EL TERRORISMO Y SU TRANSFORMACIÓN

Tcrn. de E.M. Richard Paúl Arias Tapia [1]
Mayo. de C.B. Luis Santiago Manzano Terán [2]

Resumen

La aparición de la Internet marcó un antes y un después en el modo cómo las personas acceden a los sistemas de información, donde cada acto se encuentra reflejado, pues "la red es un nuevo espacio donde los roles de los diferentes actores se construyen, evolucionan y cambian constantemente". Además, con el desarrollo acelerado de la Internet también emerge el lado oscuro y surgen nuevos términos como cibercrimen, ciberdelito, ciberterrorismo, que describen de forma genérica los aspectos ilícitos cometidos en el ciberespacio. El objetivo de la presente investigación es analizar el concepto de ciberterrorismo, que ha evolucionado como amenaza híbrida, partiendo de una variante del terrorismo que permita describir la gobernanza actual del Ecuador en ciberseguridad y la respuesta de los Estados ante esta amenaza, enmarcada en los parámetros de la sociedad global que, al igual que otras amenazas, es una preocupación mundial ocupando un lugar importante en la agenda local e internacional.

Palabras clave: Amenazas Híbridas, Ciberespacio, Ciberterrorismo, Ciberseguridad.

Abstract

The appearance of the internet marked a before and after in the way people access information systems, where each act is reflected, since "the network is a new space where the roles of the different actors are built, evolve and they're constantly changing." In addition, with the accelerated development of the Internet, the dark side also emerges and new terms such as cybercrime, cybercrime, and cyberterrorism appear, which generically describe the illegal aspects committed in cyberspace. The objective of this research is to analyze the concept of cyberterrorism, which has evolved as a hybrid threat, based on a variant of terrorism, which allows describing the current governance of Ecuador in cybersecurity and the response of the States to this threat, framed in the parameters of the global society that, like other threats, is a global concern occupying an important place on the local and international agenda.

Keywords: Hybrid Threats, Cyberspace, Cyberterrorism, Cybersecurity.

[1] Ejército ecuatoriano - Magister en Ciencias en Sistemas y Computación en el IME Instituto Militar de Ingeniería Brasil - rpat1123@yahoo.com
[2] Ejército ecuatoriano - Master en Gerencia en Seguridad y Riesgos en la UFA ESPE - santiagomanzanoteran@hotmail.com

DOI: https://dx.doi.org/10.24133/RCSD.VOL16.N01.2023.10
Revista Academia de Guerra del Ejército Ecuatoriano, Volumen 16. Núm. 1, abril 2023. pp. 134 - 146

Introducción

El ciberterrorismo, como amenaza en permanente desarrollo, es uno de los mayores problemas para muchos gobiernos del mundo moderno, no solo por el empleo del internet y de las TIC, sino por lograr el rompimiento de barreras tradicionales de ataque como el campo físico y la construcción de impacto masivo en tan corto tiempo. Por lo que el objetivo de la presente investigación es analizar el concepto de ciberterrorismo, que ha evolucionado como amenaza híbrida, partiendo de una variante del terrorismo, así como la gobernanza actual del Ecuador referente a la ciberseguridad, enmarcada en los parámetros de la sociedad internacional.

La metodología empleada en este trabajo es descriptiva con un enfoque de carácter cualitativo donde se han analizado varios hechos, documentos e información a través de varias técnicas para la recolección de datos, como las fuentes secundarias (recolección documental y bibliografía), aquellas que han obtenido información de otra fuente y la han sometido a un proceso de reestructuración, análisis y crítica.

La primera parte de este trabajo analiza algunos conceptos, proporcionando un aporte doctrinario sobre cómo el ciberterrorismo forma parte de la gran transformación del ciberespacio, permitiendo que tanto la delincuencia común como los grupos terroristas hayan trasladado gran parte de sus operaciones a las nuevas TIC's.

En una segunda parte se analizarán las tendencias actuales en las cuales se puede mencionar la evolución de dos elementos diferenciadores: los ciberataques y la guerra de la información.

En la tercera parte se examina la dinámica del ciberterrorismo en la web como una faceta del terrorismo que combina varias tácticas del pasado con las nuevas tecnologías y con el avance actual, en un mundo sistematizado, esa combinación se enfoca en explotar las vulnerabilidades de la infraestructura crítica de una nación.

La cuarta parte de este trabajo describe la respuesta de los Estados ante el ciberterrorismo, que al igual que otras amenazas, es una preocupación a nivel global, por lo que ocupa un lugar importante en la agenda internacional de los países y sin lugar a duda en el Ecuador también, y que en cooperación con organizaciones internacionales enfocan sus esfuerzos para combatir esta amenaza por medio de la ciberseguridad.

En la parte final estarán las conclusiones que buscan sintetizar el trabajo de investigación, destacando cómo la comunidad internacional unifica esfuerzos para enfrentar al ciberterrorismo, buscando nuevas formas de operar dentro de la web, generando una dinámica evolutiva mutua en donde la carrera por adquirir tecnología y desarrollar mayores capacidades tecnológicas hacen la diferencia.

Por lo expuesto anteriormente se han considerado las siguientes hipótesis:

- La conceptualización del ciberterrorismo es difícil de establecer, ya que por sus particularidades y su constante evolución, varía en referencia a contextos y motivación, lo que dificulta aún más al adoptar la característica de hibridez.
- El ciberterrorismo como amenaza híbrida, cuenta con los recursos necesarios y está a la par con los avances tecnológicos, por lo que puede modificar su modus operandi, al igual que la dinámica funcional dentro de la red, ocultándose en sus profundidades, adquiriendo una mayor flexibilidad que la hacen difícil de contrarrestar, seguir y localizar.
- La evolución del ciberterrorismo aún no ha finalizado ni lo hará en mucho tiempo, lo que supone que la cibercriminalidad continuará expandiéndose y evolucionando en las décadas venideras. Se ha debatido mucho sobre el origen, propósito y características que incluye, por ejemplo: actos sanguinarios, masivas campañas de *fakenews*, ciberataques contra estructuras críticas y la manipulación de las redes sociales.
- Para los Estados representa un verdadero reto enfrentar esta y otras amenazas híbridas que se ocultan en la web, ya que requiere de un gran esfuerzo en el desarrollo de capacidades e inversión de recursos para enfrentarlas y en su mayoría son gestionadas por la ciberseguridad.

1. ANÁLISIS DE CONCEPTOS

Actualmente, los diversos actores han dado a los conceptos relacionados con la seguridad y de otras áreas, cierta característica de hibridez con base a la tendencia mundial de emplear varias combinaciones de herramientas en diversos aspectos como; militar, civil/social, infraestructuras críticas, medios de comunicación, económico, político, normativo y ciberespacio, para alcanzar un objetivo determinado (Galán, 2018).

Según el Parlamento Europeo (2015), en el contexto de la práctica de protección de la seguridad nacional de los Estados y sus límites legales, es más preciso y adecuado utilizar las expresiones *amenaza híbrida* o *conflicto híbrido* que *guerra híbrida*. Esto debido a que las definiciones de amenazas híbridas varían y deben permanecer flexibles para responder a su naturaleza evolutiva, el concepto se dirige a capturar la mezcla de actividad coercitiva y subversiva, métodos convencionales y no convencionales (es decir, diplomáticos, militares, económicos, tecnológicos), que pueden ser utilizados de manera coordinada para lograr objetivos específicos mientras permanecen por debajo del umbral de una guerra declarada formalmente.

Tabla 1
Varios conceptos

Amenaza Híbrida	"Fenómeno resultante de la convergencia e interconexión de diferentes elementos que, en conjunto, constituyen una amenaza más compleja y multidimensional, Teniendo en cuenta los diferentes niveles de intensidad de la amenaza y la intencionalidad de los actores involucrados" (Pawlak, 2015).
Conflicto Híbrido	"Situación en la cual las partes se abstienen del uso abierto de la fuerza (armada) y actúan combinando la intimidación militar (sin llegar a un ataque convencional) y a la explotación de vulnerabilidades económicas, políticas, tecnológicas y diplomáticas o medios tecnológicos para perseguir sus objetivos" (Pawlak, 2015).
Guerra Híbrida	La amalgama de los diferentes tipos de guerra, abarcando capacidades convencionales, tácticas irregulares, acciones terroristas, inducción de la violencia y coerción (Santos et al., 2019, p. 91).

