Escuela Superior de Guerra

“General Rafael Reyes Prieto”

Maestría en Ciberseguridad y Ciberdefensa

FACTORES DETERMINANTES EN LA EVOLUCIÓN DEL TERRORISMO INTERNACIONAL EN EL CIBERESPACIO

MAYOR. JULIAN ESTEBAN BARRERA GOMEZ

Director de trabajo de grado

Mgtr. Mónica Flórez Cáceres

Bogotá D.C, Colombia; 29 de abril del 2022.

Dedicatoria

A mis hijos Emiliano y Juan Martin les dedico todo el esfuerzo y dedicación puestos en el desarrollo de este trabajo de investigación, pues son ellos los que me motiva a crecer todos los días, quiero ser su mejor ejemplo de superación, responsabilidad y humildad; valores que son fundamentales para el desarrollo de la sociedad y serán ellos los llamados a transformarla.

A todo el pueblo Colombiano y sus necesidades de mejoramiento y desarrollo de entornos digitales estables y pacíficos; y las instituciones de seguridad que dedican sus esfuerzos en la consolidación de soluciones efectivas a los nuevos panoramas construidos por tecnologías de la información y las telecomunicaciones.

Agradecimientos

Agradezco a Dios por permitirme tener a mi lado personas que me han enseñado el verdadero valor de la responsabilidad, dedicación, deseo de superación y humildad que me han caracterizado durante el desarrollo de mi vida profesional.

Gracias a mi glorioso Ejercito Nacional por brindarme esta grata oportunidad de superación profesional, permitiéndome profesionalizarme en campos que se encuentran a la vanguardia de la defensa y seguridad de nuestro país, generando capacidades cognitivas que me permitirán aportar mis mejores capacidades en beneficio de esta maravillosa institución y de la sociedad colombiana.

Por último y no menos importante quiero agradecer de todo corazón a mis tutores, al Mgtr. Henry Mauricio Acosta Guzmán (tutor metodológico), a la señorita Mgtr. Mónica Flórez Cáceres (tutora temática) que con su Experiencia, dedicación y entrega han conducido a buen término esta investigación; fue un gusto contar con su apoyo y orientación.

Tabla de contenido

Abreviaturas

Tech – el término hace alusión al concepto de tecnología.

Core –

CCOCI – Comando Conjunto Cibernético

OEA – Organización de los Estados Americanos

OTAN- Organización del Tratado Atlántico Norte

Dasboard – tablero de automatización de datos para la reducción de incertidumbre a la hora de tomar decisiones.

Resumen

El terrorismo cibernético es un fenómeno de naturaleza hostil que goza de características y factores procedimentales complejos. Hablar de terrorismo cibernético no refiere únicamente a una serie de ataques de naturaleza ciber con altos niveles tecnológicos. Hay otro tipo de terrorismo que ha venido en auge, y refiere a problemáticas dispersas, sujetas a la utilización de medios y métodos digitales con fines coercitivos o de intimidación. Ese tipo de terrorismo cibernético es el que da origen al presente estudio.

El objetivo en esta investigación es identificar los factores que han facilitado la evolución del terrorismo internacional generado en el ciberespacio, desde el año 2010 hasta 2021. El periodo seleccionado obedeció a dos delimitantes: el incremento de ciber ataques registrados por la Secretaría de Seguridad Multidimensional de la OEA y la transmutación de diferentes elementos y escenarios en los que se emplea el terrorismo cibernético.

Para llevar a cabo el proceso de investigación se utilizó un enfoque cualitativo, y un diseño exploratorio dividido en cinco partes: diseño teórico, marco jurídico, análisis de datos, comprobación de hipótesis y triangulación final de resultados, datos y conceptos clave.

