ANÁLISIS SOBRE LA CIBERDELINCUENCIA

BOLETÍN

EN ESTA EDICIÓN

Terrorismo en la Red Riesgos para la Seguridad Nacional

DIRECCIÓN DE CIBERDELITOS
MINISTERIO DEL INTERIOR
2025

Boletín de Análisis: “Terrorismo en la Red Riesgos para la Seguridad Nacional”

Ministerio del Interior

Subsecretaría de Combate al Delito

Dirección de Ciberdelitos

Responsables y Colaboradores

Redacción técnica del documento:

INGENIERO DIEGO TEJADA CAMPOS, Analista de Ciberdelitos

MAGISTER GABRIEL REINOSO MARTÍNEZ, Analista de Ciberdelitos

MAGISTER CARLOS SIMBAÑA COBA, Analista de Ciberdelitos

INGENIERO CÉSAR TRELLES SEGOVIA, Analista de Ciberdelitos

SOCIÓLOGO PEDRO EMILIO MANOSALVAS PAREDES, Especialista Contra la Delincuencia Organizada Transnacional y Terrorismo

Revisión técnica del documento:

MAGISTER JORGE NÉJER GUERRERO, Especialista de Ciberdelitos

MAGISTER FERNANDO MOYA LEIMBERG, Especialista de Ciberdelitos

INGENIERO FREDDY GALLARDO SOSA, Especialista de Ciberdelitos

Redacción y compilación:

MAGISTER DUVAL MONTATIXE CAIZALUISA, Analista de Ciberdelitos

Contenido

PRESENTACIÓN

En un entorno donde la tecnología se ha integrado de manera profunda en la vida de las personas, resulta indispensable reconocer los desafíos que representa el fenómeno de la ciberdelincuencia.

En el marco de las competencias del Ministerio del Interior, a través de la Subsecretaría de Combate al Delito y la Dirección de Ciberdelitos, este documento ofrece una visión actualizada del panorama global, regional y nacional de la ciberdelincuencia, incorporando el análisis de modalidades de ataque, casos relevantes, perfilamiento de actores y cifras que permiten dimensionar el impacto de las conductas delictivas. Asimismo, examina las implicaciones sociales y políticas de estos fenómenos y revisa el marco normativo que sustenta la acción del Estado en su prevención y combate al delito.

Este boletín busca servir como una herramienta de referencia para las instituciones públicas, el sector privado, la academia y la sociedad civil, fortaleciendo las capacidades de detección, prevención y respuesta frente a las amenazas que enfrentamos en el entorno digital.

Jorge Fernando Illescas Peña

Director de Ciberdelitos del Ministerio del Interior

INTRODUCCIÓN

El ciberterrorismo es una de las principales amenazas a la seguridad a nivel mundial; las tecnologías de la información y la comunicación (TIC) son usadas para planificar, ejecutar o difundir actos con fines terroristas. Este acto delictivo combina las capacidades propias de la ciberdelincuencia, incluyendo el sabotaje digital, la propagación de malware o el acceso ilícito a sistemas informáticos con objetivos políticos, ideológicos o religiosos, esto incrementa su peligrosidad y su impacto en la estabilidad política, social y estatal.

En Ecuador el fenómeno del ciberterrorismo adquiere relevancia por el contexto de inseguridad que vive el país y por su creciente dependencia de infraestructuras críticas digitales, como servicios financieros, telecomunicaciones y plataformas gubernamentales. Los ataques dirigidos a sistemas estratégicos no solo buscan vulnerar la confidencialidad, integridad y disponibilidad de la información, sino también infundir miedo, desestabilizar instituciones y afectar la confianza ciudadana en el Estado.

Ecuador ha centrado sus esfuerzos en combatir la delincuencia organizada, el riesgo de que estos actores locales o internacionales usen tácticas de ciberterrorismo es una realidad latente. La importancia de fortalecer los marcos normativos, consolidar capacidades de ciberseguridad y fomentar la cooperación interinstitucional e internacional para prevenir, detectar y responder a este tipo de amenazas emergentes.

CIBERTERRORISMO: CONCEPTOS Y CARACTERÍSTICAS FUNDAMENTALES

El Ciberterrorismo: una amenaza que toca a la puerta de casa

Imagina que, en lugar de un ataque físico con bombas, un grupo extremista utiliza la tecnología para paralizar servicios esenciales de nuestro país, como la red eléctrica, el suministro de agua o los bancos. Esto es el Ciberterrorismo. Su objetivo es el mismo que el terrorismo tradicional: sembrar el miedo y desestabilizar a la sociedad, pero utiliza el ciberespacio como su campo de batalla. En Ecuador, esto representa una seria amenaza para la seguridad nacional, ya que puede afectar directamente nuestra vida diaria y nuestra capacidad como Estado para funcionar (ESPE, 2024) .

Cuando la tecnología se usa para la delincuencia: La Ciberdelincuencia Organizada

La ciberdelincuencia organizada es como la delincuencia común, pero en el mundo digital. No se trata de un ladrón solitario, sino de redes delincuenciales que actúan de forma coordinada, usando herramientas tecnológicas para cometer delitos con fines de lucro. Piensa en el robo de datos bancarios, el fraude a través de internet o el secuestro de información (ransomware) para pedir rescate. Su motivación es puramente económica, y sus víctimas somos todos: desde ciudadanos comunes hasta grandes empresas e instituciones (Infoem, 2020).

El espionaje de la era digital: Ciberespionaje

El Ciberespionaje es el arte de robar secretos, pero a través de la red. En lugar de agentes secretos con micrófonos ocultos, se utilizan hackers para infiltrarse en sistemas informáticos y robar información confidencial. Puede ser que un gobierno intente robar secretos militares de otro país, o que una empresa intente obtener la fórmula secreta de un competidor. El fin

es obtener una ventaja estratégica, comprometiendo la seguridad y la soberanía de una nación (Criollo, Flores, Flores, Santacruz, & Ron, 2023).

Guerra en el ciberespacio: La Ciberguerra

La ciberguerra no es una película de ciencia ficción, sino una realidad. Se refiere a los ataques en línea entre Estados, donde el objetivo es paralizar los sistemas informáticos del adversario. Esto puede incluir la interrupción de las comunicaciones, la deshabilitación de la infraestructura de transporte o incluso el sabotaje de sistemas militares. En Ecuador, nuestro gobierno considera el ciberespacio como un territorio más que debe ser defendido, por lo que la ciberguerra es una amenaza directa a nuestra soberanía (MINTEL, 2021)

Nuestra vitalidad digital: Las Infraestructuras Críticas

Las infraestructuras críticas son el corazón digital de nuestro país. Son esos sistemas y redes que, si fallan, pueden causar un caos total. Piensa en la red de energía eléctrica que alimenta nuestros hogares, los sistemas bancarios donde manejamos nuestro dinero, las redes de telecomunicaciones que nos mantienen conectados, e incluso los sistemas de salud que salvan vidas. Protegerlas es una prioridad absoluta para garantizar que nuestra vida diaria no se detenga (Criollo, Flores, Flores, Santacruz, & Ron, 2023).

La amenaza invisible: Amenazas Híbridas

Las amenazas híbridas son un nuevo tipo de peligro que combina ataques en línea con acciones fuera de la red. Imagina que una campaña de noticias falsas (desinformación) en redes sociales se combina con un ciberataque a los sistemas de un banco. El objetivo es confundir a la gente y sembrar el pánico, mientras los atacantes se aprovechan del caos para lograr sus objetivos. Es una estrategia multifacética que busca explotar las vulnerabilidades de una sociedad desde múltiples frentes (Darkdata, 2023).

Tabla 1

Diferencias entre Ciberterrorismo, Ciberdelito y Hacktivismo

Categoría	Objetivo Principal	Motivación	Foco del Daño
Ciberterrorismo (Denning, 2020)	Provocar terror, inestabilidad y violencia a gran escala.	Política, ideológica, ego, delictiva o religiosa.	Infraestructura crítica, vulnerabilidades tecnológicas, seguridad física de la población, presión social, servicios estratégicos del Estado.
Ciberdelito (Infoem, 2020)	Obtener un beneficio económico, patrimonial o personal.	Lucro, venganza, fraude, robo de datos.	Individuos, empresas, instituciones (daño material o reputacional).
Hacktivismo (UNAH, 2021) (LISA, s/f)	Promover una agenda política o social.	Ideológica, política o activista.	Sitios web gubernamentales o corporativos (generalmente daño simbólico o reputacional).

Nota: *Elaboración Dirección de Ciberdelitos – Ministerio del Interior*

OBJETIVO

En el contexto actual de acelerada transformación digital, los entornos virtuales se han convertido en espacios vulnerables ante nuevas formas de amenaza, entre ellas el terrorismo en la red. Esta modalidad de ciberdelincuencia no solo implica la difusión de propaganda extremista, sino también la planificación, financiamiento y ejecución de actos que pueden desestabilizar la seguridad nacional.

La creciente sofisticación de las herramientas digitales utilizadas por actores maliciosos exige una respuesta coordinada entre instituciones públicas, privadas y organismos internacionales. En Ecuador, la necesidad de fortalecer los mecanismos de prevención, detección y respuesta ante este tipo de amenazas se vuelve imperativa para garantizar la estabilidad democrática, la protección ciudadana y la resiliencia institucional.

A fin de combatir los delitos cometidos con el uso de las tecnologías asociados al terrorismo, se ha estructurado el presente boletín de análisis de la ciberdelincuencia, el cual tiene como objetivo el analizar el fenómeno del terrorismo en la red como una amenaza para la seguridad nacional, identificando sus principales manifestaciones, actores involucrados, consecuencias sociales y riesgos asociados, con el fin de proponer lineamientos estratégicos para la coordinación interinstitucional, el fortalecimiento de capacidades técnicas y la formulación de políticas públicas orientadas a la prevención, mitigación y combate de este tipo de delitos. Además, se busca fomentar una cultura de conciencia digital, promoviendo el rol activo de la población en la detección y reporte de contenidos peligrosos que puedan representar una amenaza para la convivencia y la seguridad pública.

PANORAMA GEO CIBERDELINCUENCIAL

A nivel mundial

La empresa dedicada a proveer servicios de investigación de mercado y consultoría Mordor Intelligence, en su informe llamado “El informe de Análisis de participación y tamaño del mercado de lucha contra el Ciberterrorismo tendencias y pronósticos de crecimiento (2024-2029)” indica que tamaño del mercado global contra el Ciberterrorismo en 2024 se estima en 32,80 mil millones de dólares, con una proyección de alcanzar los 38,47 mil millones de dólares en 2029, lo que representa un crecimiento a una tasa anual compuesta (CAGR) del 3,26% durante este periodo; así mismo el tamaño del mercado de guerra cibernética se estima en 77,54 mil millones de dólares en 2024 y se espera que alcance los 185,65 mil millones de dólares en 2029, creciendo a una tasa compuesta anual del 19,08% en este mismo periodo.