Las amenazas híbridas pueden iniciar su proceso tanto de Estados como de actores no estatales y desarrollar formas de confrontación violentas y no violentas, como los actos terroristas de Al-Qaeda o Daesh, actos contra la ciberseguridad de los Estados o instituciones, acciones de grupos delictivos armados como los de los cárteles de la droga colombianos, disputas marítimas como las que se ubican en el mar de China Meridional, restricciones al uso del espacio, actos económicos hostiles como el bloqueo de las exportaciones japonesas por parte de China en 2010 (Council of Europa, 2018, p. 9).

Como conflicto híbrido podemos destacar los *little green men* en Ucrania, el ataque a los servidores de correo electrónico del Comité Nacional Demócrata de los Estados Unidos, los cuales buscan alcanzar sus objetivos estratégicos incidiendo en la toma de decisiones de sus víctimas y socavando sus valores, su estructura social y la confianza de la población (Fly et al., 2018).

El término "Guerra Híbrida" fue acuñado por el Dr. Frank Hoffman y fue considerado por la OTAN a inicios de la década del 2000, enmarcando una combinación entre la guerra convencional[1] y no convencional, actuando de tal forma que puedan eludir responsabilidades en el no cumplimiento de las normas establecidas para la guerra, de esta forma también se incluyen operaciones cibernéticas y electromagnéticas, la interrupción y el sabotaje, como en el caso de los combatientes islamistas en Irak y Siria, que emplearon las redes sociales para reclutar combatientes, desacreditar a los gobiernos, difundir su terrorismo y transmitir disposiciones a otros terroristas (Johnson, 2018, p. 141).

El crecimiento de la guerra híbrida ha sido impulsado por el surgimiento de diversos actores, modernos tipos de armas y una innovadora imagen ideológica, a diferencia de la definición de amenaza híbrida que está dirigida para situaciones en las que los Estados o actores no estatales emplean instrumentos de guerra y los integran con la aplicación de la fuerza armada o de la amenaza (Da Silva, 2020, p. 25).

Generalmente, los protagonistas de las acciones hibridas no aceptan su responsabilidad en las operaciones y evaden las consecuencias jurídicas de sus acciones valiéndose del complejo ordenamiento jurídico y sus vacíos, circundando los límites legales, operando en espacios no regulados, posibilitando la ejecución de acciones difíciles de perseguir por la vía legal y que producen todo el desorden e imprecisión para disimular sus acciones. Este argumento no significa que exista un vacío legal, sino que es compleja la aplicación de la legislación nacional o internacional respectiva, incluido el DIH[2], hacia los actores de las amenazas hibridas (Casalunga & Pinheiro, 2019, p. 3).

El veloz desarrollo tecnológico ha motivado el surgimiento de un nuevo dominio; el ciberespacio, en el cual las reglas de juego a nivel local y mundial aún no están claramente establecidas. No es lo adecuado considerar al ciberespacio como un territorio con límites y fronteras, sino como un campo operacional, un espacio de batalla, un dominio que representa un desafío incierto en relación a la idea clásica de seguridad (Ignacio, 2022, p. 88).

La digitalización de la sociedad, la forma en la que se produce y se introduce la información, el uso masivo de las redes sociales y la aparición de nuevos autores de opinión, la velocidad para propagarse por todo el mundo y la manera cómo se accede a la misma traspasando límites han evidenciado la necesidad de tomar en consideración la cultura, tradición, pensamientos, políticas y concepción de entender la vida en aquel lugar, porque la información que se produce en una ciudad puede interpretarse de maneras muy diferentes en otros sitios. Internet se ha transformado en un nuevo espacio de batalla donde las reglas aún se están manifestando, las noticias falsas, la desinformación y los hechos basados en opiniones alborotan el dominio público. El resultado es que uno de los pilares fundamentales de las

1 Acciones armadas no encubiertas
2 Derecho Internacional Humanitario

sociedades, como lo es la confianza, se está desgastando (Hernández, 2017, p. 63).

La Internet es interpretada por estos grupos como un medio que facilita la consecución de sus objetivos a menor coste y con mayor anonimato, evidenciando la existencia de procesos inteligentes y adaptativos destinados a la captación y radicalización de adeptos, haciendo uso de la propaganda como medio para conquistar las voluntades de las personas, utilizando la persuasión y la manipulación necesaria para producir un cambio en las creencias y en la ideología de los individuos. En consecuencia, la guerra de la información en el ciberespacio se proyecta mediante la ejecución de acciones con el objetivo de mantener la integridad de los sistemas de información, prevenir su destrucción por parte del enemigo y proporcionar información oportuna para lograr la victoria.

Gracias a la tecnología digital, el acceso a la información es más fácil y barato, su consumo ha tenido un crecimiento sin precedentes. Esto ha facilitado el incremento de los intermediarios online en un marco regulatorio que no los hace responsables del control editorial ni de la mala conducta de sus usuarios, caracterizando frecuentemente a las noticias online por la falta de verificación de los hechos y escasa originalidad.

Producir y difundir desinformación es mucho más fácil y barato gracias a la disponibilidad de una gran infraestructura de plataformas digitales para el intercambio de información. Antiguamente, sólo los medios de comunicación con recursos suficientes podían llegar a las grandes audiencias, pero hoy en día se ha quebrantado la correlación entre la divulgación de noticias y los controles de calidad, resultando que cualquiera puede ser un editor con alcance global.

No hay motivos para esperar que las plataformas digitales renuncien a la desinformación mientras las noticias falsas generen tráfico y dinero, como por ejemplo la publicidad sin la contrapartida de la responsabilidad; no hay una razón sólida para esperar que las plataformas digitales tengan un incentivo para tomar decisiones contundentes y soluciones contra la desinformación. En consecuencia, la respuesta más efectiva a la desinformación en un mundo rico y lleno de información es la concientización y la alfabetización, como por ejemplo, mediante la ayuda de sistemas que simulen una inteligencia similar a la humana (inteligencia artificial).

Jalloul (2018) define al terrorismo como "una forma de criminalidad emprendida por una organización criminal cuyos objetivos son crear alarma social y dominación a través del terror, cometer actos de violencia contra la sociedad, y todo ello persiguiendo un fin determinado" y según Schmidt 2013, existen varios tipos de terrorismo de acuerdo a su objetivo (Cespedosa Rodríguez, 2019, p. 6).

Si bien el concepto de terrorismo no tiene una exactitud bien definida, el concepto de ciberterrorismo carga consigo esa característica, por lo que varios autores plantean diferentes definiciones, aunque acertadas, cada una presenta una característica y enfoque diferente sin llegar a un consenso (Tabla 2).

Tabla 2

Varios conceptos de Ciberterrorismo

Autor	*Concepto*	*Fuente*
Dr. Barry Collin	As a planned attack performed by terrorists on data and computer systems.	(Collin, 1997)
Marck M. Pollit	Es el ataque premeditado y políticamente motivado contra información, sistemas computacionales, programas de computadoras y datos que puedan resultar en violencia contra objetivos no combatientes por parte de grupos sub nacionales o agentes clandestinos.	(Pollitt, 1998, p. 9)
Dorothy E. Denning	Es la convergencia entre terrorismo y ciberespacio […]. Para calificar como ciberterrorismo, un ataque debe ocasionar violencia contra personas o contra la propiedad, o al menos causar el daño suficiente como para generar miedo. Ataques que deriven en muertes o personas heridas, explosiones, choques de aviones, contaminación de agua o severas pérdidas económicas pueden servir de ejemplo.	(Denning, 2000)
Orta Martínez	Convergencia del ciberespacio y el terrorismo.	(Martínez, 2005)
Alicia Chicharro	Forma de terrorismo que emplea las tecnologías de la información y la comunicación para intimidar, coaccionar o causar daños a la población, a los gobiernos o a las organizaciones internacionales, con el fin de lograr sus objetivos políticos.	(Chicharro, 2013)

Existen muchos otros conceptos que no están lejos de la realidad de lo que engloba el ciberterrorismo, pero que cada uno guarda relación entre sí, por ejemplo: se originan por grupos terroristas, emplean las TIC´s como herramientas para aplicar técnicas violentas, buscan un objetivo político, buscan sembrar miedo, intimidar a un estado y sus ciudadanos para imponer su voluntad.