Palabras clave: ciber-terrorismo, cibernético, evolución, medios, digitales

Abstract

Cyber terrorism is a phenomenon of a hostile nature that has complex procedural characteristics and factors. Talking about cyber terrorism does not only refer to a series of attacks of a cyber nature with high technological levels. There is another type of terrorism that has been on the rise, and it refers to scattered problems subject to the use of digital means and methods with coercive fines or intimidation. This type of cyber terrorism is what gives rise to this study.

The objective of this research is to identify the determining factors that have allowed the evolution of international terrorism generated in cyberspace from 2010 to 2021. The period of time selected was due to two constraints: the increase in cyber-attacks registered by the Secretariat of Multidimensional Security of the OAS and the transmutation of the different elements and scenarios in which cyber terrorism is used.

In this research, a qualitative approach was used, and an exploratory design divided into five parts: theoretical design, legal framework, data analysis, hypothesis testing and final triangulation of results, data and key concepts.

Key Words: cyber terrorism, cyber, evolution, media, digital

Introducción

El terrorismo internacional cibernético se ha convertido en una de las problemáticas con mayor número de impactos en el esquema de seguridad y defensa de los Estados (Rubio, Alcaraz, Román y López, 2019, p. 3). De acuerdo con Conti, Dargahi y Dehghantanha (2018), las actividades ciberterroristas aumentaron un 62% en el 2021. Tal aumento no solo representa una amenaza de tipología compleja; también representa un núcleo de factores delictivos que se categorizan bajo el umbral de las nuevas guerras híbridas.

Para entender cómo el fenómeno se ha expandido en escenarios digitales cotidianos es indispensable comprender su definición desde la perspectiva de Fernández (2018), para quien resulta ser, no un hecho como tal, es decir, no crimen común, sino una fenomenología en constante cambio, la cual requiere estudios segmentados y exploratorios.

La definición *per se* del término dista del posible núcleo de afectaciones que pudieren emerger por su expansión en sistemas y subsistemas de información. En la investigación que se titula Internet, la nueva era del delito: ciber delito, ciberterrorismo, legislación y ciberseguridad, Gamón (2017) explica cuán necesario resulta comprender el núcleo funcional del terrorismo internacional cibernético, mucho más porque su *core* cambia constantemente, se transforma y adapta a nuevas circunstancias o necesidades delictivas del contexto.

La transformación del ciberterrorismo ha sido objeto de estudio en diferentes ocasiones. Por ejemplo, en el estudio de Sánchez (2015) y desde su perspectiva, el ciberterrorismo es en un desafío estructural y funcional, no solo para los actores del Estado que se encargan del concepto de seguridad y defensa nacional, sino también para otras instituciones cuyo nivel de vulnerabilidades es superior.

Se habla entonces de terrorismo cibernético, que representa una amenaza no tradicional, y que afecta diferentes elementos sujetos al concepto “desarrollo” inter-sector. Otra postura

investigativa que permite establecer un hito con el cual justificar el proceso evolutivo del ciberterrorismo es la que ofrece Amado (2007).

La perspectiva de Amado (2007) se centra en el estudio del fenómeno desde la tipificación de su conducta delictiva. De acuerdo con el autor, el ciberterrorismo posee naturalezas criminales complejas; especialmente porque no se habla de autoría única o individualización de responsabilidades, pues en muchas ocasiones un ciber ataque es el resultado de la actuación de inteligencias artificiales inmateriales e intangibles.

La concepción teórica de Amado (2007), aunque abstracta desde la funcionabilidad tecnológica, es consecuente desde el planteamiento dogmático jurídico que exige el hecho de clasificar, explorar y analizar el fenómeno desde el argot legal, entendiendo que este último es un fenómeno de naturaleza hostil que goza de características y factores procedimentales complejos.

Con base en lo anterior, es imperativo que en Colombia se establezca esta tipificación de acciones, pues es necesario contextualizar el ciberterrorismo y regular los medios tecnológicos utilizados para la difusión de mensajes con fines terroristas, con los cuales generar caos, desesperación y coerción en el actor poblacional, desestabilizando la política de seguridad y defensa nacional.