La guerra cibernética implica operaciones ofensivas y defensivas, como ataques cibernéticos, espionaje y sabotaje. El número de ciberataques en todo el mundo está aumentando significativamente. La guerra cibernética utiliza todos los vectores accesibles a los ciberdelincuentes. Estos incluyen virus, archivos adjuntos de correo electrónico, ventanas

emergentes, mensajes instantáneos y otras formas de engaño en Internet (Intelligence, Mordor, 2019).

Como ejemplo tenemos el mayor sistema de pagos de atención médica de EE. UU., operado por Change Healthcare y que gestiona unos 14 000 millones de transacciones al año, sufrió un ataque de ransomware perpetrado por el grupo Blackcat/ALPHV[1]. Su sistema estuvo inactivo durante casi un mes tras el ataque del 21 de febrero de 2024 (Candan, 2024).

Global Risks Report 2024 del Foro Económico Mundial sitúa a la inseguridad en entornos digitales entre los principales riesgos mundiales.

La Oficina de Naciones Unidas contra la Droga y el Delito (UNODC), indica que los grupos extremistas emplean la red para el ciclo completo de actividades ilícitas como:

- Propaganda y Reclutamiento en plataformas de redes sociales, foros y la dark web para difundir ideologías de odio, reclutar nuevos miembros y radicalizar a individuos vulnerables a través de contenido audiovisual de alto impacto.
- Fuente de ingresos para el terrorismo a través de delitos como el ransomware, el phishing y el fraude con criptomonedas, para obtener fondos que son difíciles de rastrear y que sirven para financiar sus operaciones logísticas y ataques físicos.
- Utilizan las herramientas de comunicación cifrada actuales para coordinar células, planificar atentados y compartir información táctica de forma segura, eludiendo la vigilancia de las instituciones de inteligencia en los diferentes países.

Frente al avance de las ciberamenazas, existe el Índice Global de Ciberseguridad (IGC) de la Unión Internacional de Telecomunicaciones (UIT) dónde 175 países evalúan y fortalecen su seguridad digital en un marco de cooperación internacional donde promueve el intercambio

1 Ransomware ALPHV: Análisis del ataque BlackCat After Change Healthcare; https://www-picussecurity-com.translate.goog/resource/blog/alphv-ransomware?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc

de conocimientos sobre este tema. Este esfuerzo colaborativo, del cual el Ecuador también es parte activa, permite identificar vulnerabilidades, compartir estrategias defensivas y priorizar acciones clave: desde la protección de servicios esenciales como hospitales, alimentos y comunicaciones, entre otros, hasta la formación de equipos especializados en emergencias digitales y campañas de concienciación ciudadana.

A nivel regional, según el índice de inteligencia de amenazas IBM X-Force 2025, América Latina en el año 2024 representó el 8% de los incidentes de seguridad, afectando principalmente infraestructuras críticas y la continuidad de los sistemas financieros.

En América Latina, el principal factor de riesgo en la región es la presencia del delito organizado transnacional y su creciente sinergia con el ciberdelito. Grupos delictivos con operaciones en varios países utilizan el ciberespacio para el lavado de activos, la extorsión y el tráfico de drogas y armas. Esta convergencia entre el delito y el terror es particularmente peligrosa, ya que las tácticas, herramientas y redes de la ciberdelincuencia son adoptadas por células terroristas o contratadas como servicio con fines proselitistas, de reclutamiento, financiamiento o comunicación.

El Estado ecuatoriano frente al ciberterrorismo una perspectiva nacional

En el ámbito nacional, el Ecuador ha fortalecido progresivamente sus capacidades institucionales para enfrentar el ciberterrorismo. Un hito relevante es la creación del Comando de Ciberdefensa de las Fuerzas Armadas según lo establece el Estatuto Orgánico de Gestión Organizacional por Procesos del Comando Conjunto de las Fuerzas Armadas (Acuerdo No. 049 de 13 de abril de 2018) tiene como misión ***"Efectuar operaciones de defensa y exploración en el Ciberespacio en forma permanente, protegiendo la infraestructura crítica tecnológica de Fuerzas Armadas y otras asignadas, degradando o neutralizando la***

infraestructura critica tecnológica del adversario con orden, a fin de contribuir al cumplimiento de la misión del Comando Conjunto de las Fuerzas Armadas".

CIBERTERRORISMO EN EL CONTEXTO MUNDIAL MOTIVACIONES Y EFECTOS CASOS RELEVANTES

Motivaciones

Los ciberterroristas pueden tener motivaciones sociales, políticas, ideológicas, religiosas o económicas, actuando como respuesta a desigualdades, marginación o tensiones comunitarias, en busca de reconocimiento o reivindicación. También pueden perseguir fines políticos al intentar influir en decisiones gubernamentales, desafiar la autoridad del Estado o presionar para cambios mediante ataques a infraestructuras críticas. En otros casos, promueven ideologías extremistas o religiosas, imponiendo su visión del mundo mediante el miedo y la violencia digital. Finalmente, pueden actuar con fines económicos, causando pérdidas financieras o desestabilización como forma de presión o para respaldar otras acciones terroristas. La elección del ciberespacio como campo de acción responde a su bajo costo, alto alcance y anonimato, lo que lo convierte en un entorno ideal para este tipo de

operaciones. Estas motivaciones, combinadas con la facilidad tecnológica, hacen del Ciberterrorismo una amenaza compleja y en constante evolución (Yunos, Mohd, Ariffin, & Ahmad, 2017).

Efectos

Los efectos o consecuencias del Ciberterrorismo son amplios y profundos, abarcando desde la disrupción de infraestructuras críticas, como servicios de energía, agua, salud, transporte y telecomunicaciones, lo que puede paralizar regiones enteras y poner en riesgo vidas humanas, hasta un impacto económico severo, con pérdidas millonarias para gobiernos y empresas debido a daños directos, interrupciones operativas y pérdida de confianza. Además, estos ataques generan miedo y pánico social, al erosionar la percepción de seguridad pública, y provocan desestabilización política, al minar la confianza en las instituciones estatales. También se observa una clara afectación psicológica y emocional en la población, generando ansiedad colectiva y respuestas desproporcionadas ante amenazas. Finalmente, contribuyen al debilitamiento de la ciberseguridad nacional, al exponer fallas que obligan a redirigir recursos y reformular estrategias defensivas frente a una amenaza digital en constante evolución (Iftikhar, 2024).

Casos relevantes

Actualmente nos enfrentamos a un entorno de amenazas cada vez más sofisticado, con la llegada de tecnologías disruptivas como la IA o el blockchain y la masificación de las redes y equipos móviles, actores cibernéticos respaldados por Estados o grupos con altos niveles de sofisticación; hacktivistas motivados ideológicamente que ahora poseen la capacidad de ejecutar ataques más peligrosos que simples actos aislados; y ciberdelincuentes con fines económicos que actúan de forma persistente. haciendo uso de herramientas para llevar a cabo ataques de inhabilitación o destructivos contra infraestructuras críticas. Por ejemplo, actores patrocinados por gobiernos podrían activar esos grupos especiales durante

situaciones de crisis con el objetivo de provocar daños físicos estructurales, pérdida de vidas humanas y la interrupción de servicios esenciales. Asimismo, otros grupos que operan de manera independiente o como aliados de países adversarios, como aquellos vinculados a al-Qaeda, Hamás, u otros, han llevado a cabo ataques cibernéticos contra infraestructuras críticas o esenciales. En particular, los conflictos en Gaza han incentivado a diversos actores ideológicos y hacktivistas delincuenciales a desarrollar ofensivas destructivas dirigidas contra sectores claves (Departamento de Seguridad Nacional de los Estados Unidos, 2025).

Casos relevantes que configuran Ciberterrorismo o ciberguerra se presentan a continuación:

STUXNET - Planta nuclear de Natanz (2010)

Stuxnet es un gusano informático sofisticado y malicioso que fue descubierto en junio de 2010 y se considera la primera arma cibernética de alta tecnología usada para atacar infraestructura crítica real. Su objetivo principal fue la central nuclear de Natanz en Irán, donde infectó los sistemas de control industrial (SCADA) que gestionaban las centrifugadoras encargadas del enriquecimiento de uranio para el programa nuclear iraní. Stuxnet logró tomar el control de aproximadamente 1,000 centrifugadoras, haciéndolas funcionar a velocidades dañinas que causaron su destrucción física progresiva.

El gusano se propagó inicialmente a través de memorias USB infectadas y luego se infiltró en la red de la planta, buscando específicamente los controladores lógicos programables (PLC) que controlaban las centrífugas. Stuxnet estaba diseñado para reprogramar estos controladores y ocultar sus intervenciones, enviando información falsa a los sistemas de monitoreo para evitar que se detectara el sabotaje. El ataque logró deshabilitar cerca del 20% de las centrifugadoras, causando un daño significativo al programa nuclear de Irán y marcando un hito como el primer ataque cibernético con efectos destructivos en el mundo físico, lo que lo caracteriza como un ciberterrorismo de alta tecnología.

Además, Stuxnet explotó varias vulnerabilidades desconocidas del sistema operativo Windows, y se cree que fue desarrollado con el apoyo de gobiernos como Estados Unidos e Israel, estableciendo un precedente en la guerra cibernética moderna.

El caso de Stuxnet puede ser parcialmente considerado como ciberterrorismo, pero también es ampliamente descrito como un acto de ciberguerra o ciberataque con fines militares. Stuxnet fue una ciberarma altamente sofisticada diseñada para atacar infraestructura crítica, concretamente la planta nuclear de Natanz en Irán, causando daños físicos significativos a sus centrifugadoras. Su objetivo era claramente estratégico y político, con la intención de sabotear un programa nuclear que se percibía como una amenaza.

Ataque a los sistemas SCADA de la planta eléctrica en Ucrania (2015 y 2016)

Responsables: Grupo Sandworm (vinculado a Rusia).

El 23 de diciembre de 2015 ocurrió un apagón no programado que afectó a varias empresas distribuidoras eléctricas en Ucrania, dejando sin suministro a cientos de miles de usuarios por varias horas. Según el informe IR-ALERT-H-16-056-01 de CISA, se detectó la presencia del malware BlackEnergy en los sistemas de TI de esas compañías, aunque su rol exacto en el apagón no ha sido completamente confirmado. El ataque fue atribuido a actores cibernéticos patrocinados por el Estado ruso, y se documentó la colaboración entre agencias de EE. UU. y autoridades ucranianas para investigar y entender el incidente (CISA, 2021).