Bajo este contexto y de acuerdo al análisis realizado de los diferentes conceptos, se ha determinado doctrinariamente que el ciberterrorismo forma parte de la gran transformación del ciberespacio, permitiendo que tanto la delincuencia común como los grupos terroristas hayan trasladado gran parte de sus operaciones a las nuevas Tecnologías de la Información y Comunicaciones, usando ampliamente la Internet debido a las características intrínsecas que posee el ciberespacio, como la instantaneidad, el anonimato y el fácil acceso, lo que implica una enorme dificultad para defenderse o prevenir este tipo de amenaza híbrida.

2. LAS NUEVAS TENDENCIAS DEL CIBERTERRORISMO

Hoy en día se puede mencionar la evolución de dos elementos diferenciadores: los ciberataques y la guerra de la información. Para los ciberataques, como se conoce en los últimos tiempos, varios países como Alemania, Estados Unidos, Estonia, Finlandia, Georgia, Holanda, Lituania, Reino Unido o Ucrania han denunciado haber sido víctimas de ciberataques rusos. Algunos países europeos, como medidas reactivas, han aprobado leyes antiterroristas que pueden utilizarse contra tales amenazas, sin embargo, algunas de estas respuestas podrían llegar a violar los derechos humanos y originan dudas sobre su compatibilidad con la libertad de expresión. Se debe tener siempre presente que las amenazas híbridas tienen como propósito fundamental alcanzar sus objetivos sin recurrir a la guerra real, enfrentando sociedades y no ejércitos, con lo que se desploma casi íntegramente la distinción entre combatientes y ciudadanos (Pawlak, 2015).

En lo referente a la guerra de la información se relaciona al "conflicto entre dos o más grupos en el ámbito de la información" que pretende imponer un punto de vista específico a un determinado auditorio. Se trata de una combinación de guerra electrónica y operaciones psicológicas cuyo objetivo es degradar la moral y el bienestar de los ciudadanos de una nación difundiendo, por lo común, información falsa a través de redes sociales y medios de comunicación. Estas campañas de desinformación tienen más éxito en regiones que ya son inestables (Porche et al., 2013).

Últimamente han venido apareciendo los denominados *online trolls*, agentes de desinformación, que son personas y actores no estatales que expresan opiniones afines a la agenda política de un Estado en particular y crean una zona gris en la que es muy difícil distinguir dónde situar la frontera entre la libertad de expresión de los activistas y la injerencia en el Estado victima (Amnesty International, 2017).

El nuevo contexto geoestratégico relacionado principalmente a los problemas de estrategia y de seguridad nacional con los agentes geográficos, las TIC´s y las nuevas configuraciones estructurales mencionan que estas formas de agresión permanecerán y evolucionarán en el futuro.

Los grupos terroristas buscan difundir el pánico y miedo hacia todas las personas que no piensan como ellos, captando adeptos para mantener viva la lucha en todas sus vertientes. Se aseguran de que los atentados queden grabados para luego poder difundirlos por los medios de comunicación, tanto para el público en general como para aquellos adeptos a los que pretendían que se alistasen en sus filas. Indudablemente todo evoluciona con el paso del tiempo y aunque el mensaje es el mismo, la difusión ha mejorado de una manera alarmante. Anteriormente, la propaganda se distribuía de manera clandestina por los reclutadores mediante el contacto personal entre los mismos e individuos a los que se pretendía captar. La participación de los medios de comunicación en estas actividades era prácticamente nula y solo daban voz a las organizaciones terroristas cuando se cometían atentados con graves consecuencias y durante los días siguientes, posteriormente caían en el olvido (Akhgar, 2014, p. 12).

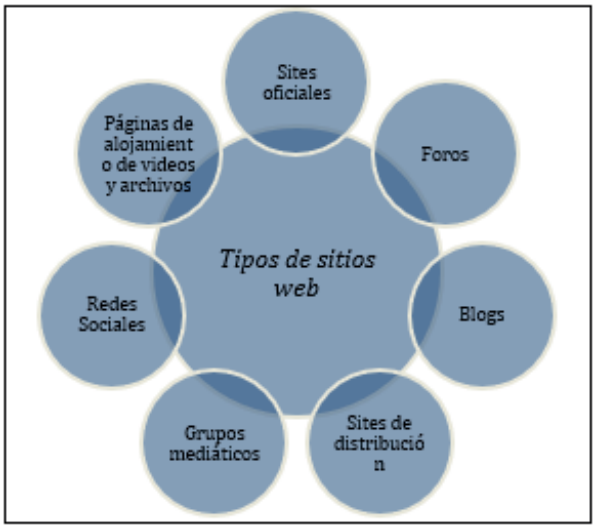
Actualmente todo ha cambiado con el aparecimiento de las nuevas tecnologías, se puede consumir propaganda, ejecuciones, videos de atentados y cualquier información promovida contra los denominados infieles, desde cualquier lugar del mundo con un teléfono móvil u otro dispositivo. Este suceso hace que cambien totalmente las reglas del juego y solo con un "click", el mensaje puede llegar a millones de personas en cuestión de segundos y a cualquier sitio (Akhar, 2014, p. 24).

El ciberterrorismo es una faceta del terrorismo que combina varias tácticas del pasado con las nuevas tecnologías y con el avance actual, en un mundo sistematizado, esa combinación se enfoca en explotar las vulnerabilidades de la infraestructura crítica de una nación[3], para lo cual debe estar motivado, disponer de recursos y deseos de causar daño (Cano, 2014, p. 2). Sea cual sea la razón (ideológica, económica o social) la motivación más importante es la motivación política, ante lo cual los grupos terroristas se desempañan en el interior de la *dark web*[4] (DW, por sus siglas en inglés) para comunicarse entre sí, promocionar sus actividades promoviendo su ideología y reclutar personas que contribuyan a sus intenciones (Alayda et al., 2021, p. 3002), cambiando constantemente de dirección sumergiéndose por varios tipos de sitios web (Figura 1).

3 Infraestructuras críticas de una nación: energía eléctrica, producción, almacenamiento y suministro de gas y petróleo, telecomunicaciones, bancos y finanzas, sistemas de suministro de agua, transporte, servicios de emergencia y operaciones gubernamentales, aquellos sistemas que hacen parte de la dinámica de la economía de un país y el bienestar de los ciudadanos.

4 Páginas, foros y comunidades que ocultan su contenido, es decir, no se puede acceder a estos sitios a través de medios convencionales.

Figura 1
Tipología de los sitios web utilizados por los grupos terroristas



El ciberterrorismo ofrece algunas ventajas en el momento de la realización de los ciberataques ya que los riesgos al emplear el ciberespacio son menores a los métodos anteriores, un ciberataque puede ser perpetrado desde la comodidad de su hogar, desde cualquier lugar del mundo, limitando la utilización de explosivos o que tenga que suicidarse en la realización del ataque (Viegas, 2004, p. 5).

No se debe confundir el ciberterrorismo con el cibercrimen, ya que el ciberterrorismo es más severo que otras actividades que se realizan "en" o "a través" del ciberespacio (Mayer Lux, 2018, p. 12). El cibercrimen se define como cualquier comportamiento delictivo realizado en el ciberespacio, entendiendo además por el mismo el ámbito virtual de interacción y comunicación personal definido por el uso de las TIC, y dando cabida, por tanto, a conductas cuyo contenido ilícito es nuevo y se relaciona directamente con los nuevos intereses o bienes sociales existentes en el ciberespacio, así como también a comportamientos tradicionalmente ilícitos en los que únicamente cambia que ahora se llevan a cabo por medio de Internet (Llinares, 2012).

El ciberterrorismo es tratado como una amenaza transversal a partir del auge del Estado Islámico, adoptando un carácter polifacético, transformándolo en una amenaza híbrida que requiere la atención de todos los atores estatales y privados a tomar participación en las acciones necesarias para enfrentar esta amenaza (Demurtas, 2021, p. 105).