Pero, para contextualizar, identificar y establecer patrones conexos al concepto terrorismo cibernético en el caso colombiano e incluso en el escenario internacional, es necesario estructurar un estudio exploratorio que conduzca al reconocimiento de factores determinantes que dinamizaron la evolución del terrorismo cibernético en el ciberespacio desde el año 2010 hasta el 2021.

Lo anterior, porque es fundamental plantear un núcleo de recomendaciones para mejorar la estrategia de ciber-defensa que regula al Estado colombiano, contando con el análisis de categorías evolutivas interrelacionadas al rápido avance del terrorismo cibernético

como fenómeno internacional, pero también como suceso de naturaleza nacional, adoptado por amenazas tradicionales y emergentes.

El periodo de tiempo seleccionado para esta investigación obedeció a dos delimitantes: incremento de ciber ataques registrados por la Secretaría de Seguridad Multidimensional de la OEA y transmutación de los elementos y escenarios en los que se emplea el terrorismo cibernético.

Siendo así, el lector encontrará primeramente un estudio del concepto terrorismo aplicado al ciber espacio. Es importante subrayar que el ciclo exploratorio no se centra únicamente en el análisis figurativo de amenazas tecnológicas con estándares de realización tecnificados, sino en amenazas tradicionales que han optado por utilizar la red o medios digitales para la ejecución de hechos delictivos.

Una vez analizado el concepto se pasa a la clasificación de factores que han influido en la evolución del ciber terrorismo desde el año 2010 hasta 2021. Acá, se dividen las amenazas en aquellas que gozan de complejidad digital y las que se cualifican en hibridad: tradicional y utilización de medios digitales.

Después del análisis de estos conceptos, se describirán los factores determinantes que condujeron a la evolución del terrorismo internacional generados en el ciberespacio desde el año 2010 hasta 2021, lo cual condujo al planteamiento de la siguiente tesis:

La evolución del ciber terrorismo ha sido un proceso secuencial sujeto a dos factores, el conocimiento y el desarrollo tecnológico. Su dinámica evolutiva ha ido a la par de fenómenos internacionales como la globalización y la hiper conectividad. Ahora, en el caso colombiano este fenómeno no es indiferente, ya que la utilización de medios tecnológicos por parte de grupos terroristas marcó un hito en el concepto asimétrico de la guerra.

CAPÍTULO I

Planteamiento de la Investigación

Estado del Arte

El terrorismo internacional cibernético se convirtió en una de las problemáticas con mayor número de impactos para el esquema de seguridad y defensa de los Estados (Rubio, Alcaraz, Román y López, 2019). De acuerdo con Conti, Dargahi y Dehghantanha (2018), las actividades ciberterroristas aumentaron en un 62% para 2021. Este aumento no solo representa una amenaza de tipología compleja; también presenta un núcleo de factores delictivos que se podría categorizar bajo el umbral de las nuevas guerras híbridas.

Para entender cómo el fenómeno se ha expandido en escenarios digitales cotidianos, es indispensable comprender su definición desde la perspectiva de Fernández (2018), citando a Barry Collin, quien aborda este problema, no una acción de naturaleza criminal, sino como un factor que está en constante cambio. Al respecto, el autor declama lo siguiente:

> (…) si la definición de terrorismo no tiene una aceptación general, aún menos un término tan bisoño como el ciberterrorismo. Tendiendo a la simplificación se podría denominar como la convergencia del ciberespacio y del terrorismo que fue adoptada por el creador del término ciberterrorismo, (Fernández, 2018, p. 134)

La definición *per s*e del término dista del posible núcleo de afectaciones que pudieren emerger por su expansión en sistemas y subsistemas de información. En la investigación *Internet, la nueva era del delito: ciber delito, ciberterrorismo, legislación y ciberseguridad*, Gamon (2017) explica cuán necesario es comprender el núcleo funcional del terrorismo internacional cibernético, mucho más porque su *core* cambia constante, se transforma y se adapta a nuevas circunstancias o necesidades delictivas del contexto.