Ataques a plantas de agua en EE. UU. (2023)

En noviembre de 2023, CISA, el FBI, la NSA y otras agencias emitieron una alerta conjunta (AA23-335A) confirmando que actores cibernéticos afiliados a la Guardia Revolucionaria Islámica de Irán (IRGC), conocidos como CyberAv3ngers, explotaron vulnerabilidades en controladores lógicos programables (PLCs) de la empresa israelí Unitronics. Estos PLCs se utilizaban en sistemas de agua, aguas residuales y otros sectores críticos en EE. UU. El

acceso fue posible debido a configuraciones inseguras, como el uso de credenciales por defecto y conexiones a internet sin protección (CISA, 2024)

Según el informe técnico de CISA, los atacantes modificaron la lógica de control de los PLCs (ladder logic), bloquearon interfaces HMI y reemplazaron pantallas de inicio por mensajes ideológicos como: *"Every equipment 'made in Israel' is CyberAv3ngers legal target"*. Los dispositivos afectados estaban presentes en sectores como agua, energía, transporte y manufactura. Las agencias instaron a los operadores a cambiar contraseñas, desactivar accesos remotos innecesarios y segmentar sus redes para evitar accesos no autorizados (CISA, 2024).

Uno de los incidentes más notorios ocurrió en una planta de agua en Aliquippa, Pensilvania, donde el ataque interrumpió operaciones automáticas y obligó al cambio a modo manual. CyberAv3ngers mostró mensajes políticos como parte de una campaña de represalia por el apoyo de EE. UU. a Israel.

Aunque no hubo interrupciones significativas del suministro, CyberScoop e Infosecurity Magazine reportaron que estas intrusiones demostraron la fragilidad de sistemas OT mal configurados, con expertos alertando sobre el riesgo de ataques más destructivos en el futuro (Vasquez & Vicens, 2023)

TERRORISMO DIGITAL: RIESGOS PARA LA SEGURIDAD NACIONAL

Modalidades y técnicas utilizadas

En los primeros estudios sistemáticos sobre el fenómeno, la atención estaba centrada en la posibilidad de que grupos terroristas utilizaran las tecnologías de la información para alcanzar objetivos de carácter militar o estratégico. Entre las modalidades identificadas destacaban los ataques a sistemas de defensa y control, con escenarios hipotéticos que incluían el desvío de misiles o la neutralización de infraestructuras militares críticas. Junto a ello, se subrayaba el papel de los "insiders"[2], es decir, empleados o técnicos con acceso privilegiado a los sistemas, quienes podían actuar como vectores de sabotaje interno. A la par, se identificaba la presencia de "outsiders" jóvenes vinculados a subculturas digitales que, aun sin fines terroristas iniciales, podían ser captados o instrumentalizados. Finalmente, se

[2] Insider es un individuo que tiene acceso legítimo a información confidencial de una organización, https://mineryreport.com/ciberseguridad/glosario/tipos-de-amenazas/termino/insider/

resalta la operación en redes descentralizadas, sin jerarquías rígidas, lo que dificultaba la detección y neutralización de células digitales. (Breen, 2008)

Con el paso del tiempo, y especialmente en estudios recientes como el de Aldada y Ali en 2022, el foco se amplió hacia modalidades más operativas y orientadas al impacto social e institucional inmediato. Entre ellas, se identifican los ataques contra infraestructuras críticas (energía, transporte, agua, banca, telecomunicaciones), cuya vulneración puede paralizar servicios esenciales y generar un efecto dominó en la economía y la gobernabilidad. También se consolidó el uso de herramientas técnicas como malware, ransomware y ataques de denegación de servicio (DDoS), capaces de inutilizar portales oficiales y obstaculizar servicios gubernamentales.

Paralelamente, las redes sociales se han convertido en un instrumento central de propaganda, desinformación y reclutamiento, facilitando la radicalización en línea y la difusión masiva de mensajes extremistas. A ello se suma el área financiera, con el uso de criptomonedas y plataformas digitales para canalizar recursos y sostener las operaciones clandestinas. (Aldada, 2022)

Estrategias de Combate

El desarrollo de diversas modalidades de terrorismo digital a lo largo del tiempo ha obligado a los Estados y a la comunidad internacional a perfeccionar sus respuestas. En la etapa inicial, las medidas de combate se centraban en el control de accesos, auditorías sistemáticas, monitoreo permanente de los sistemas críticos y cooperación interagencia, especialmente en el ámbito militar y de inteligencia. Estas acciones buscaban neutralizar a los denominados insiders y garantizar la seguridad de infraestructuras estratégicas. (Breen, 2008)

En una segunda etapa, con la incorporación de técnicas propias del mundo cibernético, las estrategias de combate se ampliaron hacia la creación de marcos normativos específicos, la capacitación de equipos especializados en ciberseguridad y forensia digital, y la coordinación estrecha entre gobiernos, sector privado y sociedad civil. (Bishmanov, 2024). El objetivo principal era cerrar la brecha entre la innovación delictiva y la capacidad de respuesta estatal.

Esta comparación temporal evidencia que, mientras hace unas décadas predominaban las preocupaciones estratégicas vinculadas al acceso interno, la amenaza militar y la lógica de redes; en la actualidad las modalidades identificadas responden a un escenario mucho más diversificado, donde convergen técnicas de desinformación digital, radicalización en línea y explotación de infraestructuras críticas. De esta manera, el ciberterrorismo se configura como un fenómeno dinámico que combina amenazas tradicionales con métodos emergentes cada vez más sofisticados y de alcance global.

Para dimensionar el alcance real de estas técnicas en la actualidad, se presentan algunos datos y ejemplos recientes que reflejan su magnitud e impacto:

1. **Ataques a infraestructuras críticas**

   Entre enero 2023 y enero 2024, se registraron más de 420 millones de ciberataques dirigidos a infraestructuras críticas a nivel mundial esto equivale a 13 ataques por segundo, con un aumento del 30% respecto a 2022 (Ribeiro, 2024)

   Tras un ataque terrorista en Pahalgam (India), ese país ha enfrentado entre 30 y 40 ciberataques significativos diarios, dirigidos especialmente al sector financiero y energético. (Vishnoi, 2025)

2. **Propaganda y radicalización en redes sociales**

En el Reino Unido, pese a la promulgación de la Ley de Seguridad en Línea (Online Safety Act) en marzo de 2025, permanecen más de mil cuentas vinculadas a grupos terroristas (como Hezbollah y los hutíes) activas en X, Telegram, Facebook, Instagram, TikTok y YouTube, publicando desde videos de ejecuciones hasta tutoriales para fabricar explosivos. (Sellman, 2025)

En Francia, un 70% de los detenidos por presuntos complots tenían menos de 21 años, y la radicalización comenzó a través de contenido violento en línea accesible desde una edad temprana. (Leicester, 2025)

Plataformas de videojuegos en vivo, como Discord, están siendo usadas para radicalizar adolescentes; en el Reino Unido, 13 % de las investigaciones antiterroristas actualmente involucran individuos menores de 18 años, triplicándose en solo tres años. (Brooks, 2025)

3. **Ataques impulsados por inteligencia artificial**

Se estima que en 2025 se realizan hasta 2.200 ciberataques diarios a nivel global, algunos potenciados por herramientas de IA que automatizan y escalan las operaciones (Capitol, 2025).

Un 30 % de las intrusiones totales se basan en ataques relacionados con la identidad del usuario (credential phishing usando cuentas válidas), impulsados en parte por IA. (IBM, 2025)

El concepto de radicalización algorítmica muestra que los algoritmos de recomendación (como en TikTok, YouTube, Facebook) pueden llevar a usuarios rápidamente hacia contenido cada vez más extremo, contribuyendo a la radicalización sin detección. (Camargo, 2020)

ATAQUES A INFRAESTRUCTURAS CRÍTICAS

El Ciberterrorismo y la seguridad nacional

Los ciberataques a infraestructuras críticas no buscan información; con mayor frecuencia, buscan acceder a sistemas de control con fines de interrupción, ya sea para terrorismo nacional o extranjero, o acceder a secretos con fines de espionaje. Y si bien estos ataques están en aumento a nivel mundial, no son nuevos.

La infraestructura crítica, esencial para el funcionamiento de la sociedad, incluye sectores como la energía, el transporte, la salud, la banca, las comunicaciones y el gobierno. Su protección no solo garantiza la seguridad nacional, la estabilidad económica y la seguridad pública, sino que también sostiene la vida diaria de las personas, protegiendo su salud y bienestar y facilitando la convivencia en sociedad. Por lo tanto, asegurar la continuidad de servicios fundamentales como la electricidad, el agua y las telecomunicaciones es una tarea neurálgica (Martinez, 2024).

La Comisión Económica para América Latina y el Caribe (CEPAL) de Naciones Unidas en agosto de 2023 público el informe “Ciberataques a la logística y la infraestructura crítica en

América Latina y el Caribe" el cual se realizado a 10 países de la región incluido Ecuador el periodo de la investigación fue 2020 a 2022, donde podemos ver los "*Eventos destacados en logística e infraestructuras críticas"* tabla 2 (Diaz & Núñez, 2023).

Tabla 2

Cantidad de incidentes encontrados por país

País	Cantidad	Porcentaje
Brasil	27	19
Colombia	20	14
Argentina	19	13
Chile	16	11
México	15	10
Perú	11	8
Uruguay	11	8
Ecuador	10	7
República Dominicana	8	6
Panamá	7	5

Nota: *Fuente CEPAL* (Diaz & Núñez, 2023)

En este contexto el Ministerio de Defensa del Ecuador, como organismo rector que emite políticas para la defensa y administración de las Fuerzas Armadas y organismos adscritos a fin de garantizar la soberanía nacional e integridad territorial, emito el **Plan Específico de Defensa 2019-2030**, en su análisis de la problemática de la defensa indica que las una de las amenazas que atentan contra el Estado ecuatoriano son los ciberataques a la infraestructura crítica; el empleo del manejo de las tecnologías de la información y comunicaciones (TIC) y redes informáticas vulneran la seguridad y defensa del Estado, a través de ciberataques como phishing, hacking, cracking hasta el ciberterrorismo.

En su objetivo estratégico 1 indica lo siguiente : "***Fortalecer la Defensa y Seguridad del Estado****: el Estado participará activamente en el control efectivo del territorio nacional (espacios terrestres, marítimos, aéreos y el ciberespacio) impulsando el desarrollo de políticas y estrategias para la ciberseguridad, ciberdefensa y defensa aeroespacial,*

permitiendo que estas se encuentren en las mejores condiciones para afrontar las amenazas y riesgos que atenten a la paz y seguridad" (Ministerio de Defensa, 2019).