Sin embargo, ante el aumento exponencial de amenazas y riesgos en la web, varios Estados están desarrollando políticas que limitan la privacidad y la libertad en la misma en sus ciberterritorios, a cambio de una mayor garantía de seguridad. Con estas propuestas en beneficio de la seguridad se van minimizando los márgenes de libertad, que es la principal característica que había definido al ciberespacio. Pero sin embargo, se evidencia un aumento incontrolado y desmesurado de la propaganda terrorista (Lapayese, 2018, p. 206).

En la actualidad se destinan varios recursos, principalmente para implementar una serie de medidas importantes tendientes a combatir las actividades terroristas que se llevan a cabo en Internet a nivel global. Estas medidas representan la brecha prioritaria en materia de seguridad (Llinares, 2012, p. 145).

La propagación del terrorismo por medio de las redes representa la difícil situación de la sociedad, los conflictos tradicionales se desplazan en la red, el ciberespacio se ha establecido como la línea inicial de combate de los conflictos actuales. Los actores de seguridad y defensa de los Estados no sólo se enfrentan a escenarios tangibles, sino también a escenarios virtuales.

3. DINÁMICA DEL CIBERTERRORISMO EN LA WEB 2.0

Actualmente, el ciberespacio como escenario de enfrentamiento, permite publicar desde cualquier sitio, todo tipo de información como mensajes, ideologías radicales, proselitismo o lanzar un ciberataque y posteriormente, no dejar o borrar vestigios y huellas digitales dificultando que las autoridades puedan detenerlos.

El terrorismo se fundamenta en una lógica de confrontación de "no combate de modo directo con el oponente", sino a través de "métodos no convencionales de violencia", el ciberespacio se presenta como el medio más adecuado para llevar a cabo el combate asimétrico, en el cual los terroristas buscan el desgaste de quienes consideran enemigo.

El acceso ilimitado y sin control al ciberespacio se convierte en un elemento imprescindible para explicar porqué muchas organizaciones terroristas han apostado drásticamente por el uso de la red. "La extensión del terrorismo en el curso de los últimos decenios del siglo XX no obedece en consecuencia a una revolución de los medios de la violencia, sino a una explotación de la revolución mediática" (Münkler, 2005).

3. 1. La Organización Terrorista "Daesh" en el Ciberespacio

Daesh tiene sus orígenes en 1992 iniciando como un grupo llamado Jund Al Sham (soldados del Levante) combatían principalmente al gobierno jordano y los gobiernos árabes de la región, posteriormente después de la invasión de Irak en el 2003 reaparece con el nombre de "Yama'at al-Tawhid wal-Yihad ("Comunidad del Monoteísmo y la Yihad") para combatir la ocupación estadounidense uniéndose a la organización Al-Qaeda y cambia su nombre "Tanzim Qa'idat al-Yihad fi Bilad al-Rafidayn" ("al-Qaeda en Irak"), sus ideas fundamentalistas y el deseo de formar

un estado islámico le permitió engrosar sus filas, y por sus prácticas extremistas en 2014 se separa de al-Qaeda y es nombrado como ISIS, posteriormente, con el acrónimo de "Daesh" un término peyorativo empleado por sus enemigos (Jordán Enamorado, 2015, p. 111).

Tres son los objetivos de la propaganda del Daesh: "aterrorizar al adversario, reclutar adeptos y tratar de rescatar la utopía suní de la creación de un nuevo orden político que ponga fin a lo que consideran siglos de humillación", para lo cual la organización tiene su propio canal de televisión vía satélite para difundir contenidos propagandísticos, se llama Bein HD4, que se emite en Nilesat, una compañía egipcia, y cuenta con más de 500 mil espectadores, además dispone de una estación de radio en Mosul, llamada Al-Bayan, que es su estación principal, y cubre todas las operaciones militares en Siria e Irak con el objetivo de ejercer presión psicológica sobre la población (Sánchez-Gil, 2021, p. 14).

Posee una revista oficial llamada Dabiq, la cual ha sido creada como una herramienta más de captación y es distribuida por medio de internet de forma mensual. Cuenta con una agencia de noticias llamada Amaq, que se ha convertido en una pieza muy importante en la estrategia propagandística de la organización. En relación a las redes sociales que usa la organización, estas son numerosas, lo cual obedece al propósito de captar nuevos integrantes, extender el terror y despreciar a los occidentales, convirtiendo a estas plataformas en armas de guerra (Paredes, 2021, p. 40).

Daesh ha creado una red de 29 productoras audiovisuales, de las cuales tres se encargan de hacer producciones dirigidas a una audiencia global y las otras 26 crean productos segmentados para cada región que controla el grupo terrorista en Siria, Irak, Egipto, Libia, Yemen, el oeste de África y Afganistán. Ha creado varias aplicaciones para Android (Fajr al-Basha'ir) que estuvo disponible en Google Play y publicaba las noticias actuales del mundo islámico (Poveda, 2019).

Bajo este contexto, la organización Daesh y sus adeptos interactúan con el entorno global a través de la red mostrando sus ejecuciones sanguinarias hacia determinados grupos que no comparten su ideología y visión perturbada. Utilizan revistas y videos para expandir su mensaje y resaltar que la organización no detendrá la difusión de su califato ni el holocausto que se está cometiendo hasta que no termine por completo su guerra santa contra los denominados infieles (Lapayese, 2018, p. 216).

Esta integración organización Daesh – ciberespacio, ha permitido llevar a la práctica una verdadera evolución social y con ello el nacimiento de un nuevo modelo terrorista. Son terroristas yihadistas internautas o "yihadistas de sofá, que desde la comodidad de su casa, y a través de las fuentes libres juntan material para difundir la yihad y expresar sus ideas radicales" (Sageman, 2017).

Normalmente Twitter y Facebook son las herramientas de comunicación que la organización terrorista utiliza para narrar sus actos de barbarie cometidos, pero ante los diversos bloqueos de las autoridades competentes se ha dado lugar al desarrollo de una plataforma propia llamada "5elafabook" (ABC INTERNACIONAL, 2015) en la cual se difunde diariamente y en forma natural las grabaciones de las barbaridades cometidas contra los infieles que tenían secuestrados.

Un caso destacable dentro de este análisis radica en el ciberataque yihadista lanzado por Daesh al canal internacional francés TV5 Monde, el 9 de abril de 2015. La clave de este ataque terrorista se fundamentaba en que no fue indispensable realizar detonaciones, destrucción de infraestructura o matanzas sanguinarias en lugares abiertos para provocar el caos. La organización se dedicó simplemente a desarrollar ataques cibernéticos a los servidores y a las redes sociales de TV5 Monde, televisora con más telespectadores, con el propósito de causar un daño psicológico de consideración. El objetivo no es solo la destrucción física, los efectos psicológicos del ciberterrorismo pueden ser tan poderosos como los reales (Luque, 2019).

Desde el 2014 aproximadamente, los atentados cometidos por Daesh son difundidos casi inmediatamente en el ciberespacio, además cuentan con el apoyo de las revistas online Dabiq y Rumiyah que se constituyen en los altavoces mediáticos del grupo terrorista en el internet y de la agencia de comunicación Amaq, cuyo propósito es reivindicar los atentados a través del ciberespacio (AZMAN, 2022, p. 4).

Daesh ha ejecutado sus actos terroristas por medio de las redes sociales activando un gran contingente de simpatizantes en países occidentales. Desde el 2014 se está observando el crecimiento de manera impresionante y perturbadora del uso de la red por parte de la organización Daesh en la obtención, estimulación y realización de actos terroristas, y a pesar de haber sufrido por la Coalisión Internacional una reducción considerable de sus territorios en Irak y Siria, se ha podido percibir que al final del 2018 no sólo mantiene activos sus dispositivos y sistemas virtuales de obtención y publicidad, sino que está ampliando sus actividades de amenaza digital sobre la multitud a la que desea horrorizar y desaparecer (Lapayese, 2018, p. 221).

3.2. La organización terrorista "Al Qaeda"

Este grupo terrorista fue fundado por Osama Bin Laden y significa "La Base", en 1988 se mantiene como una red de terrorismo internacional, fue responsable del ataque terrorista del 11 de septiembre del 2001 en Estados Unidos, del 11 de marzo del 2004 en España, entre otras; en 2011 su líder fue asesinado, lo sucedió Ayman Al Zawahiri y con base a su estructura fragmentaria con células militantes y un sinnúmero de contactos clandestinos, han manteniendo la idea de

guerra santa junto con Daesh, se convierten en la mayor amenaza a la seguridad internacional (Lima, 2017, p. 3).

