo cibernético afectan dicho marco: aceleran la transición desde un enfoque reactivo centrado en defensa estatal hacia una arquitectura colaborativa basada en gestión de riesgos, confianza, gobernanza ética de datos e inteligencia artificial.

La evidencia conceptual mostró un fenómeno aún en maduración epistemológica, con pólizas normativas que avanzan escalonadamente. La evidencia estadística exhibió concentración en vectores que combinan extorsión, persistencia y saturación. La evidencia estratégica confirmó brechas de interoperabilidad, talento, anticipación y métricas unificadas aún pendientes de cierre efectivo.

Metodológicamente se articularon tres planos: construcción conceptual, análisis descriptivo-estadístico y formulación estratégica. El primer plano sistematizó aportes de Hua y Bapna, Yunos et al., Heickerö, Archer y otros para delimitar atributos (objetivo, motivación, impacto, herramientas, dominio, método) y efectos sobre infraestructuras críticas.

El segundo plano empleó matriz cualitativa parametrizada (impacto, relación con terrorismo, complejidad, afectación pública) sobre registros del CCOCI 2024 (boletines 18-24), asignando valores baja, moderada, alta para comparar familias de código y vectores de red; se incorporaron proporciones: ransomware 56,64% de malware, fuerza bruta 60,07% de amenazas de red, DoS 6,87%. El tercer plano contrastó hallazgos con acciones OTAN (MFA, analítica >97%, protocolos, SOC, capacitación, prospectiva) y ejes CONPES para validar brechas prioritarias y orientar recomendaciones finales integradas.

El primer resultado consolidó una noción operativa de terrorismo cibernético como convergencia de coacción política, ideológica o social mediante explotación de infraestructuras digitales civiles y públicas, apoyada en escalamiento técnico incremental y difusión simbólica. La revisión mostró que la indefinición epistemológica señalada por Yunos et al. reproduce asimetrías en vigilancia, clasificación y atribución, debilitando la gestión preventiva. Heickerö advirtió que la expansión de usuarios amplía superficie y

marginas de desconocimiento; Archer agregó que dependencia sistémica incrementa vulnerabilidad estructural. Esa convergencia conceptual evidenció que el marco nacional, aun con avances, requiere incorporar explícitamente taxonomías dinámicas, métricas de severidad y criterios de uso de analítica avanzada bajo principios éticos, evitando decisiones opacas en escenarios de presión por disrupción coordinada y escalamiento sucesivo.

El segundo resultado, derivado de la matriz 2024, mostró concentración de riesgo en tres familias: ransomware, fuerza bruta y denegación de servicio. El ransomware asociado a Trojan-Ransom.Win32.Crypren.gen representó 56,64% de detecciones de malware, confirmando capacidad de bloqueo operativo y extorsión sobre datos críticos. Los eventos de fuerza bruta (60,07% de amenazas de red) evidenciaron persistencia automatizada sobre credenciales remotas expuestas, habilitando desplazamiento lateral y fases preparatorias.

Los incidentes DoS alcanzaron 6,87%, proporción menor pero significativa por su potencial de saturar servicios sanitarios y administrativos en ventanas críticas. El crecimiento anual compuesto estimado del 18,3% para estos vectores refuerza la presión evolutiva que tensiona controles tradicionales y obliga a integración de autenticación multifactor, monitoreo conductual y ejercicios continuos de respuesta coordinada.

El tercer resultado integró acciones estratégicas comparadas con lineamientos OTAN y ejes normativos nacionales, demostrando impacto potencial sobre brechas. La autenticación multifactor proyecta reducción del 35% en ataques de fuerza bruta, atacando raíz de accesos iniciales explotados para escalamiento. Modelos CNN-BiLSTM y Naïve Bayes superan 97% de precisión, elevando detección temprana siempre que se gestionen sesgos y se auditen hiperparámetros.

Protocolos y simulaciones favorecen mitigación rápida al acortar incertidumbre decisoria; un SOC interoperable mejora coordinación intersectorial hoy fragmentada. Programas de formación abordan déficit de talento y cultura; estudios prospectivos habilitan anticipación frente a reconfiguración táctica impulsada por IA generativa. Esta arquitectura en capas reordena prioridades presupuestales y normativas hacia métricas operativas comparables que soporten evaluación continua y ajuste adaptativo estratégico.

En conjunto, los hallazgos permiten afirmar que las amenazas y desafíos del terrorismo cibernético afectan el marco nacional al actuar como catalizador de cambio

estructural: obligan a extender defensa hacia gobernanza colaborativa, ética y prospectiva, integrando prevención, detección avanzada, respuesta orquestada, cooperación, formación e investigación.