IMPLICACIONES POLÍTICAS Y SOCIALES

El terrorismo en la red representa un riesgo significativo para la seguridad nacional, con profundas implicaciones políticas y sociales. Afecta la gobernabilidad al desestabilizar los estados, amenaza la seguridad ciudadana y erosiona la confianza en las instituciones. Además, tiene un impacto negativo en la economía, la salud pública y la cohesión social. (ICE, 2025)

Implicaciones políticas y sociales:

Se puede contar con un sin número de implicaciones entre las más significativas tenemos:

Desestabilización política: El terrorismo en la red puede socavar la legitimidad de los gobiernos, provocar disturbios sociales y alterar el orden público, dificultando la gobernabilidad. (Naciones Unidas, n.d.)

Aumento de la polarización: La propaganda y la desinformación pueden exacerbar las divisiones sociales, creando tensiones entre diferentes grupos y socavando la cohesión social. (Naciones Unidas, n.d.)

Miedo y desconfianza: El terrorismo en la red puede generar miedo y desconfianza en la población, afectando la confianza en las instituciones y en la capacidad del gobierno para proteger a sus ciudadanos. (Jordán, 2025)

Restricciones a las libertades civiles: En respuesta al terrorismo en la red, los gobiernos pueden implementar medidas de seguridad que restrinjan las libertades civiles, como la vigilancia masiva o la censura en línea, lo que plantea preocupaciones sobre los derechos humanos y la privacidad. (ONU, 2022)

Impacto en la economía: Los ataques terroristas en la red pueden afectar negativamente a la economía, causando pérdidas en sectores clave, interrumpiendo el comercio y la inversión.

Efectos en la salud mental: La exposición a la violencia en línea y el miedo al terrorismo pueden generar problemas de salud mental, como estrés postraumático, ansiedad y depresión, tanto en las víctimas directas como en la población en general. (ICE EEUU, 2025)

Seguridad nacional y gobernabilidad:

La seguridad nacional se ve comprometida por el terrorismo en la red, ya que afecta la capacidad del Estado para proteger a sus ciudadanos y mantener el orden público. La gobernabilidad se ve amenazada por la desestabilización política, la polarización social y la pérdida de confianza en las instituciones. Es crucial abordar este problema de manera integral, combinando medidas de seguridad con políticas de prevención, educación y promoción de la cohesión social (ICE EEUU, 2025).

Riesgos para la Seguridad Nacional y la Gobernabilidad:

Entre los riesgos más relevantes se puede tener:

Ataques cibernéticos: Los grupos terroristas utilizan internet para ataques cibernéticos contra infraestructuras críticas, sistemas financieros y comunicaciones, causando interrupciones y daños severos. (Arias & Luis, 2023).

Propaganda y radicalización: Las plataformas digitales se utilizan para difundir propaganda terrorista, reclutar nuevos miembros y radicalizar individuos, a menudo jóvenes, a través de mensajes extremistas. (Mayorga & Holguín, 2024)

Financiación y logística: La red facilita la financiación de actividades terroristas, incluyendo el lavado de activos y la recaudación de fondos, así como la coordinación de operaciones y el reclutamiento de personal.

Desinformación y manipulación: La proliferación de noticias falsas y desinformación en línea puede generar miedo, desconfianza y polarización social, socavando la estabilidad política.

Ataques híbridos: La combinación de ataques cibernéticos, desinformación y propaganda puede llevar a ataques híbridos que combinan elementos virtuales y físicos, complicando la respuesta.

Medidas para combatir el terrorismo en la red

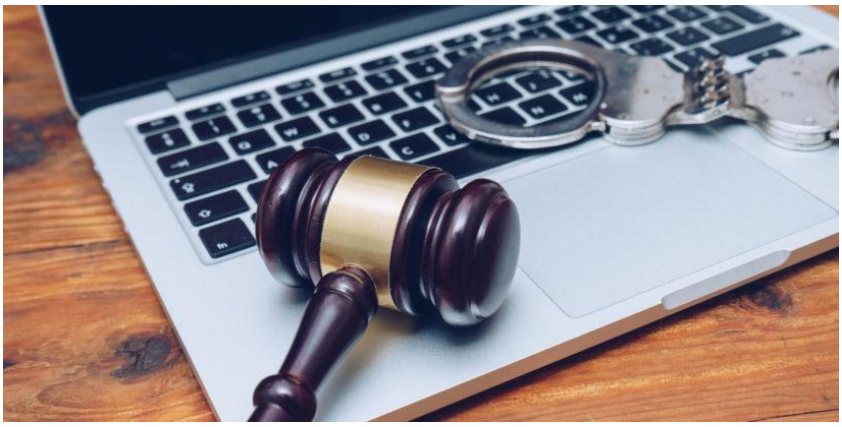
Fortalecimiento de la Ciberseguridad: Invertir en sistemas de ciberseguridad y capacitar a profesionales en la detección y prevención de ataques cibernéticos es crucial para proteger la infraestructura crítica y la información sensible. (Arias & Luis, 2023). En este contexto el Estado ecuatoriano ha logrado establecer instrumentos estratégicos que permitan enfrentar las amenazas cibernéticas en el campo de la seguridad y defensa como **Estrategia y Política Nacional de Ciberseguridad del Ecuador**.

Promoción de la Educación y la Conciencia: Educar a la población sobre los riesgos del terrorismo en línea y promover el pensamiento crítico puede ayudar a prevenir la radicalización y el reclutamiento. (Arias & Luis, 2023)

Apoyo a las Víctimas: Brindar apoyo psicológico y social a las víctimas de ataques terroristas es fundamental para su recuperación y para prevenir la victimización secundaria.

Finalmente se puede manifestar que el terrorismo en la red representa un desafío multifacético que requiere una respuesta integral que involucre a gobiernos, instituciones, sociedad civil y ciudadanos. La cooperación internacional, el fortalecimiento de la ciberseguridad, la promoción de la educación y el apoyo a las víctimas son clave para combatir esta amenaza y proteger la seguridad nacional y el bienestar social

Bajo este contexto, la concepción de la seguridad del Estado ecuatoriano tiene un enfoque multidominio, encaminado a desarrollar actividades dirigidas a proteger el ciberespacio, lo que conlleva a incrementar medidas de seguridad de las instituciones gubernamentales y sectores estratégicos. (Paredes & Semanate, 2024). En este sentido, el país ha establecido instrumentos como **La Estrategia de Ciberdefensa y la Guía Político – Estratégica de Ciberdefensa** que permitan Incrementar y fortalecer las capacidades de Ciberdefensa del Estado ecuatoriano y protección de servicios esenciales en el ciberespacio.



MARCO NORMATIVO NACIONAL E INTERNACIONAL

Marco normativo nacional

El Marco Normativo Nacional del Ecuador se sustenta en la Constitución de la República, que reconoce como deber primordial del Estado garantizar, sin discriminación alguna, el efectivo goce de los derechos establecidos en la norma suprema y en los instrumentos internacionales. Dentro de estos deberes, se establece la obligación de

asegurar a los habitantes el derecho a una cultura de paz y a la seguridad integral (Constitución, art. 3, núm. 8). De igual forma, se reconoce y garantiza la inviolabilidad de la vida y el derecho a la integridad personal como pilares esenciales del ordenamiento jurídico (Constitución, art. 66, núm. 1 y 3). Estos preceptos constituyen la base sobre la cual se desarrollan las políticas y acciones del Estado en materia de protección ciudadana.

En el ámbito de la justicia penal, la Fiscalía General del Estado es la institución encargada de dirigir la investigación preprocesal y procesal penal, de oficio o a petición de parte, ejerciendo la acción pública con sujeción a los principios de oportunidad y mínima intervención penal, y otorgando especial atención a los derechos de las víctimas (Constitución, art. 195). Por su parte, el Estado está llamado a garantizar la seguridad humana a través de políticas integradas que promuevan la convivencia pacífica, la prevención de la violencia y la discriminación, así como la reducción de los índices de criminalidad en todas sus formas (Constitución, art. 393).

El Código Orgánico Integral Penal (COIP) complementa este marco al normar el poder punitivo del Estado y tipificar las conductas constitutivas de infracciones penales (COIP, art. 1). Bajo el principio de mínima intervención, se establece que la acción penal solo será legítima cuando sea estrictamente necesaria para proteger los derechos de las personas (COIP, art. 3). El COIP define la infracción penal como una conducta típica, antijurídica y culpable (COIP, art. 18), clasifica las infracciones en delitos y contravenciones (COIP, art. 19), e incorpora disposiciones específicas frente a amenazas complejas como el terrorismo y su financiación, sancionando aquellas conductas que buscan sembrar el terror, atentar contra la vida o la integridad de las personas, o comprometer la seguridad de infraestructuras estratégicas (COIP, arts. 366-367).

A su vez, la Ley de Seguridad Pública y del Estado establece el marco para la protección integral de la sociedad y la defensa de la democracia, definiendo como objeto la regulación de la seguridad integral en el Estado de derechos y justicia, a fin de garantizar el orden público, la convivencia pacífica y el buen vivir de los ciudadanos (Ley de Seguridad Pública, art. 1). Esta normativa dispone que las políticas y estrategias de seguridad deben orientarse a salvaguardar la soberanía, la integridad territorial, la seguridad de las personas y las instituciones, contemplando tanto la complementariedad entre lo público y lo privado como la participación activa de la ciudadanía (Ley de Seguridad Pública, art. 2). Asimismo, reafirma que es deber ineludible del Estado promover y garantizar la seguridad de todos los habitantes, comunidades y nacionalidades (Ley de Seguridad Pública, art. 3), guiándose bajo principios de integralidad, proporcionalidad, prioridad, prevalencia y responsabilidad (Ley de Seguridad Pública, art. 4).

En conjunto, este marco normativo configura un sistema coherente que busca no solo sancionar las conductas delictivas, sino también prevenir la violencia, fortalecer la convivencia social y garantizar la seguridad humana como condición indispensable para el desarrollo del país, estableciendo así un equilibrio entre la protección de derechos fundamentales y el ejercicio del poder punitivo del Estado.

Marco normativo internacional

Instrumentos universales

- **Resolución 1373 (2001) del Consejo de Seguridad - ONU**: insta a los Estados a prevenir y sancionar el financiamiento, apoyo y refugio a terroristas; incluye la cooperación frente al uso de tecnologías de comunicación utilizadas por grupos terroristas.

- **Resolución 1566 (2004) del Consejo de Seguridad - ONU** y posteriores (2178 de 2014, 2396 de 2017): abordan la prevención de desplazamientos de combatientes extranjeros, la radicalización en línea y el uso de internet para fines terroristas.
- **Estrategia Global de las Naciones Unidas contra el Terrorismo (2006, última revisión 2021)**: instrumento global único para fortalecer los esfuerzos nacionales, regionales e internacionales en la lucha contra el terrorismo.

Instrumentos regionales (OEA / Interamericanos)

- **Convención Interamericana contra el Terrorismo (OEA, 2002)**: obliga a los Estados parte a adoptar medidas de prevenir, sancionar y eliminar el terrorismo.
- **Resoluciones del Comité Interamericano contra el Terrorismo (CICTE-OEA)**: promueven capacidades regionales en el combate del terrorismo.