Al Qaeda se constituyó en la primera organización terrorista que impulsó la utilización del ciberespacio para su accionar con resultados muy positivos. Tras las operaciones ejecutadas por Estados Unidos en Oriente Medio, la organización sufrió un gran detrimento que le obligó a reinventarse, encontrando en el ciberespacio un nuevo campo de operaciones a través del cual redireccionar sus intervenciones y poder alcanzar sus propósitos planificados, utilizando la Internet como medio para ampliar su propaganda y las expresiones de su líder, alcanzando velozmente ser percibidos por millones de personas (Sánchez, 2015, p. 101).

Azzam Publications una editorial con sede en Londres que vendía documentación electrónica para apoyar y financiar los atentados y extender las redes de captación terroristas; en España Al Qaeda también desplegó el uso intenso del ciberespacio a través de su Red Ánsar Al Mujahideen (RAAM), grupo que aparece conformado por un reducido "núcleo duro"́ de personas con una dilatada trayectoria en plataformas yihadistas en Internet, por medio de las cuales se estimulaba a perpetrar actos terroristas.

Los integrantes de esta red RAAM incitaban a cometer atentados y planificaban cursos online para llegar a ser terroristas, logrando a través del uso de las TIC convertir el ciberespacio en uno de los medios más productivos para captar, reclutar y adoctrinar a nuevos integrantes para Al Qaeda. Actualmente, Al Qaeda no solamente aprovecha la tecnología para difundir su propaganda, sino que se ha convertido en un movimiento social que permite el acceso a cualquier individuo y en cualquier lugar del planeta, que disponga de un dispositivo electrónico y una conexión a internet (Alcântara, 2018, p. 59).

Bajo este contexto, es importante mencionar que el número de grupos terroristas operando en internet cada vez es mayor, por consiguiente, la probabilidad de alterar el equilibrio securitario a través de medios virtuales aumenta cada vez más. El internet permite a las distintas organizaciones terroristas planear sus operaciones bajo la sombra, facilitando la comunicación y con la garantía de un anonimato casi indescifrable.

Un aspecto curioso es el empleo de la *deep web*[5] por parte de los terroristas. La presencia de un *black market* amplio y acentuado facilitaba a los yihadistas encontrar documentación para autoradicalizarse, material para realizar explosivos caseros o conseguir las competencias necesarias para planificar y ejecutar un ciberataque efectivo que cause un grave daño psicológico en la población. Estos acontecimientos mostraban que los miembros de las organizaciones terroristas no partían desde cero para la creación de las ciberarmas, simplemente acudían a la *deep web* y adquirían todo lo que necesitaban a un precio y riesgo muy moderado (Alayda et al., 2021, p. 3002).

5 Archivos que hay en Internet que no están indexados por los buscadores, área de Internet que está "oculta" y tiene poca regulación.

3.3. El ciberterrorismo y sus tendencias en el Ecuador

El ciberespacio en la actualidad se conforma como un nuevo dominio para la defensa de la soberanía, integridad territorial y seguridad del Estado. En este nuevo contexto se desarrollan actividades sociales, productivas y económicas, impulsadas por el veloz desarrollo tecnológico y originando vulnerabilidades que, sin lugar a duda, pueden ser explotadas por diversas amenazas, causando efectos estratégicos sobre la estructura, institucionalidad, estabilidad y gobernabilidad, ocasionando una alteración de la paz colectiva y la soberanía del Estado ecuatoriano. El código orgánico integral penal de Ecuador dedica varias normas orientadas a regular distintas expresiones del terrorismo, y específicamente menciona al ciberterrorismo y sus tendencias relacionadas a la comisión del delito por medios tecnológicos.

En el país no existe una marcada tendencia de grupos ciberterroristas, sin embargo, la ascendente popularidad y utilización de nuevas soluciones digitales ha conducido a criminales a beneficiarse de estos servicios para obtener utilidades ilícitas. La pandemia sin lugar a duda ha agilizado el proceso debido a la gran cantidad de transacciones y actividades que se realizan en línea. La cantidad de delitos cibernéticos está creciendo en Ecuador, lo que muestra un número cada vez mayor del total de delitos registrados. La cantidad de delitos cibernéticos denunciados en los 3 últimos años se ha duplicado, siguiendo una tendencia general a nivel de Latinoamérica y mundial, esto debido a que la ciberdelincuencia actualmente es de naturaleza transnacional, aumentando en complejidad, innovación técnica y nivel de organización. La limitada educación digital y la poca conciencia en temas de ciberseguridad conducen a la sociedad a ser perjudicada por la ciberdelincuencia.

Las víctimas de este tipo de delitos no son conscientes de que sus activos han sido comprometidos, existiendo una ignorancia general sobre cómo actuar ante este tipo de delitos. Normalmente no se confía en que la ley y su aplicación puedan resolver el problema, debido a que la indagación y juicio pueden dilatarse por las reducidas capacidades de las autoridades, lo que conlleva frecuentemente a que no sea denunciado el delito cibernético. Se ha determinado que el fraude informático, robo de identidad y la violación de datos personales son los delitos cibernéticos más generales en el Ecuador.

Esta innegable adopción de tecnologías ha devenido en desarrollo y, consecuentemente, en problemas de ciberseguridad. Al menos en Ecuador, las estadísticas referentes a violaciones a la seguridad han sido en su mayoría dentro del sistema financiero. Un incremento en sus cifras ha convertido a la ciberseguridad en un tema preocupante, especialmente para la banca ecuatoriana. Por ejemplo, en 2014 se registró un aumento de 37% de robos a la banca virtual, 14% en tarjetas de crédito

y 46% en cajeros electrónicos. Pero no solo los problemas han sido en los sistemas de la banca. La prensa ecuatoriana también ha sido expuesta a varios ataques en sus sitios web que utilizan el "dominio.ec", de la misma manera, ataques a sitios web del gobierno atribuidos al grupo Anonymous, ataques al sistema informático electoral del Ecuador, supuestos ataques cibernéticos procedentes de Colombia, Estados Unidos, Rusia, China y Francia sobre cuentas o datos personales de ciudadanos ecuatorianos, así como ataques a twitters y redes sociales de personajes públicos y portales web de opinión libre (Vargas Borbúa et al., 2017)

En el 2020 en Ecuador, según ESET, hubo más de 51 mil registros relacionados con *cryptominers* (malware utilizado para la minería de criptomonedas), alrededor de 140 mil detecciones de *exploits* (código utilizado para aprovechar vulnerabilidades en software), cerca de seis mil detecciones de *ransomware* (malware para el secuestro de información) y casi ocho mil detecciones de *spyware* (software espía), como datos de algunos tipos de software malicioso. El *ransomware* es el que más daño ha causado a las empresas públicas y privadas en Ecuador. Los atacantes aprovechan la mayor superficie de exposición de las organizaciones y usuarios para comprometer la seguridad, afectando con diversos tipos de amenazas, donde el *ransomware* ha tenido un importante protagonismo, con ataques cada vez más dirigidos, con mayor impacto, con características más agresivas y con montos solicitados por el rescate de la información cada vez más elevados. Además, el *phishing*, ataque de ingeniería social que usa medios digitales para el robo de datos, son las herramientas más utilizadas para comprometer la seguridad de las empresas y las personas (Ortiz, 2021)

En octubre de 2021, el Banco Pichincha sufrió un ciberataque que interrumpió sus operaciones y dejó fuera de servicio el cajero automático y al portal de banca online, este ataque fue considerado como uno de los mayores en el mundo ese año. Esta fue la segunda vez en tan solo meses que el banco se vio afectado; en febrero fue víctima de otro ciberataque que también afectó al Ministerio de Finanzas (Welivesecurity.com, 2021).

El 16 de abril, el Municipio de Quito recibió un ciberataque a su infraestructura informática, a través de un malware de tipo *ransomware* de la cepa BlackCat vinculado a Rusia. Cuando se logró detener la propagación del virus, el 20% del contenido de la base de datos de la administración central del cabildo había sido afectada (Caceres, 2022). El 10 de marzo, la plataforma informática del CIES sufrió un ataque, comprometiendo la información procesada por esta institución y a los subsistemas de Inteligencia de la Policía y Fuerzas Armadas (Televistazo, 2022).