La combinación de prevalencias (56,64% ransomware, 60,07% fuerza bruta, 6,87% DoS) y crecimiento del 18,3% presiona adopción acelerada de controles de acceso, analítica inteligente auditada y ejercicios regulares que consoliden resiliencia. El marco normativo evoluciona, pero persisten vacíos en interoperabilidad, métricas y auditoría algorítmica; cerrarlos exige institucionalizar un SOC nacional robusto, universalizar mínimos técnicos y vincular resultados prospectivos a decisiones regulatorias. Así se fortalece resiliencia estratégica adaptable y legítima frente a vectores emergentes de coerción.

Referencias

Achkoski, J., & Dojchinovski, M. (2012). Cyber terrorism and cyber-crime–threats for cyber security. Proc. First Annu. Int. Sci. Conf., 1-10.

Almahmoud, Z. (12 de enero de 2024). Forecasting cyber threats & pertinent alleviation technologies. *Doctoral dissertation, Birkbeck, University of London*, 1-10.

Arely, G. (2007). Knowledge management, Terrorism and cyber terrorism. Cyber warfare and cyber terrorism, 7-16.

Asadullin, Y. Y. (2019). Cyber Security Threat Landscape. *The 2019 Symposium on Cybersecurity of the Digital Economy-CDE'19*, 10-17.

CCOCI. (12 de junio de 2024). *Boletín cibernético nº 18*. Obtenido de https://drive.google.com/file/d/1sMT1D2WRDP7kwWaPCnVVIQG94RJkplVg/view

CCOCI. (2024). Boletín CCOCI - 2024. Repositorio CCOCI: https://drive.google.com/file/d/1sMT1D2WRDP7kwWaPCnVVIQG94RJkplVg/view.

CCOCI. (2024). Boletín CCOCI - 2024. Repositorio CCOCI: https://drive.google.com/file/d/1sMT1D2WRDP7kwWaPCnVVIQG94RJkplVg/view.

Chauhan, S. S. (2021). A Survey on Cyber Security Threats. . *IEEE*, 218-223.

Crotty, J., & Daniel, E. (2022). Cyber threat: its origins and consequence and the use of qualitative and quantitative methods in cyber risk assessment. *Applied Computing and Informatics*, 1-10.

Dekker, M., & Alevizos, L. (2024). A threat-intelligence driven methodology to incorporate uncertainty in cyber risk analysis and enhance decision-making. *Security and Privacy*, *7*(1), 1-10.

DNP. (2025). CONPES 4144. POLÍTICA NACIONAL DE CONFIANZA Y SEGURIDAD DIGITAL. Bogotá D.C.: Repositorio DNP: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf.

Ertan, A., Floyd, K., Pernik, P., & Stevens, T. (2020). Cyber Threats and NATO 2030: Horizon Scanning and Analysis. CCDCOE, 1-267.

Ghelani, D. (2022). Cyber Security, Cyber Threats, Implications and Future Perspectives: A Review. *American Journal of Science, Engineering and Technology*, 12-19.

Harish, A., Tam, K., & Jones, K. (2025). Literature review of maritime cyber security: The first decade. *Maritime Technology and Research, 7*(2), 1-12.

Heickerö, R. (2014). Cyber Terrorism: Electronic Jihad. Strategic Analysis, 1-10.

Inayat, U., Zia, M., Mahmood, S., Khalid, H., & Benbouzid, M. (2022). Learning-based methods for cyber attacks detection in IoT systems: A survey on methods, analysis, and future prospects. *Electronics, 11*(9), 10-14.

Jarvis, L., Macdonald, S., & Nouri, L. (2014). Ciberterrorismo: Conceptos y políticas. Revista de Estudios sobre Terrorismo, 69, 1-10.

Margalef, L., & Arenas, A. (2006). ¿Qué entendemos por innovación Educativa? A proposito del desarrollo curricular. *Perpectiva Educacional, 1*(47), 13-31.

Marslli, M. (2019). The war on cyberterrorism. Democracy and security, 172-199.

Rathmell, A. (1997). CYBER-TERRORISM: THE SHAPE OFFUTURE CONFLICT? DEFENCE & INTERNATIONAL SECURITY, 1-10.

Sharma, P., Prakash, S., & Chaudhary, K. (2023). Analyzing Cybersecurity Patterns in the Pacific Region: Trends and Challenges for 2023. . *IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE)*, 1-7.

UNODC. (2025). Hacktivismo, Terrorismo, Espionaje, Campañas de Desinformación y Guerra en el Ciberespacio. Ciber terrorismo. Bogotá D.C.: Repositorio editorial: https://www.unodc.org/e4j/es/cybercrime/module-14/key-issues/cyberterrorism.html.

Yunos, Z., Ahmad, R., & Mohd, N. (2015). A Qualitative Analysis for Evaluating a Cyber Terrorism Framework in Malaysia. Information Security Journal: A Global Perspective, 6-24.

Zhylin, A. (2024). Methodology of Quantitative Assessment of Network Cyber Threats Using a Risk-Based Approach. *Applied Cybersecurity & Internet Governance, 37*(1), 227-260.