Instrumentos especializados en el ciberespacio

- **Convenio de Budapest sobre Ciberdelincuencia (2001, Consejo de Europa)**: primer tratado vinculante que tipifica ciberdelitos y delitos cometidos mediante el uso de las TICs y establece mecanismos de cooperación judicial internacional (Ecuador es Estado adherente).
- **Segundo Protocolo Adicional al Convenio de Budapest (2022)**: relativo a la cooperación reforzada y la divulgación de pruebas electrónicas
- **Grupo de Acción Financiera Internacional (GAFI):** Organismo internacional que establece estándares para la lucha contra el blanqueo de capitales (ALD), la financiación del terrorismo (FFT) y la financiación de la proliferación (FPC)
- **UIT / Índice Global de Ciberseguridad**: mecanismos de cooperación técnica y de evaluación de capacidades estatales frente a amenazas digitales.

PERFILAMIENTO DEL CIBERTERRORISTA

Dirección Contra La Delincuencia Organizada Transnacional y Terrorismo

Dirección de Ciberdelitos

Ministerio del Interior

De acuerdo con el artículo de Denning (2000) Statement of Dorothy E. Denning, el ciberterrorismo es la convergencia entre el terrorismo y el ciberespacio, una conjunción de fuerzas que, utilizando las ventajas y capacidades del terrorismo físico, ahora basado en fallas y vulnerabilidades tecnológicas, logran intimidar o presionar a un estado y sus ciudadanos.

Por otro lado, Nelson, Choi, Iacobucci, Mitchell y Gagnon (1999) indican que el ciberterrorismo se asocia con las vulnerabilidades de infraestructuras críticas de una nación los estados, tales como: centrales eléctricas, plantas de gas (GLP) cadenas de producción y suministro de hidrocarburos o agua, infraestructuras de telecomunicaciones, bancos y finanzas, sistemas de transporte masivo y servicios de emergencia, estos hacen parte de la base económica de un país y por ende de la población. Si bien las vulnerabilidades de los

sistemas tecnológicos o físicos no son sinónimo de amenazas, estas requieren un actor principal (grupo o persona) con la motivación, recursos y conocimientos para explotarlas.

Según Gordon y Ford (2003), las acciones ciberterroristas son actividades terroristas ejecutadas en el entorno virtual. en este trabajo señalan y delinean un modelo base para comprender el ciberterrorismo, como una extensión del terrorismo, para lo cual establecen siete elementos de análisis, a saber:

- ¿Quién es el perpetrador?: un grupo o un individuo;
- El sitio donde se adelanta la acción;
- La acción misma realizada;
- La herramienta o estrategia utilizada: violencia, secuestro, bomba, etc.;
- El objetivo de la acción: el gobierno, una organización particular;
- La afiliación a la que pertenece el perpetrador y finalmente
- La motivación.

Por lo expuesto, no existe un consenso sobre el significado de ciberterrorismo; sin embargo, la definición de Pollitt, mencionada en el trabajo de Taylor, R., Caeti, T., Kall Loper, D., Fritsch, E. y Liederbach, J. (2006, p. 23) sugiere una forma interesante de comprender el mismo: “El ciberterrorismo es un ataque premeditado, política o ideológicamente motivado o una amenaza de ataque contra la información, los sistemas de información, programas de computadores y datos que puede llevar una acción violenta contra objetivos civiles”.

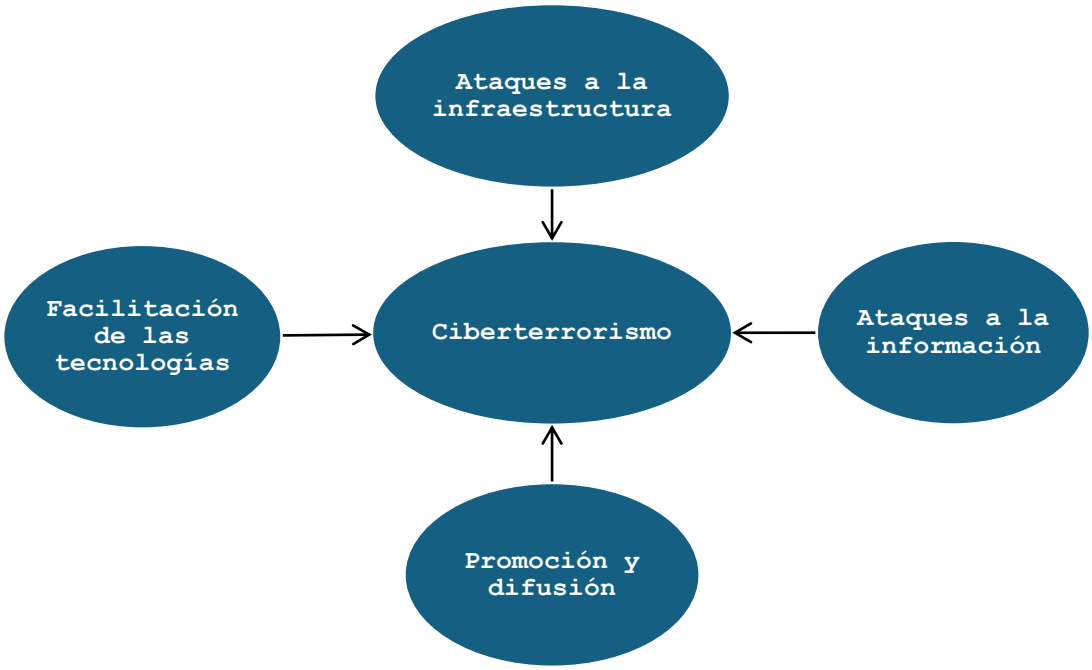
En este sentido, el ciberterrorismo abarca cuatro (4) variables que deben ser parte del análisis de esta nueva amenaza, la cual se confunde con las fallas mismas de los sistemas de información, y deja sin argumentos tanto a los profesionales de la seguridad, como a los analistas de inteligencia.

Las variables propias del ciberterrorismo son:

- Ataques a la infraestructura de tecnologías de información, TI,
- Ataques a la información,
- Utilización de las TI para labores de coordinación de los planes terroristas, y
- La promoción y difusión de sus consignas ideas, así como del entrenamiento de sus grupos de acción.

Figura 1

Variables relacionadas con el Ciberterrorismo



Nota: *Elaboración Dirección de Ciberdelitos – Ministerio del Interior (Taylor, R., Caeti, T., Kall Loper, D., Fritsch, E. y Liederbach, J. (2006))*

Estas cuatro variables y su relación, convergen en ver comportamientos emergentes que permitirán ver cómo los estados, las organizaciones y la sociedad deben tomar acciones para que el terror en línea no escale y se convierta en una amenaza invisible y predecible que se advierte (Council of Europe, 2007) (Rollins & Wilson, 2007).

Si la tendencia persiste, el mundo estará dando pie a eventos de mayor magnitud y complejidad, el atacante demostrará que puede atemorizar a un estado, y que éstos no cumplen con su deber de protección a la ciudadanía ahora en el ciberespacio.

Por otro lado, la Dirección de Ciberdelitos y la Dirección Contra La Delincuencia Organizada Transnacional y Terrorismo del Ministerio del Interior concluyen que es posible trazar perfiles criminológicos de los ciberdelincuentes que podrían encajar en la categoría de "ciberterroristas" (entendiendo este término como autores de ataques cibernéticos graves, sea con motivación política o delictiva). En general, las autoridades han identificado a individuos jóvenes, de formación principalmente autodidacta en informática y con alto nivel de conocimientos técnicos, que actúan tanto solos como en pequeñas células. Un ejemplo emblemático es el llamado *"Hacker del Sombrero Negro"*, cuyo verdadero nombre (Carlos S. P.) fue revelado tras vincularlo con más de 50 intrusiones a entidades públicas y privadas en Ecuador desde 2021 (Torres , 2022). Este actor, de apenas 31 años de edad, quiteño, sin título académico formal en sistemas, pero con notable destreza técnica, logró violentar sistemas de instituciones que van desde la Policía Nacional e instituciones financieras hasta petroleras estatales como Petroecuador. Su caso ilustra el perfil de un exfuncionario con acceso privilegiado (fue agente de inteligencia en la extinta Secretaría de Inteligencia (Senain, hasta 2017) que usó sus habilidades para el lucro personal: sustrajo datos clasificados y luego intentó venderlos o extorsionar a sus víctimas exigiendo rescates millonarios en criptomonedas. Este individuo operaba bajo varios pseudónimos (*Uroborox*, *Hotarus Corp*, etc.) y colaboraba con al menos otro hacker de similares características (un ex miembro de la Armada ecuatoriana de 30 años), evidenciando que estos ciberdelincuentes locales suelen conformar pequeñas redes de confianza, muchas veces con orígenes comunes (entrenamiento militar o vínculos previos) y compartiendo conocimientos para potenciar sus ataques.

En términos sociodemográficos, el perfil típico identificado se corresponde mayoritariamente con hombres jóvenes (entre 20 y 35 años), con alta competencia

tecnológica y familiaridad con herramientas de hacking. No necesariamente poseen estudios superiores concluidos; en cambio, demuestran haber adquirido conocimientos en comunidades en línea, foros clandestinos o incluso dentro de instituciones donde tuvieron contacto con sistemas críticos. Algunos han aprovechado su posición interna para extraer información (casos de *insiders*), mientras que otros actúan externamente, pero con sofisticación comparable a la de profesionales en seguridad informática. Un rasgo notable es su adaptabilidad y autodesarrollo continuo: se mantienen al día con vulnerabilidades, crean sus propios *scripts* o malware (el *Hacker del Sombrero Negro* llegó a publicar el código de la explotación usada contra un banco en su cuenta de GitHub) y dominan tácticas de anonimización (uso de alias múltiples, correos cifrados como ProtonMail, canales en la *dark web*, etc.).

La motivación principal observada en estos perfiles ecuatorianos suele ser económica (extorsión, fraude, robo de información vendible) más que puramente ideológica. No obstante, existe un solapamiento con casos de hacktivismo político: algunos individuos o grupos han atacado objetivos gubernamentales por desacuerdo con políticas (como *Anonymous* en el caso Assange, o posibles afiliaciones políticas insinuadas en ciertos hackeos a instituciones durante coyunturas críticas). Esto sugiere que el espectro del "ciberterrorista" nacional va desde el ciberdelincuente oportunista (motivación lucrativa) hasta el activista digital radicalizado (motivación política o social). En ambos casos, comparten características criminológicas como alta confianza en la impunidad (dada la dificultad de rastreo y la falta de preparación histórica de la justicia local para procesarlos) y una cierta osadía exhibicionista: varios han divulgado públicamente sus logros ilícitos para amedrentar a las víctimas o ganar reputación entre pares (por ejemplo, anunciando en Twitter y foros los datos robados y plazos para pago (Torres , 2022), o dejando su firma en *defacements* de sitios gubernamentales en

portales como Zone-H). Estas conductas reflejan un patrón de ego y desafío a la autoridad común en el perfil delincuente informático.