De acuerdo con el Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL) mediante su Centro de Respuesta a Incidentes Informáticos Ecucert, se notificaron 7.292 ataques en los cuatro primeros meses del 2022, mientras que en 2021 hubo 15.847 alertas, lo que demuestra que desde el primer cuatrimestre del año ya se ha superado el número de incidentes del año pasado. Por esta razón hoy en día el término ciberdefensa se ha desarrollado más al existir ciberterrorismo y cibercrimen, con mecanismos de defensa exclusivos para abordar un ciberataque (Llumiquinga, 2022).

4. LA RESPUESTA DE LOS ESTADOS ANTE EL CIBERTERRORISMO

El ciberterrorismo, al igual que otras amenazas que circulan por el ciberespacio, es una preocupación a nivel global, por lo que ocupa un lugar importante en la Agenda Internacional de los Estados y en cooperación con las organizaciones internacionales enfocan sus esfuerzos para combatir estas amenazas por medio de la ciberseguridad.

La Organización de Naciones Unidas (ONU), en 1985 creó la Unión Internacional de Telecomunicaciones (UIT) como organismo especializado para las tecnologías de la información y comunicación y una de sus funciones principales es la elaboración y difusión de las normas técnicas que permiten una interconexión armoniosa de redes y tecnologías para mejorar el acceso a las TIC, así como también el tema de la gobernanza de la Internet (ITU, 2022).

En 2004 la Unión Europea (UE) crea la Agencia de la Unión Europea para la Ciberseguridad (ENISA) con la misión de mantener un alto nivel de ciberseguridad en toda Europa, contribuyendo en el fortalecimiento de la economía conectada, mejorar la resiliencia de la infraestructura crítica de la UE y proteger a la sociedad y ciudadanía europea de las amenazas digitales (ESINA, 2022).

En el caso de América, en la Organización de Estados Americanos específicamente, la lucha contra el terrorismo ha permitido formular amplias políticas para hacer frente a esta amenaza en la región, ante lo cual crean el Comité Interamericano contra el Terrorismo (CICTE), y este a su vez genera el programa de ciberseguridad para colaborar con los Estados miembros en el incremento de capacidades de ciberseguridad referentes a políticas públicas y nivel técnico para garantizar un ciberespacio seguro y resistente (OEA, 2009).

A estas organizaciones se suman la Comisión Internacional de Telecomunicaciones (CITEL) que establece normas técnicas para un Internet seguro, también la Reunión de Ministros de Justicia de América (REJMA) que promueve a todos los países miembros la formulación de normativas para proteger a los usuarios y a las redes de información, la Junta Interamericana de Defensa (JID) que emitió la Guía de Ciberdefensa y la Fundación Interamericana de Defensa, que mediante la cooperación internacional enfocan sus

esfuerzos a generar ciberestrategias para hacer frente a las ciberamenazas, destacándose Chile, Argentina y Colombia como países pioneros en implementar una política y estrategia de ciberseguridad y ciberdefensa (MIDENA, 2021, p. 48).

4.1. Gobernanza de la Ciberseguridad en el Ecuador

Al hablar de la ciberseguridad en el Ecuador nos referimos a la protección del quinto dominio, el ciberespacio, y debido a la complejidad de este, no es únicamente responsabilidad de las Fuerzas Armadas o Policía Nacional, ya que requiere un mayor desarrollo de capacidades en diferentes ámbitos que conciernen tanto a actores estatales, como actores privados nacionales, de esta forma se alcanza una gobernanza responsable referente a la ciberseguridad.

En el Ecuador el ciberterrorismo se encuentra estipulado como un riesgo[6] a la seguridad y defensa nacional en la Política de Defensa Nacional 2018 (PND); aunque su tratamiento no es directo como tal, no es considerado como una amenaza o amenaza híbrida, sin embargo, la posibilidad de ocurrencia lo deja inmerso dentro de los ciberataques y vulneración a la infraestructura crítica del Estado como un mecanismo tecnológico al igual que el ciberdelito, cibercrimen, ciberespionaje, e infiltración de los sistemas informáticos, que pueden atentar contra la infraestructura del Estado y llegar a poner en peligro la seguridad nacional (MIDENA, 2018).

Con el objetivo propuesto por parte del Estado, de lograr un Ecuador digital ciberseguro mediante la protección de servicios, de la infraestructura crítica y de la seguridad de la población en el ciberespacio, en el año 2021 se emite la Política Nacional de Ciberseguridad (PNC) en la cual el Gobierno ha definido su campo de trabajo en siete pilares claves: (1) Gobernanza de la ciberseguridad, (2) Sistemas de información y gestión de incidentes, (3) Protección de infraestructura crítica y servicios esenciales, (4) Soberanía y defensa, (5) Seguridad pública y ciudadana, (6) Diplomacia en el ciberespacio y cooperación internacional, y (7) Cultura y educación de la ciberseguridad (MINTEL, 2021).

Esta política se encuentra alineada con otras políticas de gobierno, así también con un robusto marco normativo nacional junto con instrumentos internacionales, los cuales buscan hacer frente al ciberterrorismo, así como también a los demás riesgos y amenazas que provienen del ciberespacio. Cada uno de los siete pilares está conformado por diversos actores con lineamientos bien definidos e interconectados entre sí.

El Ministerio de Defensa (MIDENA) es el responsable directo por dos pilares, en base a su misión y función dentro del Estado, pero no se deslinda de la coordinación y cooperación interagencial entre los actores públicos y privados; el primero es la "Protección de la infraestructura crítica digital y servicios esenciales", aquí se garantiza la continuidad de las operaciones y la resiliencia ante ataques o incidentes; el segundo pilar es la "Soberanía y Defensa", aquí se establece que la ciberdefensa es una parte de la ciberseguridad y como tal debe propender la defensa contra las amenazas y riesgos establecidos en la PND, siendo su principal objetivo el ser humano, estos pilares garantizan la defensa de la integridad territorial y soberanía nacional, promoviendo la cooperación regional e internacional en ciberdefensa (MINTEL, 2021).

Posteriormente, el Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL), como ente articulador de la ciberseguridad, emite la Estrategia Nacional de Ciberseguridad con una vigencia de 3 años (2022-2025), en ella ratifica al MIDENA como ente rector de la ciberdefensa a través del Comando Conjunto de las Fuerzas Armadas (CC.FF.AA.) y establece el objetivo estratégico para la Ciberdefensa:

> Objetivo 4.1: Incrementar y fortalecer las capacidades de ciberdefensa del Estado ecuatoriano para alcanzar la actitud estratégica defensiva definida en la Política de la Defensa Nacional, para la protección de la infraestructura crítica digital (ICD) y servicios esenciales en el ciberespacio (MINTEL, 2022).

El CC.FF.AA. en el año 2021 emite la Estrategia de Ciberdefensa, siendo el ente planificador y quien conduce las operaciones militares, al igual que las ciberoperaciones para enfrentar las ciberamenazas, las cuales considera como: ciberconflictos, ciberespionaje, ciberterrorismo, ciberdelincuencia y hacktivismo, para ello se encuentra conformado por el Comando de Ciberdefensa (COCIBER), la Fuerza Terrestre, Naval y Aérea, quienes realizaran operaciones de defensa, exploración y respuesta en el ciberespacio, también cuentan con el apoyo de otras instituciones estatales y la cooperación de organismos internacionales (MIDENA, 2021).

Esta gobernanza de la ciberseguridad propende al desarrollo de las capacidades gubernamentales y cooperación internacional, también apunta al desarrollo académico nacional, estos nuevos retos serán de sumo beneficio para la sociedad ecuatoriana, contribuyendo de esta manera con la seguridad integral del país, así como a la protección de la integridad territorial y soberanía nacional.