La transformación del ciberterrorismo ha sido objeto de estudio en múltiples ocasiones. Por ejemplo, para Sánchez (2015) el ciberterrorismo es un desafío estructural y funcional, no solo para los actores del Estado que se encargan del concepto de seguridad y defensa nacional, sino también para instituciones con altos niveles de vulnerabilidad.

Se habla entonces, de un terrorismo cibernético que representa una amenaza no tradicional, y que afecta diferentes elementos sujetos al concepto *desarrollo* inter-sector. Otra postura que establecer un hito para justificar el proceso evolutivo del ciberterrorismo es la que ofrece Amado (2007). La perspectiva de Amado (2007) se centra en el estudio del fenómeno desde la tipificación de su conducta delictiva. Para el autor, el ciberterrorismo posee naturalezas criminales complejas; especialmente porque no se habla de autoría única o individualización de responsabilidades, ya que en muchas ocasiones un ciber ataque resulta de la actuación de inteligencias artificiales inmateriales e intangibles.

La postura que presenta Amado (2007), aunque abstracta desde la funcionalidad tecnológica, es consecuente desde el planteamiento dogmático jurídico que exige el hecho de clasificar, explorar y analizar el fenómeno desde el argot legal. Otra investigación que también busca explicar el proceso evolutivo del ciberterrorismo como acción de naturaleza criminal en contra del *statu quo* es la que presenta Medero (2015).

Medero (20215) realiza un análisis histórico del ciclo evolutivo del fenómeno y de allí salieron dos aspectos relevantes. Primero, que fenómenos como el terrorismo cibernético van de la mano de otras concepciones sociológicas como el desarrollo de los seres humanos, en especial, desarrollo tecnológico y transformaciones digitales ligadas a la interacción social. Segundo, que los ciberterroristas han hallado en el escenario digital un medio para difundir no solo terror poblacional, sino tan bien formas coercitivas que conducen a la presunción o disuasión de hecho.

En resumen, la evolución del ciberterrorismo es una consecuencia del avance tecnológico sin protocolos de control, supervisión o intervención.

Similar a la postura de Medero (2015), Poveda (2016) entra a este debate para explicar que el ciberterrorismo como conducta delictiva presenta características complejas, poco analizadas con la óptica de seguridad y defensa. Por ejemplo, la intromisión de los ciberataques, no desde el dominio tecnológico, sino desde el dominio mediático se presenta como una preocupación constante. Véase lo que autor expresa frente al hecho:

> Internet se ha convertido en la mayor plataforma de expresión disponible en todo el mundo. Hoy en día se puede encontrar todo tipo de material en la red, y resulta casi imposible para los diversos servidores y los gobiernos controlar todo el contenido que se vierte sobre el ciberespacio. De ahí que las nuevas tecnologías, y en concreto Internet, ofrezcan a los grupos terroristas vías alternativas (o más bien complementarias) para difundir libremente, sin prácticamente censuras, sus mensajes (Poveda, 2015, p. 101)

Un punto de vista importante que Medero (2015) trae a colación es la exposición de relación que hay entre el internet como factor de transmisión, y el mensaje terrorista. Esto quiere decir que el terrorismo cibernético no se centra únicamente en la utilización tecnológica especializada de los sistemas de información, pues hay otras formas con las que se incurre en el marco delictivo.

La explicación de una de esas formas está en el documento que titula Capacidades Prospectivas y de Defensa en la Lucha en Contra del Ciberterrorismo, publicada por González y González (2020). Se argumenta que la diversificación de ciber-ataques y ciber-crímenes se ha dado con el tiempo, por una necesidad categorial. Esa necesidad reposa en la clasificación de tipología de conductas criminales en la red.

Como se planteó con anterioridad, el terrorismo digital de naturaleza internacional no siempre acude al uso de ciberataques por medios tecnológicos complejos, sino a la difusión de mensajes perceptivos que se esparcen de forma inmediata.