En síntesis, el perfil criminológico del ciberdelincuente ecuatoriano de alto nivel combina juventud, habilidad técnica autodidacta, motivaciones de lucro o protesta, y aprovechamiento de brechas institucionales. Son individuos que explotan la falta de protocolos robustos de evidencia digital y la escasa coordinación policial, factores que han dificultado su captura y sanción en Ecuador. Identificar estos perfiles resulta clave para el diseño de estrategias de contrainteligencia y prevención del ciberterrorismo en el país.

Componentes criminológicos del Ciberterrorista

El perfil psicológico del ciberterrorista o ciberdelincuente está marcado por una combinación de motivaciones personales, rasgos de personalidad afines a la actividad delictiva informática y, en ocasiones, factores grupales de radicalización. En primer lugar, sobresalen las motivaciones que impulsan sus actos: la mayoría de los casos analizados muestran un afán de lucro económico o beneficio personal directo. Los autores intelectuales de grandes hackeos suelen buscar recompensas monetarias, ya sea mediante extorsión (pidiendo rescate por datos secuestrados, como en los ataques de ransomware) o comercialización de información (venta de datos sensibles robados en mercados negros digitales). Este ánimo de lucro se observa claramente en la conducta del *Hacker del Sombrero Negro*, quien al vulnerar sistemas de bancos y entidades estatales no dudó en exigir pagos de hasta USD 2 millones en Bitcoin para no divulgar la información sustraída. La promesa de ganancias sustanciales, sumada a la baja probabilidad percibida de ser capturado, actúa como potente incentivo psicológico.

No obstante, también existen motivaciones ideológicas o políticas en ciertos ciberatacantes. Estos individuos, más cercanos al concepto de *terroristas digitales*, están

movidos por una causa o resentimiento contra instituciones. Pueden ver sus acciones como una forma de protesta extrema o venganza. Por ejemplo, miembros locales de *Anonymous* y otros grupos de hacktivistas han justificado ataques a páginas gubernamentales como una lucha contra la corrupción o en defensa de la libertad de expresión. Estos actores psicológicamente se ven a sí mismos como justicieros o guerreros de una causa, racionalizando el daño colateral de sus acciones como "sacrificios necesarios" para un bien mayor. Tal convicción puede volverlos más peligrosos, pues están dispuestos a arriesgarse sin esperar recompensas materiales, buscando más bien impacto público, miedo o repercusión mediática, que son precisamente los fines del terrorismo convencional.

En cuanto a patrones conductuales, muchos ciberdelincuentes exhiben rasgos de personalidad asocial o disociada de las consecuencias reales de sus actos. La interacción detrás de una pantalla puede disminuir su empatía hacia las víctimas; robar datos o colapsar un servicio se percibe como un desafío técnico más que como un delito con afectados de carne y hueso. Asimismo, se detecta en ellos un componente de ego y necesidad de reconocimiento. Paradójicamente, aunque buscan el anonimato para evadir a la ley, al mismo tiempo suelen dejar *firmas* o presumir de sus hazañas en comunidades clandestinas, buscando la aprobación de sus pares. Esto se evidencia en el uso de alias distintivos bajo los cuales ganan fama en el *underground*. En psicología criminal, este comportamiento denota rasgos narcisistas: el hacker disfruta el sentimiento de poder y superioridad intelectual al burlar sistemas de alta seguridad, y anhela reconocimiento por esas habilidades. De ahí que divulguen pantallazos de sus logros o desafíen públicamente a las autoridades anunciando ataques, generando una especie de *juego de prestigio* dentro de la subcultura hacker.

Otro elemento por considerar es la racionalización y falta de remordimiento. Muchos ciberatacantes se autojustifican alegando que sus víctimas (bancos, gobiernos,

corporaciones) tienen recursos para recuperarse o que se lo “merecen” por supuestas malas prácticas. En otros casos, sobre todo los motivados políticamente, se convencen de que están haciendo “lo correcto” por ejemplo, filtrando información confidencial para exponer verdades al público. Esta distorsión cognitiva les permite continuar delinquiendo sin disonancia moral, considerándose a sí mismos más como revolucionarios que como delincuentes.

En cuanto a factores colectivos, cuando los ciberatacantes operan en grupo, entra en juego la dinámica de refuerzo grupal y radicalización. Grupos como *Anonymous* funcionan bajo principios de identidad colectiva donde el individuo diluye su responsabilidad en la masa, alentando actos más osados de los que haría solo. Asimismo, comunidades en la darknet y foros de hackers actúan como cámaras de eco que pueden intensificar posturas extremistas (por ejemplo, incitando ataques contra un gobierno percibido como opresor). En Ecuador, si bien no hay evidencia pública de células terroristas cibernéticas altamente estructuradas, sí existen pequeños colectivos digitales radicalizados desde hackers de ideología anarquista hasta grupos vinculados con movimientos sociales que podrían escalar sus métodos hacia formas más disruptivas de protesta digital.

Por último, es relevante destacar los posibles factores psicológicos individuales como la búsqueda de emoción (sensation-seeking) y la tendencia al desafío intelectual. El hacking ofrece un campo de constante reto y creatividad; individuos con alta inteligencia lógica y habilidades técnicas encuentran en ello un estímulo. Algunos casos sugieren incluso elementos de aislamiento social o dificultades de integración, donde el mundo virtual se vuelve su ámbito primario de éxito y validación. Aunque estos rasgos no son universales, se asemejan a perfiles de delincuentes informáticos en otros países, donde a veces se han detectado trastornos leves del espectro autista o personalidades introvertidas pero obsesivas en la resolución de problemas computacionales.

Contexto sociopolítico que influye en el riesgo de Ciberterrorismo

El contexto sociopolítico ecuatoriano juega un papel fundamental en la gestación y contención del riesgo de Ciberterrorismo. Por un lado, ciertas condiciones internas han podido favorecer la aparición de actores dispuestos a perpetrar ciberataques de gran escala; por otro, también existen factores que pueden mitigar o dificultar estas amenazas.

Entre los elementos que pueden favorecer el riesgo, destaca la polarización política que vive el país desde hace más de una década. Ecuador ha atravesado periodos de alta confrontación entre facciones políticas, con amplios movimientos de protesta social. En este clima polarizado, la esfera digital se convierte en una extensión de la arena política: grupos de simpatizantes y opositores trasladan sus disputas a redes sociales, campañas de desinformación y, en casos extremos, a ataques cibernéticos contra adversarios. La atribución (acertada o no) de hackeos a actores políticos rivales se ha vuelto parte del discurso público.

Asimismo, la infiltración del crimen organizado transnacional en Ecuador, particularmente de carteles del narcotráfico, añade otra dimensión sociopolítica. Aunque tradicionalmente estos grupos operan mediante violencia física, existen indicios globales de que están incorporando capacidades cibernéticas (contratando hackers para espionaje o sabotaje de sistemas de seguridad) (Baltazar, 2018) (Asman, 2025). En Ecuador se ha reportado cooperación entre narcotraficantes y técnicos informáticos para obtener información de agencias de seguridad. Por ejemplo, investigaciones internacionales revelaron que el Cártel de Sinaloa empleó un hacker para rastrear a un agente del FBI en territorio ecuatoriano y vulnerar cámaras de vigilancia, demostrando la convergencia entre crimen organizado y ciberdelito (Reuters, 2025). Este precedente sugiere que, en un contexto de aumento del narcotráfico en el país, células delictivas podrían recurrir al ciberataque para eliminar pruebas,

vigilar a autoridades o causar caos que distraiga a las fuerzas del orden. Si estas organizaciones altamente financiadas deciden potenciar su arsenal con ataques cibernéticos, el impacto podría ser similar al de actos terroristas, por el miedo generalizado que pueden infundir (imaginemos un ataque simultáneo al sistema de transporte o a la red eléctrica orquestado por mafias, algo que ya preocupa en otras latitudes).

No obstante, también existen factores en el contexto ecuatoriano que mitigan el riesgo o al menos dificultan la proliferación de ciberterrorismo. Uno de ellos es la creciente conciencia gubernamental y pública sobre la importancia de la ciberseguridad. Tras episodios sonados de fugas de información y ataques, la ciudadanía ha presionado por mayor protección de sus datos y las autoridades han respondido con medidas concretas (como la creación de la Comité Nacional de Ciberseguridad y la política nacional mencionada). Esta atención trae consigo más inversión en ciberdefensa y capacitación, lo que eleva la barrera para los potenciales atacantes. Además, Ecuador colabora activamente con organismos internacionales (OEA, Interpol) en materia de ciberseguridad, lo que le permite apoyarse en una red global para prevenir y responder a incidentes. Por ejemplo, la adhesión al Convenio de Budapest y la participación en simulacros regionales de ciberataques fortalecen la resiliencia nacional.

Otro factor atenuante es que, a diferencia de otras regiones, en Ecuador no existen grupos terroristas domésticos conocidos con plataformas digitales sofisticadas. Si bien hay grupos radicales, ninguno ha declarado una guerra cibernética abierta contra el Estado. Esto significa que el principal origen del riesgo ciberterrorista proviene de individuos o colectivos sueltos, más que de organizaciones terroristas establecidas. Esta dispersión puede limitar la capacidad de daño coordinado a gran escala. No es lo mismo enfrentar a un *lone wolf*[3]digital

[3] Persona que prefiere trabajar, actuar o vivir sola

que a una estructura terrorista con financiación y mando jerárquico dedicando recursos al ciberespacio. Por ahora, los incidentes en Ecuador, aunque serios, han sido reactivos o puntuales y no parte de una campaña sostenida de terror cibernético.

El tejido social ecuatoriano también cuenta con características que podrían frenar la radicalización digital: la penetración de Internet, aunque en aumento, aún deja fuera a una porción de la población, especialmente en zonas rurales, reduciendo la base desde la cual podrían reclutarse masivamente ciberterroristas internos. Asimismo, el debate público en redes ha generado una activa comunidad de expertos y periodistas digitales que rápidamente exponen noticias de ataques y piden cuentas a autoridades, creando presión para reforzar defensas. Esta visibilidad actúa como elemento disuasorio, ya que un potencial atacante sabe que un incidente mayor provocará investigaciones exhaustivas con apoyo internacional.

ESTADÍSTICAS DEL FENÓMENO DE LA CIBERDELINCUENCUENCIA

El *Terrorismo en la Red o Ciberterrorismo* como una forma de actuar del terrorismo, y que para el efecto utiliza el ciberespacio, como una zona sin censura donde espacios como la deepweb, darknet, entre otros, favorecen el cometimiento de actividades ilícitas como tráfico

ilícito de armas, tráfico ilícito de sustancias catalogadas sujetas a fiscalización, asociación ilícita, ataque a bienes protegidos entre otras, permitiendo que el terrorismo siga incrementando sus tentáculos y sus capacidades de acción.