En las dos últimas décadas los ciberataques en el Ecuador se han incrementado, en su mayoría se mencionan hackeos a correos electrónicos, extracción de datos por medios electrónicos, violación a la privacidad, entre otros, con el pasar del tiempo y los avances tecnológicos los ciberataques también alcanzan objetivos mayores, como en el caso de la Agencia Nacional de Tránsito del Ecuador, que en el 2018 sus sistemas informáticos fueron comprometidos, generando una pérdida de más de un millón de dólares para el país, posteriormente

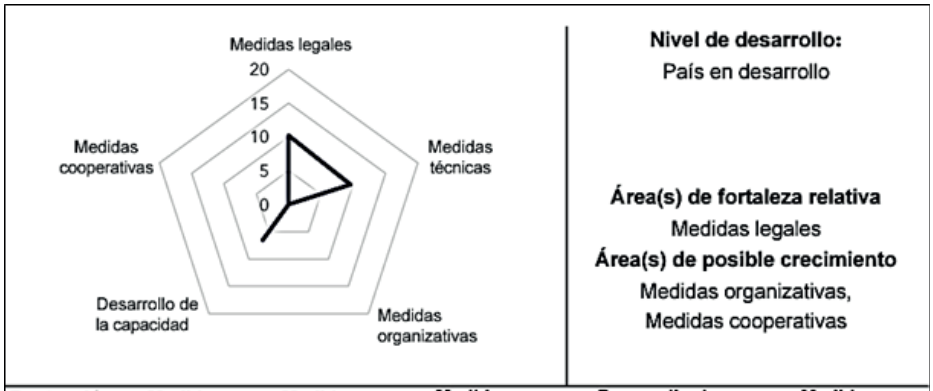
6 Los riesgos son considerados como condición interna o externa generada por situaciones de origen natural o antrópico que pudieran afectar a la seguridad y defensa del Estado; su posibilidad de ocurrencia es incierta…

se le atribuye más de 40 millones de ciberataques al Ecuador ocurridos en abril del 2019, al retiro de asilo de Julián Assange de la embajada Ecuatoriana en Londres, estos consistían en ataques de denegación de servicios dirigidos hacia instituciones públicas (Cancillería, Ministerios, Presidencia, Servicio de rentas Internas y Municipios), provenientes de Estados Unidos, Austria, Gran Bretaña, Holanda, Francia, Rumania, Alemania, Brasil e incluso de Ecuador (Villacís, 2022).

Según la Global Cybersecurity Index (2020), para el 2020 el Ecuador ocupaba el lugar 119 en el mundo y el puesto 19 de entre los países de las Américas en el ranking de vulnerabilidad en ataques cibernéticos, en al análisis realizado sobre el perfil de la gobernanza de ciberseguridad establece que el Ecuador dispone de fortalezas en el área normativa[7] y área técnica[8] pero que están por debajo de la media del resto de los países de Sudamérica, seguido de una capacidad de desarrollo[9] que supera por poco los parámetros básicos de gestión, para recaer en la falta total de medidas cooperativas[10] y medidas organizativas[11] (Figura 2).

Figura 2

Perfil de Ciberseguridad en Ecuador 2020



Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
26,30	10,22	9,55	0,00	6,53	0,00

Nota. Obtenido de International Telecommunication Union (2020).

Ante la realidad actual y el desarrollo acelerado de la tecnología, a la PNC se le presentan verdaderos desafíos en cuanto al desarrollo de capacidades e implementaciones en su sistema de gobernanza, a simple vista podríamos decir que la PNC no es suficiente, ya que han existido ciberataques bajo su protección, pero también se debe considerar que diariamente existen miles de ataques que provienen de diferentes partes del mundo y que no han logrado burlar el inmenso filtro digital que la PNC ha conseguido, por lo que se debe considerar que la PNC necesita evolucionar igual de rápido que la tecnología, mediante la destinación de recursos para adquirir tecnología de punta, personal altamente capacitado, estrategias interagenciales y demás acciones que permitan potencializar esta ámbito para reducir la amenaza y alcanzar los objetivos establecidos.

CONCLUSIONES

Las aportaciones doctrinarias presentadas en esta investigación muestran cómo las amenazas, en este caso el ciberterrorismo, se han tornado flexibles, saliendo de su contexto habitual con una flexibilidad y capacidad para adaptarse y combinar muchos de los métodos tradicionales con la tecnología actual, lo que explica por qué es una amenaza hibrida, ya que las organizaciones terroristas han generado un innovador tipo de terrorismo que usa el marketing y la comunicación digital para extender el terror a nivel global, y actualmente de forma prioritaria para transformar el terror en algo popular, deseable e imitable.

Se ha determinado doctrinariamente que el ciberterrorismo forma parte de la gran transformación del ciberespacio, permitiendo que tanto la delincuencia común como los grupos terroristas hayan trasladado gran parte de sus operaciones a las nuevas Tecnologías de la Información y Comunicaciones, usando ampliamente el Internet debido a las características intrínsecas que posee el ciberespacio, como la instantaneidad, el anonimato y el fácil acceso, lo que implica una enorme dificultad para defenderse o prevenir este tipo de amenaza híbrida.

7 Medidas basadas en la existencia de marcos legales en materia de ciberseguridad y ciberdelincuencia.
8 Medidas basadas en la existencia de instituciones técnicas y un marco que se ocupe de la ciberseguridad.
9 Medidas basadas en la existencia de programas de investigación y desarrollo, educación y formación, profesionales certificados y organismos del sector público que fomentan el desarrollo de capacidades.
10 Medidas basadas en la existencia de asociaciones, marcos cooperativos y redes de intercambio de información.
11 Medidas basadas en la existencia de instituciones de coordinación, políticas y estrategias para el desarrollo de la ciberseguridad a nivel nacional.

En este mundo globalizado, la comunidad internacional unifica esfuerzos para enfrentar al ciberterrorismo, la concentración de recursos, la amplitud del marco normativo y los avances tecnológicos dificultan cada vez más el accionar de estos grupos terroristas, obligándolos a buscar nuevas formas de operar dentro de la web, generando una dinámica evolutiva mutua en donde la carrera por adquirir tecnología de avanzada y desarrollar mayores capacidades tecnológicas parecen hacer la diferencia entre las ciberoperaciones de la comunidad internacional y los ciberterroristas.

En el Ecuador las amenazas no están vinculadas a la característica de hibridez, las cuales mantienen su fisonomía rígida desde la PND del 2018, en la que el ciberterrorismo es catalogado como un riesgo, sin embargo, en la nueva Estrategia de Ciberdefensa 2021 consta como una amenaza, por lo que se debe plantear la actualización de la PND.

El propender desarrollar las capacidades sobre ciberseguridad en el Ecuador implica un costo relativamente elevado, así como el desarrollo académico, también se deben fortalecer las relaciones civil-militar y mejorar la interoperabilidad entre instituciones, ya que con una consolidación dinámica de medios y recursos humanos se puede enfrentar a las amenazas actuales, cualquiera que sea su característica, por lo que el presente artículo abre nuevas líneas de investigación para temas afines.

Referencias

ABC INTERNACIONAL. (2015). «Califatobook», la red social de los seguidores del Estado Islámico. abc. https://www.abc.es/internacional/20150313/abci-califatobook-social-seguidores-estado-201503121236.html

Akhgar, B. (2014). *Cyber crime and cyber terrorism investigator's handbook*. Elsevier.

Alayda, S., ALmowaysher, Najd. A., Alserhani, F., & Humayun, M. (2021). *Terrorism on Dark Web. 12*(10), 6.

Alcântara, B. T. D. (2018). *Internet, terror e ciberterrorismo: uma análise comparativa.* Universidade federal do rio grande do sul..

Amnesty International. (2017). *DANGEROUSLY DISPROPORTIONATE*. 70. https://www.amnesty.org/en/documents/eur01/5342/2017/en/

AZMAN, N. A. (2022). 'ISLAMIC STATE' (IS) *PROPAGANDA. 8*(10), 7.

Caceres, A. (2022, abril 18). Municipio de Quito suspende trámites digitales por ataque de hackers. *El Comercio*. https://www.elcomercio.com/actualidad/municipio-quito-ataque-hacker-tramites.html

Cano, J. (2014). Cibercrimen y Ciberterrorismo: Dos Amenazas Emergentes. *Journal Online*, 7.

Casalunga, F. H., & Pinheiro, A. C. (2019). Guerra híbrida e ciberconflitos: uma análise das ferramentas cibernéticas nos casos da Síria e conflito Rússia-Ucrânia. 5(3), 17.