Una explicación de la condición *forma inmediata* podría extraerse de los postulados investigativos de Cespedosa (2019). El ciberterrorismo encontró en el internet un canal de difusión, el cual expande límites tangibles y acelera los alcances persuasivos del actor terrorista. Véase, por ejemplo, que la red social YouTube fue, hasta cierto punto, un canal de difusión para el grupo terrorista ISIS (Weimann, 2010).

Las descripciones investigativas dadas hasta este punto del Estado del arte se remiten a la búsqueda de las categorías: ciberterrorismo, evolución y factores de cambio. Ahora, con el fin de aumentar el proceso objetivo de la búsqueda se pasa al siguiente grupo de categorías: ciberterrorismo, terrorismo internacional y sociedad actual. De esa búsqueda salieron dos resultados. El primero se encuentra en la investigación titulada Alcances del Ciberterrorismo en la Sociedad Contemporánea, publicada por Reyes (2014).

Para Reyes (2014), el ciberterrorismo evolucionó en diferentes campos para el desarrollo humano. Sobre todo, en contextos digitales comunicativos. En ese nicho, los actores terroristas digitales encontraron formas de intercomunicación o con sus actores subordinados o con audiencias antes inalcanzables.

Frente a la categoría de lo *contemporáneo*, el ciberterrorismo habría crecido gracias al avance de medios tecnológicos de impacto como la tecnología 4G, pero también al número o cantidad de usuarios que poseen acceso a la red. En otros términos, a mayor audiencia, mayor impacto.

Otra investigación también relacionada titula *La Innovación Yihadista: propaganda, ciberterrorismo, armadas y tácticas*, publicada por Jesús (2009). Si bien esta investigación es atemporal para el rango de búsqueda del Estado del arte, sí es apropiada para comprender cómo

innovación y *terrorismo* forman ecuaciones sociológicas de impacto negativo a macro-escala. Según Jesús (2009), grupos como Al Qaeda o el Estado Islámico han empleado las tecnologías de la información y las comunicaciones para expandir terror; de una manera más efectividad y más eficiente.

No obstante, debe reconocerse que no solo ha sido el uso de estas tecnologías el elemento relevante. Lo anterior, porque el mensaje diseñado es el componente que más impactos ha causado, en especial cuando este se conecta con variables sociológicas que generar miedo, confusión y coerción. Un aspecto ejemplificante es el uso de las redes sociales para expandir mensajes asociados al concepto *nuclear* o *destrucción masiva*.

La búsqueda de antecedentes investigativos permitió instaurar un análisis categórico con el cual hallar dos vacíos en el conocimiento. Ambos vacíos son conducen al proceder de esta investigación. Los vacíos son:

- Ausencia de investigaciones con las cuales estudiar el ciclo evolutivo que ha presentado el fenómeno ciberterrorismo o terrorismo cibernético. Es decir, investigaciones con las que se expliqué como ha cambiado esta amenaza, y bajo que hitos o elementos sociológicos e históricos lo ha hecho.
- Segundo, no hay investigaciones en las que se aplique una búsqueda categorial para clasificar las variables conexas al ciberterrorismo o terrorismo cibernético.

Formulación del problema

¿Cómo ha sido el proceso evolutivo llevado a cabo por el terrorismo cibernético internacional entre el periodo temporal 2010 - 2021?

Objetivos de la investigación

Objetivo general

- Identificar los factores determinantes que han permitido la evolución del terrorismo internacional generado en el ciberespacio desde el año 2010 hasta el año 2021.

Objetivos específicos

- Analizar el concepto del terrorismo aplicado en el escenario ciberespacial.
- Categorizar los factores que han influido en la evolución del ciberterrorismo desde el año 2010 hasta el año 2021
- Proponer recomendaciones a la estrategia de ciberseguridad y ciberdefensa de Colombia, teniendo en cuenta las categorías evolutivas del ciberterrorismo.