Estadísticas de delitos relacionados con el terrorismo en Ecuador

Si bien en muchos casos las acciones terroristas no se ejecutan exclusivamente en el ciberespacio, este constituye un entorno propicio para facilitar, planificar o encubrir operaciones de carácter violento, incluyendo la adquisición ilícita de armas, el financiamiento mediante criptomonedas o el tráfico transfronterizo de información sensible. En este sentido, el Ciberterrorismo se articula como un componente transversal que puede potenciar otras tipologías delictivas relacionadas con las economías criminales, tales como el lavado de activos, el tráfico ilícito de armas o incluso el tráfico de migrantes, al proveer canales digitales de comunicación, coordinación y ocultamiento.

Los registros estadísticos disponibles en torno a denuncias e incidentes vinculados a la actividad terrorista en entornos digitales, aunque limitados, constituyen un insumo clave para dimensionar el grado de exposición del país frente a este tipo de amenazas. Su análisis no solo permite identificar tendencias de infiltración del terrorismo en el ciberespacio, sino también fortalecer los mecanismos de prevención, cooperación internacional y respuesta integral, dentro de un esquema de seguridad multidimensional

Tabla 3

Noticias del Delito relacionadas con el terrorismo (agosto 2025)

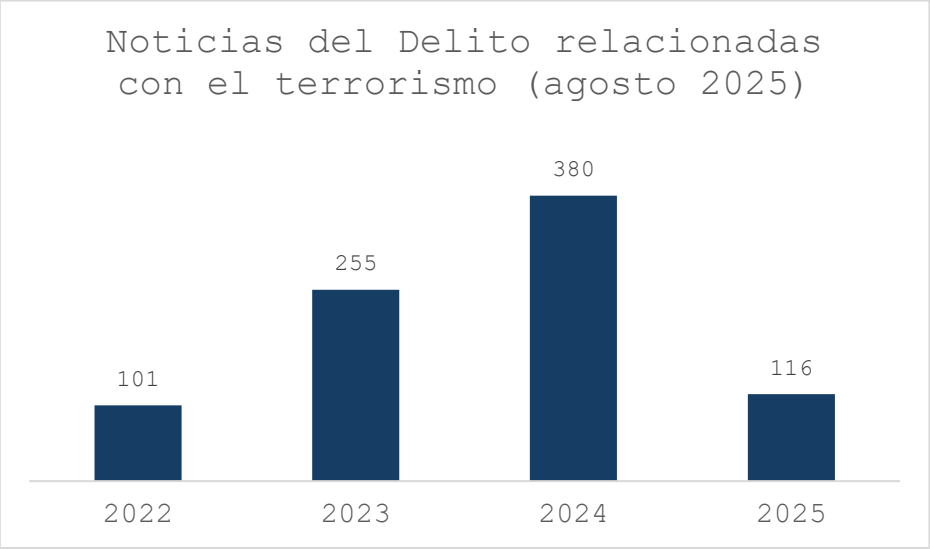
Año	2022	2023	2024	2025[4]	Total
Terrorismo	100	254	379	116	849
Financiamiento al Terrorismo	1	1	1	0	3
Total	101	255	380	116	852

Nota: *Fuente Fiscalía General del Estado*

[4] agosto 2025

Figura 2

Noticias del Delito relacionadas con el terrorismo



Nota: *Fuente Fiscalía General del Estado*

CONCLUSIONES

- Se puede identificar que el terrorismo en la red es un problema complejo y multifacético con graves consecuencias para la seguridad nacional y la gobernabilidad, que requiere de una respuesta integral que aborde tanto los aspectos técnicos como los sociales y políticos, con énfasis en la cooperación internacional, la protección de las libertades civiles y la promoción de la resiliencia comunitaria.
- Los componentes psicológicos del ciberterrorista ecuatoriano combinan motivaciones fuertes (económicas o ideológicas), con rasgos de personalidad que facilitan la comisión de delitos tecnológicos: sentimiento de poder, desafío a la autoridad, racionalización del daño y necesidad de validación por la comunidad hacker. Abordar el fenómeno requiere no solo medidas técnicas y legales, sino también comprensión psicológica para labores de profiling (perfilamiento) y programas de disuasión, por ejemplo, ofreciendo cauces positivos a jóvenes talentosos en computación para que no sean cooptados por la ciberdelincuencia.
- El contexto sociopolítico ecuatoriano presenta una dualidad frente al riesgo de ciberterrorismo: por un lado, la polarización, los conflictos sociales y la incursión del crimen organizado crean caldo de cultivo para motivaciones de ataque; por otro, la respuesta del Estado y la sociedad –aún incipiente pero creciente– en materia de ciberseguridad ofrece contención. El país se encuentra en una carrera para cerrar brechas antes de que adversarios más organizados las exploten. La estabilidad política y la reducción de la confrontación interna también contribuirían a disminuir el incentivo de ciertos actores para recurrir a medidas extremas en el ciberespacio. En definitiva, fortalecer la cohesión social y la institucionalidad, junto con las capacidades

técnicas de ciberdefensa, son las mejores estrategias para que Ecuador no solo reaccione sino prevenga escenarios de ciberterrorismo en el futuro inmediato.

BIBLIOGRAFÍA

Aldada, A. &. (2022). Cyberterrorism: Methods Objectives and Coping Mechanisms. *World Research of Political Science Journal*, 153-162.

Arias, R., & Luis, M. (1 de abril de 2023). *EL TERRORISMO Y SU TRANSFORMACIÓN*. Obtenido de Revista Academia de Guerra del Ejército Ecuatoriano, Volumen 16. Núm. 1, abril 2023: https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://journal.espe.edu.ec/ojs/index.php/Academia-de-guerra/article/download/2938/2404&ved=2ahUKEwiU0eHbqueOAxXVSzABHXItAdgQ-tANegQIKRAO&usg=AOvVaw15pNdoaejP3gpMW5e77ZFR

Asman, P. (02 de julio de 2025). *Hackeo del Cartel de Sinaloa al FBI revela grietas en la seguridad*. Obtenido de https://insightcrime.org/es/noticias/hackeo-del-cartel-de-sinaloa-al-fbi-revela-grietas-en-la-seguridad/#:~:text=Hackeo%20del%20Cartel%20de%20Sinaloa,Federal%20Bureau%20of

Baltazar, E. (04 de noviembre de 2018). *Narcos y hackers, cómo funciona esta nueva alianza delictiva que crece en la oscuridad*. Obtenido de https://www.infobae.com/america/mexico/2018/11/02/narcos-y-hackers-como-funciona-esta-nueva-alianza-delictiva-que-crece-en-la-oscuridad/#:~:text=Narcos%20y%20hackers%2C%20c%C3%B3mo%20funciona,para%20el%20delito%20como

Bishmanov, K. M. (2024). Analysis of modern types of cyberterrorism and methods of countering them. *Revista d'Internet, Dret i Política*, 41.

Breen, G. M. (2008). Examining existing counter-terrorism tactics and applying social network theory to fight cyberterrorism: An interpersonal communication perspective. *Journal of Applied Security Research*, 191-204.

Brooks, L. (31 de Julio de 2025). *Far-right extremists using games platforms to radicalise teenagers, report warns*. Obtenido de The guardian.

Camargo, C. Q. (21 de Enero de 2020). *YouTube's algorithms might radicalise people – but the real problem is we've no idea how they work.* Obtenido de http://theconversation.com/youtubes-algorithms-might-radicalise-people-but-the-real-problem-is-weve-no-idea-how-they-work-129955

Candan, B. (17 de octubre de 2024). *Top 5 critical infrastructure cyberattacks*. Obtenido de https://www-anapaya-net.translate.goog/blog/top-5-critical-infrastructure-cyberattacks?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc

Capitol, U. (3 de Enero de 2025). Obtenido de Emerging Threats to Critical Infrastructure: AI Driven Cybersecurity Trends for 2025: https://www.captechu.edu/blog/ai-driven-cybersecurity-trends-2025

CheckPoint. (2025). *El daño potencial de WannaCry*. Obtenido de CheckPoint: https://www.checkpoint.com/es/cyber-hub/threat-prevention/ransomware/wannacry-ransomware/

CISA. (2021). *Cyber-Attack Against Ukrainian Critical Infrastructure*. Obtenido de Cybersecurity & Infrastructure Security Agency (CISA): https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01

CISA. (2024). *IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including US Water and Wastewater Systems Facilities.* Washington, D.C.: Cybersecurity & Infrastructure Security Agency (CISA), Departamento de Seguridad Nacional de los Estados Unidos (DHS).

CISA. (2024). *IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including US Water and Wastewater Systems Facilities*. Obtenido de Cybersecurity & Infrastructure Security Agency (CISA): https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-335a

Cloudflare. (2025). *¿Qué son Petya y NotPetya?* Obtenido de Cloudflare: https://www.cloudflare.com/es-es/learning/security/ransomware/petya-notpetya-ransomware/

Council of Europe. (07 de 2007). *Recomendación del Comité de Ministros a los Estados miembros sobre proyectos de vida para menores migrantes no acompañados.*

Obtenido de Conferencia internacional celebrada por el Consejo de Europa sobre la cuestión del terrorismo

Criollo, E., Flores, C., Flores, C., Santacruz, J., & Ron, M. (2023). Diagnóstico y línea base de los activos. *Pro Sciences: Revista De Producción, Ciencias E Investigación*, 101-119. Obtenido de https://journalprosciences.com/index.php/ps/article/view/674/719

Cybersecurity, S. (2024). *Stuxnet: El Malware que Destruyó una Planta Nuclear*. Obtenido de Malware: https://books.spartan-cybersec.com/malware/los-malwares-mas-impactantes-de-la-historia/stuxnet-el-malware-que-destruyo-una-planta-nuclear

Darkdata. (2023). *Amenazas Híbridas: Implicaciones para la Ciberseguridad y la Ciberinteligencia.* Obtenido de https://www.darkdata.es/amenazas-hibridas-implicaciones-para-la-ciberseguridad-y-la-ciberinteligencia/

Denning, D. (mayo de 2020). *Reconceptualizing online offenses: A framework for distinguishing cybercrime, cyberattacks, and cyberterrorism in the Indian legal context - ScienceDirect.* Obtenido de https://irp.fas.org/congress/2000_hr/00-05-23denning.htm

Departamento de Seguridad Nacional de los Estados Unidos. (2025). *Homeland Threat Assessment.* Obtenido de DHS: https://www.dhs.gov/sites/default/files/2024-10/24_0930_ia_24-320-ia-publication-2025-hta-final-30sep24-508.pdf

Diaz, R., & Núñez, G. (2023). *Ciberataques a la logística y la infraestructura crítica en América Latina y el Caribe.* Comisión Económica para América Latina y el Caribe (CEPAL). Santiago: Documentos de Proyectos (LC/TS.2023/93).