Cespedosa Rodríguez, C. (2019). *Yihadismo, Internet y Ciberterrorismo.* https://repositorio.comillas.edu/xmlui/handle/11531/30875

Chicharro, A. (2013). La violencia terrorista en el Ciberespacio: Riesgos y normativa europea3_Chicharro.pdf. V Congreso Internacional Latina de Comunicación Social – V CILCS, 5, 28.

Collin, B. (1997). Future of Cyberterrorism: The Physical and Virtual Worlds Converge | Office of Justice Programs. *Crime and Justice International,* 13(2), 4. https://www.ojp.gov/ncjrs/virtual-library/abstracts/future-cyberterrorism-physical-and-virtual-worlds-converge

Council of Europa. (2018). Legal challenges related to hybrid war and human rights obligations. 14523, 16. Doc. 14523. https://pace.coe.int

Da Silva, F. (2020). Guerra Híbrida por uma discussão conceitual. *Centro do estudos estratégicos do Exercito,* 18(4), 14.

Demurtas, A. (2021). La naturaleza cambiante del fenómeno terrorista en posguerra fría: Evolución de las formas de analizarlo y afrontarlo en el marco OCDE comparando el enfoque europeo y el estadounidense. 20.

Denning, D. (2000). Cyberterrorism: The Logic Bomb versus the Truck - ProQuest. *Global Dialogue,* 2(4), 29. https://www.proquest.com/docview/211506749?pq-origsite=gscholar&fromopenview=true

ESINA. (2022). Acerca de la ENISA - Agencia de la Unión Europea para la Ciberseguridad [About ENISA]. ENISA. https://www.enisa.europa.eu/about-enisa/about/es

Fly, J., Rosemberg, L., & Salvo, D. (2018). Policy Blueprint for Countering Authoritarian Interference in Democracies. *The German Marshall Fund of the United States*, 27, 45. https://securingdemocracy.gmfus.org/wp-content/uploads/2018/06/Policy-Blueprint.pdf

Galán, C. (2018). *Amenazas híbridas: Nuevas herramientas para viejas aspiraciones. 23.*

Hernández, A. (2017). Ciberseguridad y Confianza. 897, 12.

Ignacio, F. (2022). La OTAN y el ciberespacio: un nuevo dominio para las operaciones. *Revista Ejército*, 972, 8.

International Telecommunication Union. (2020). *Global Cybersecurity Index*. ITU 2021.

ITU. (2022). Unión Internacional de Telecomunicaciones (UIT). ITU. https://www.itu.int:443/es/about/Pages/default.aspx

Johnson, R. (2018). Hybrid War and Its Countermeasures: A Critique of the Literature. *Small Wars & Insurgencies, 29*(1), 141-163. https://doi.org/10.1080/09592318.2018.1404770

Jordán Enamorado, J. J. (2015). El Daesh. Ministerio de Defensa. https://digibug.ugr.es/handle/10481/41175

Lapayese, M. J. G. (2018). Daesh: Terrorismo global y local a medio camino entre lo físico y lo virtual. Universidad Complutense de Madrid.

Lima, K. (2017). Um breve histórico Al-Qaeda: De Exército Jihadista a Movimento Ideológico. *Boletim Historiar, 19*, 18. http://seer.ufs.br/index.php/historiar

Llinares, M. (2012). *El cibercrimen: Fenomenología y criminología de la delincuencia en el ciberespacio.* 337.

Llumiquinga, R. (2022, junio 22). Ecuador es uno de los países más vulnerables para los ciberdelincuentes. https://prensa.ec/2022/06/22/ecuador-es-uno-de-los-paises-mas-vulnerables-para-los-ciberdelincuentes/

Luque, J. (2019). "Los nuevos conflictos bélicos del siglo XXI: las amenazas híbridas" [doctorado]. Universidad Católica de Murcia.

Martínez, O. (2005). Ciberterrorismo. *Revista de Derecho Informático*, 82.

Mayer Lux, L. (2018). Defining cyberterrorism. *Revista Chilena de Derecho y Tecnología, 7*(2), 5. https://doi.org/10.5354/0719-2584.2018.51028

MIDENA. (2018). *Política de Defensa Nacional Libro Blanc*o. https://www.defensa.gob.ec/wp-content/uploads/2019/01/Pol%C3%ADtica-de-Defensa-Nacional-Libro-Blanco-2018-web.pdf

MIDENA. (2021). *Estrategia de Ciberdefensa del Ecuador.* IGM.

MIINTEL. (2021). *Política Nacional de Ciberseguridad.*

MINTEL. (2022). *Estrategia Nacional de Ciberseguridad.* Ministerio de Telecomunicaciones y de la Sociedad de la Información.

Münkler, H. (2005). Viejas y nuevas guerras: Asimetría y privatización de la violencia. *Siglo*, 21, 40.

OEA. (2009, agosto 1). OEA - Organización de los Estados Americanos: Democracia para la paz, la seguridad y el desarrollo [Text]. https://www.oas.org/es/sms/cicte/prog-ciberseguridad.asp

Ortiz, D. (2021, julio 29). Ecuador está entre los países con más ciberataques en América Latina. *El Comercio.* https://www.elcomercio.com/tendencias/tecnologia/ecuador-ciberataques-america-latina-hacker.html

Paredes, M. (2021). *Ciberterrorismo: Un nuevo desafío para el Derecho Internacional Humanitario*. Pontificia Universidad Católica del Perú.

Pawlak, P. (2015). *Understanding hybrid threats* (PE 564.355; p. 2). European Parlament. https://www.europarl.europa.eu/RegData/etudes/ATAG/2015/564355/EPRS_ATA(2015)564355_EN.pdf

Pollitt, M. M. (1998). Cyberterrorism, Fact or fancy? *Computer Fraud & Security*, 1998(2), 8-10. https://doi.org/10.1016/S1361-3723(00)87009-8

Porche, I., Paul, C., York, M., Serena, C., Sollinger, J., Axelband, E., Min, E., & Held, B. (2013). *Redefining information warfare boundaries for an Army in a wireless world*. RAND.

Poveda, M. (2019). El periodismo como arma de captación terrorista. *Revista de Comunicación de la SEECI*, 59-80. https://doi.org/10.15198/seeci.2019.49.59-80

Sageman, M. (2017). *Misunderstanding Terrorism* (University of Pennsylvania Press, Vol. 1). University of Pennsylvania Press.

Sánchez, G. (2015). EL CIBERTERRORISMO: DE LA WEB 2.0 AL INTERNET PROFUNDO. *Revista Ábaco,* 3(85), 9.

Sánchez-Gil, L. M. (2021). *Reformulating the concept of cyberterrorism*. 11, 15.

Santos, D. M. A., Maltez, M. M., Gomes, T. E. da S., Freitas, G. de M., & Sanders, A. (2019). A arte da guerra no século XXI: Avançando à Multi-Domain Battle. *Coleção Meira Mattos.* https://doi.org/10.22491/cmm.a005

Televistazo. (2022, marzo 10). Otra plataforma informática del Centro de Inteligencia Estratégica fue vulnerada por hackers; www.ecuavisa.com. https://www.ecuavisa.com/noticias/ecuador/otra-plataforma-informatica-del-centro-de-inteligencia-estrategica-fue-vulnerada-por-hackers-FE1431153

Vargas Borbúa, R., Reyes Chicango, R. P., & Recalde Herrera, L. (2017). Ciberdefensa y ciberseguridad, más allá del mundo virtual: Modelo ecuatoriano de gobernanza en ciberdefensa/ Cyber-defense and cybersecurity, beyond the virtual world: Ecuadorian model of cyber-defense governance. *URVIO - Revista Latinoamericana de Estudios de Seguridad*, 20, 31. https://doi.org/10.17141/urvio.20.2017.2571

Viegas, P. (2004). Ciberterrorismo: Aspectos de Segurança. 2433, 19.

Villacís, R. P. C. (2022). Ciberseguridad y Ciberdefensa: Perspectiva de la situación actual en el Ecuador. *Revista Tecnológica Ciencia y Educación Edwards Deming*, 6(1), Art. 1. https://doi.org/10.37957/rfd.v6i1.88

Welivesecurity.com. (2021, octubre 14). Banco Pichincha sufrió ataque informático que afectó parte de sus servicios. *WeLiveSecurity.* https://www.welivesecurity.com/la-es/2021/10/14/banco-pichincha-sufrio-ataque-informatico/