Metodología

La investigación es de enfoque cualitativo. Su diseño es exploratorio secuencial y el método por utilizar es descriptivo-deductivos, buscando así explorar el núcleo problemático hasta llegar a la deducción de resultados, conclusiones, recomendaciones y elaboración del proceso de triangulación. Para llevar a cabo esta investigación se utilizarán cuatro Fases:

- Fase uno, indagación teórica y búsqueda de hitos históricos a través de la relación de un ejercicio de análisis e identificación de hitos históricos ocurridos entre 2010- 2021.
- Fase dos, una vez explicada la teoría y desarrollado el ejercicio de revisión se pasará a un análisis. Con el fin de realizar una correlación, comparación y deducción de patrones característicos.
- Fase tres, descripción de resultados y aplicación de un análisis de revisión de medios para establecer categorías difusivas asociadas el proceso evolutivo del terrorismo cibernético.
- Fase cuatro, triangulación de resultados.
- Fase cinco, redacción de conclusiones, recomendaciones

CAPÍTULO II
Marco de Referencia

Marco teórico

Terrorismo Cibernético, Sistemas de información e interacción humana

Para comprender el tema de terrorismo cibernético hay que conceptualizar dos puntos de interés. Por un lado, explicar que terrorismo cibernético no solo acude a esa concepción de surgimiento de amenazas cibernéticas técnicas, complejas, de tipología digital, con orígenes humanos. El terrorismo cibernético también hace alusión a la utilización de medios, métodos y sistemas de información digitales, con los cuales difundir acciones que conlleven a la intimidación, coacción o coerción.

Por el otro, comprender que el concepto terrorismo cibernético también se inclina a la hibridación entre medios cibernéticos, objetivos terroristas y actores delincuenciales en plena transición, cambio o trasmutación inter-sistémica.

Por ejemplo, al interpretar la postura de Manrique (2021), se diría que el ciberterrorismo no debe observarse o estudiarse con la lógica de lo tecnológico o sistemático exclusivamente, pues también hay que explorarlo con la óptica de disrupción en campos básicos como los derechos fundamentales u otro tipo de afectaciones con efecto multidimensional. El ciber espacio es un escenario en el que convergen instituciones, empresas, personas naturales y un alto volumen de datos; de ahí que el Estado sostenga responsabilidades garantes, conexas al marco de la seguridad y defensa nacional.

Hay de facto, correlación e interrelación entre un usuario digital y un sistema de información que en ciertas ocasiones puede estar vulnerable ante diversos riesgos. Una acotación interesante que plantea Manrique (2021) es que cualquier tipo de impacto causa alteración o disrupción al ser humano, específicamente a sus derechos fundamentales.

La perspectiva que expone Manrique (2021) no es errada, es más, si se comprendiera que en ciertas situaciones la vida un ser humano depende de sistemas de información médicos,

atados a una estructura de función pública, se comprendería un poco más la aseveración de Manrique.

Una ciber afectación, entendida esta el ataque directo de naturaleza cibernética, desestabiliza sistemas tecnológicos cuyo fin es específico, y se une con esa concepción de lo socio-humanístico cotidiano. Una muestra para asimilar esta afirmación es que el número de usuarios cibernéticos crece año tras año, incrementando la exposición del actor digital a escenarios en los que converge la poca experiencia, el desconocimiento técnico y centros de gravedad criminal digital, diseñados para extraer o secuestrar información o para generar impactos sociológicos, producto del empleo de redes cibernéticas.

Similar a la postura de Manrique (2021), Echeverria (2017) entra en esta discusión para debatir que el terrorismo cibernético no solo produce afectaciones a la vida humana como tal, también produce impactos a otros campos asociados con el desarrollo inter-sector. Es más, al respecto Echeverría (2017) estima que la concepción geopolítica del terrorismo cibernético va cambiando y se aproxima más al uso de los medios que a la creación de nuevas ciber amenazas.