ESPE. (2024). *El ciberterrorismo y la seguridad nacional. Academia de Guerra de la ESPE.* Obtenido de https://journal.espe.edu.ec/ojs/index.php/Academia-de-guerra/article/download/3373/2665/13811.

Fernández, I. N. (2018). La letalidad del ciberterrorismo. *Revista General de Marina*.

Fortinet. (2025). *¿Qué es el ransomware WannaCry? ¿Todavía existe WannaCry?* Obtenido de Fortinet: https://www.fortinet.com/lat/resources/cyberglossary/wannacry-ransomware-attack

IBM. (16 de Abril de 2025). Obtenido de IBM X-Force 2025 Threat Intelligence Index: https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/2025-threat-intelligence-index

ICE. (12 de March de 2025). *Terrorism and national security threats*. Obtenido de https://www-ice-gov.translate.goog/about-ice/hsi/investigate/terrorism-national-security-threats?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=sge#:~:text=Terrorism%20and%20threats%20against%20national,innovations%20and%20other%20sensitive%20materials.

ICE EEUU, S. d. (Febrero de 2025). *Terrorism and National Security Threats.* Obtenido de https://www-ice-gov.translate.goog/about-ice/hsi/investigate/terrorism-national-security-threats?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=sge#:~:text=Terrorism%20and%20threats%20against

Iftikhar, S. (2024). Cyberterrorism as a global threat: a review on repercussions and countermeasures. *PeerJ Computer Science*.

Incibe. (2024). *Ciberataque a Transport for London*. Obtenido de Incibe: https://www.incibe.es/incibe-cert/publicaciones/bitacora-de-seguridad/ciberataque-transport-London

Infoem. (2020). *El cibercrimen: fenomenología y criminología de la delincuencia en el ciberespacio.* Obtenido de https://www.infoem.org.mx/doc/biblioteca/accesoytrans/ciberdelitos/el-cibercrimen.pdf.

Intelligence, Mordor. (02 de 2018). *Lucha contra el ciberterrorismo Tamaño del mercado y análisis de acciones - Informe de investigación de la industria - Tendencias de crecimiento.* Obtenido de https://www.mordorintelligence.com/es/industry-reports/counter-cyberterrorism-trends-challenges

Intelligence, Mordor. (2019). *https://www.mordorintelligence.com/es/industry-reports/cyber-warfare-market.* Obtenido de https://www.mordorintelligence.com/es/industry-reports/cyber-warfare-market

Interpol. (n.d). *Terrorismo*. Obtenido de https://www.interpol.int/es/Delitos/Terrorismo

Jordán, J. (17 de Febrary de 2025). *Qué es el terrorismo | Global Strategy. Global Strategy.* Obtenido de https://global-strategy.org/que-es-terrorismo/#:~:text=Los%20terroristas%20tratan%20de%20generar%20un%20clima,intentan%20promover%20la%20divisi%C3%B3n%20y%20la%20desc

Kaspersky. (2025). *¿Qué es el ransomware WannaCry?* Obtenido de Kaspersky: https://www.kaspersky.es/resource-center/threats/ransomware-wannacry?srsltid=AfmBOorZQoFQC4Kk0fdNF0zrPa8A1yUX4rmOYJfc2aGNpCBVOQeR3PYk

Kaspersky. (2025). *Stuxnet explicó: qué es, quién lo creó y cómo funciona*. Obtenido de Kaspersky: https://latam.kaspersky.com/resource-center/definitions/what-is-stuxnet?srsltid=AfmBOooBcrzMacCbMJLfARlAQkjLgRHvmdgvCenphq7diEIgZMDFeajF

Lameiras, A. (2022). *Industroyer: una amenaza cibernética que derribó una red eléctrica*. Obtenido de WeLiveSecurity: https://www.welivesecurity.com/la-es/2022/06/13/industroyer-amenaza-cibernetica-derribo-red-electrica/

Leicester, J. (13 de abril de 2025). *Via porn, gore and ultra-violence, extremist groups are sinking hooks online into the very young.* Obtenido de https://apnews.com/article/technology-parenting-terror-islamic-state-police-security-attacks-4888bab2d10502edadf787d419d45b5b

Lipovsky, R. (2016). *El troyano BlackEnergy ataca a una planta de energía eléctrica en Ucrania*. Obtenido de WeLiveSecurity: https://www.welivesecurity.com/la-es/2016/01/05/troyano-blackenergy-ataca-planta-energia-electrica-ucrania/

LISA. (s/f). *Hacktivismo*. Obtenido de https://www.lisainstitute.com/blogs/blog/hacktivismo-definicion-tipos-modus-operandi-motivaciones

Maldonado, A. (Febrero de 2024). *EVALUACIÓN DE LAS AMENAZAS Y RIESGOS*. Obtenido de lex Maldonado Viera,: https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://journal.espe.edu.ec/ojs/index.php/revista-ademic/article/download/3427/2631/13606

Malwarebytes. (2025). *Los ransomware Petya y NotPetya*. Obtenido de Malwarebytes: https://www.malwarebytes.com/es/petya-and-notpetya

Martinez, A. (abril de 2024). *Desafíos de la ciberseguridad en infraestructuras críticas*. Obtenido de https://itahora.com/amp/2024/04/19/desafios-de-la-ciberseguridad-en-infraestructuras-criticas/

Mayorga, J., & Holguín, R. (1 de abril de 2024). *LAS REDES SOCIALES COMO INSTRUMENTO DEL*. Obtenido de Revista Academia de Guerra del Ejército Ecuatoriano, Volumen 17. Núm. 1 abril 2024: https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://journal.espe.edu.ec/ojs/index.php/Academia-de-guerra/article/download/3401/2668/13823&ved=2ahUKEwio8bqs3ueOAxX7SDABHfJ4FF4QFnoECBYQAw&usg=AOvVaw14inMil-rKo2K5JQ9E6-6q

Ministerio de Defensa. (2019). *Plan Especifico de Defensa 2019-2030.* Quito: Instituto Geográfico Militar.

MINTEL. (2021). *Política de Ciberseguridad.* Obtenido de https://www.telecomunicaciones.gob.ec/wp-content/uploads/2021/06/Acuerdo-No.-006-2021-Politica-de-Ciberseguridad.pdf

Moore, M. (2025). *Top Cybersecurity Threats to Watch in 2025*. Obtenido de University of San Diego : https://onlinedegrees.sandiego.edu/top-cyber-security-threats/

Naciones Unidas. (n.d.). *Lucha contra el terrorismo | Naciones Unidas*. Obtenido de https://www.un.org/es/global-issues/countering-terrorism#:~:text=El%20terrorismo%2C%20en%20todas%20sus,libertades%20fundamentales%20y%20la%20democracia.

ONU, N. (28 de Octubre de 2022). *El Comité contra el Terrorismo apoya el uso de las nuevas tecnologías para combatir esa lacra.* Obtenido de https://news.un.org/es/interview/2022/10/1516452#:~:text=La%20experiencia%20ha%20demostrado%20que,de%20lucha%20contra%20el%20t

Paredes, M., & Semanate, A. (abril de 2024). *EL CIBERTERRORISMO Y LA SEGURIDAD NACIONAL*. Obtenido de Revista Academia de Guerra del Ejército Ecuatoriano, Volumen 17. Núm. 1: https://journal.espe.edu.ec/ojs/index.php/Academia-de-

guerra/article/download/3373/2665/13811&ved=2ahUKEwjcoMPbqueOAxWHQzABHfPPDhQQFnoECB4QAQ&usg=AOvVaw2FA8roQ-6DuIP-hhCV-0cZ

Proofpoint. (2025). *Petya (NotPetya)*. Obtenido de Proofpoint: https://www.proofpoint.com/es/threat-reference/petya

Reuters. (27 de junio de 2025). *Cártel de Sinaloa usó cámaras de vigilancia para hallar informantes del FBI: gobierno EU* . Obtenido de https://www.milenio.com/policia/cartel-sinaloa-uso-datos-telefonicos-para-hallar-informantes-fbi#:~:text=FBI%20www,el%20informe%2C%20el%20hacker

Ribeiro, A. (28 de Agosto de 2024). *Critical infrastructure faces 30 percent surge in cyber attacks, KnowBe4 report highlights. Industrial Cyber*. Obtenido de https://industrialcyber.co/critical-infrastructure/critical-infrastructure-faces-30-percent-surge-in-cyber-attacks-knowbe4-report-highlights/

Rollins, J., & Wilson, C. (Enero de 2007). *Terrorist Capabilities for Cyberattack: Overview and Policy Issues.* Obtenido de https://nsarchive.gwu.edu/document/21420-document-24

Scroxton, A. (2024). *TfL cyber attack cost over £30m to date*. Obtenido de Computer Weekly: https://www.computerweekly.com/news/366616875/TfL-cyber-attack-cost-over-30m-to-date

Sellman, M. (26 de Junio de 2025). *The Times*. Obtenido de New online laws fail to stop promotion of terror groups. : https://www.thetimes.com/uk/crime/article/new-online-laws-fail-to-stop-promotion-of-terror-groups-m92g2fcxb

SentinelOne. (30 de Julio de 2025). *Key Cyber Security Statistics for 2025*. Obtenido de Key Cyber Security Statistics for 2025: https://www.sentinelone.com/cybersecurity-101/cybersecurity/cyber-security-statistics/

Torres , A. (Marzo de 2022). Obtenido de https://www.primicias.ec/noticias/en-exclusiva/hacker-sombrero-negro-escapo-justicia-ciberdelitos-ecuador/

UNAH. (2021). *Ciberterrorismo y Hacktivismo*. Obtenido de https://blogs.unah.edu.hn/csirt/ciberterrorismo-y-hacktivismo/

Vasquez, C., & Vicens, A. (2023). *Pennsylvania water facility hit by Iran-linked hackers*. Obtenido de CyberScoop: https://cyberscoop.com/pennsylvania-water-facility-hack-iran/

Vishnoi, A. (11 de Mayo de 2025). *Since Pahalgam terror attack on 22nd April, India is thwarting nearly 30-40 cyber attacks daily.* Obtenido de Economic Times: https://economictimes.indiatimes.com/news/india/since-pahalgam-terror-attack-on-22nd-april-india-is-thwarting-nearly-30-40-cyber-attacks-daily/articleshow/121064570.cms

Yunos, Z., Mohd, N., Ariffin, A., & Ahmad, R. (2017). Understanding Cyber Terrorism From Motivational Perspectives: A Qualitative Data Analysis. *University Technical Malaysia Melaka*.