Eso significa que hay sectores, territorios y Estados en los que la propensión de uso de tecnología para establecer acciones terroristas es mayor, o su acceso es más fácil. Un aporte interesante que se asocia con el tema de la geopolítica cibernética es el concepto de ciber biografía. Mírese la siguiente afirmación para continuar con la investigación:

La ciber biografía estudia las redes de comunicación computacionales, en la cual la Internet, los sitios Web, la World Wide, redes sociales, plataformas móviles, entre otros, es lo que comprende el Ciberespacio, el cual es un espacio geográfico hecho por el hombre, que está en constante cambio y que por lo tanto sus propietarios es cada persona que ocupe un lugar en el espacio, cuando se quiere causar daño o hacer terrorismo por este medio no se necesita movimiento físico para hacerlo simplemente se necesita de un espacio computacional en la esfera del universo (Manrique, 2017, p. 12)

El término ciber-biografía acude a una definición con la cual se explica que, en el escenario digital, si bien no hay límites, sí hay valores de concentración que reflejan un mayor o menor flujo de interacción. Esa mayoría o minoría está determinada por factores estadísticos como la cantidad de población que tiene acceso a internet, la calidad de los sistemas de conexión y, sobre todo, el conocimiento cibernético de los usuarios digitales.

Entonces, entender cómo funciona el ciber terrorismo con la óptica de lo socio-demográfico y jurisdiccional, implica establecer de qué manera ocurren los hechos terroristas vinculados con lo cibernético y de qué forma este fenómeno ha venido transmutando. Para entenderlo, hay que analizar la postura constructivista que de Carlini (2016).

De acuerdo con este autor, el terrorismo cibernético como fenomenología delictiva ha aumentado a la par de dos factores contextuales: la tecnología como canal dinámico y la estructuración de estrategias de defensa cibernética con las que se considera a esta última un interés de tipología estatal.

Por un lado, la tecnología representa una inversión no estática. Todo lo contrario, sus avances han dejado brechas tecnológicas y epistemológicas que causan inequidad entre el actor poblacional, los Estados y otras condiciones conexas al ser humano. Entender este punto amerita comprender que, con el avance tecnológico, otras acciones delictivas cambiaron y en algunos casos se combinaron.

Esa combinación formó amenazas híbridas que no tienen por obligación algún tipo de consideración tecnológica. Es decir, la hibridad en este caso se aproxima a la utilización de medios para dispersar componentes propios del terrorismo, y no para crear amenazas cibernéticas complejas.

Entonces, obsérvese que por ciber terrorismo no se entendería a la inmersión de facto; pues hay otras aristas que empiezan con la acción y/o determinación de una conducta humana y terminan con la utilización de sistemas de información que causan algún tipo de afectación.

En la investigación que titula *Ciberseguridad: un nuevo desafío para la comunidad internacional*, Carlini (2016) analiza múltiples espectros que conforman un ciberataque, determinando de manera explícita que estos no solo dependen de la inmediatez tecnológica, ya que hay otros elementos subsecuentes que hacen parte de la acción. Por ejemplo, su catalogación como amenaza para el Estado, la estructuración de estrategias de intervención o prevención o la simple interacción entre los usuarios digitales (factor socio humanístico) y sistemas tecnológicos complejos, cuyo funcionamiento expone una brecha de conocimiento que crece de manera exponencial.

Ciberterrorismo y concertación de nuevos planteamientos conceptuales; una explicación praxeológica del hecho delictivo.

Para comprender cómo el terrorismo cibernético llegó a ocupar un campo importante en el devenir desarrollista del ser humano, hay que conceptualizar primeramente que por terrorismo cibernético debemos entender todo acto, acción u ofensa que pueda poner en riesgo la integridad de un usuario digital o al sistema de información *per se*.

Explorar esta concepción permite entonces incluir perspectivas constructivistas las cuales entran al debate para analizar dos puntos: cuáles son las perspectivas que se centran en la referenciación del ciber terrorismo como amenaza a la seguridad y defensa nacional, y qué factores forman parte de esa perspectiva.

Pues bien, el primer interrogante se resuelve al incluir el argumento de Mahan y Griset (2003). Según estos autores, el terrorismo cibernético plantea perspectivas múltiples y desafiantes a la vez. Sus objetivos pueden ser culturales políticos, económicos o religiosos. Ahora, aunque su objetivo cambie, el medio siempre será cibernético. Por esa razón, este fenómeno debe ser considerado estático de naturaleza, pero altamente evolutivo o cambiable desde la intensión propuesta por un ciber atacante.

Las perspectivas que se tienen frente al terrorismo cibernético, particularmente, van cambiando a medida que el concepto tecnológico va evolucionando. Pero entonces, véase que no solo cambian ciertos elementos en el medio, pues el cambio también se nace el objetivo del ciber ataque. Siendo así, comprender el ciber terrorismo desde su rápida evolución llevaría esta discusión a una siguiente etapa en la se vuelve necesario conocer cómo y porqué cambian las amenazas cibernéticas.

Una apuesta interesante para analizar ambas preguntas surge en la investigación de (Nye, 2013). Para este autor, el futuro cibernético está compuesto por sucesos de entorno ligados a sistemas de información que tienen como cualidad primaria la posibilidad de alterar o cambiar el proceso desarrollista de los actores poblacionales.

Para Nye (2013), la evolución de las ciber amenazas se presenta en el cambio estructural de los ciber ataques. En otros términos, no solo evolucionan los sistemas de información, sino también las técnicas de dispersión e incluso, los modos humanos empleados para estructurar ataques ciber terroristas.

CAPÍTULO III
Caracterización del terrorismo

A lo largo de la historia de la humanidad, diversas construcciones sociales han recurrido al uso de la fuerza para defender sus intereses comunes, garantizar su sostenibilidad socioeconómica, periodos de estabilidad y paz frente a otras agrupaciones, e incluso proyectar el crecimiento de su población e instituciones públicas.

Con el paso del tiempo, estas prácticas se han atribuido como una de las principales funciones del Estado, en donde bajo su administración, este ha tecnificado sus mecanismos y protocolos de uso legítimo, teniendo como objetivo principal preservar la seguridad, prevenir amenazas o resolver conflictos frente a otros Estados.

Frente a lo anterior, y teniendo en consideración los recurrentes conflictos que han demostrado la gravedad de las practicas del uso de la fuerza, como las expuestas en los escenarios que abarcan casos como los evidenciados en la Primera y Segunda Guerra Mundial (entre otros), instituciones nacionales e internacionales, han establecido un sistema normativo que tenga por finalidad priorizar los derechos de la ciudadanía, restricciones mínimas para la conservación de mínimos vitales en la dignidad y prevención de acciones que generen consecuencias irreparables en el territorio afectado.

Resultado de esto, el plano internacional constituyó el Derecho Internacional Humanitario, o derecho a la guerra, el cual se define por la CICR (2004) como:

> Un conjunto de normas que, por razones humanitarias, trata de limitar los efectos de los conflictos armados. Protege a las personas que no participan o que ya no participan en los combates y limita los medios y métodos de hacer la guerra. (…) El DIH es parte del derecho internacional, que regula las relaciones entre los Estados. Está integrado por acuerdos firmados entre Estados –denominados tratados o convenios–, por el derecho consuetudinario internacional que se compone a su vez de la práctica de los Estados que éstos reconocen como

> obligatoria, así como por principios generales del derecho. El DIH se aplica en situaciones de conflicto armado. No determina si un Estado tiene o no tiene derecho a recurrir a la fuerza. Esta cuestión está regulada por una importante parte –pero distinta– del DIH, que figura en la Carta de las Naciones Unidas. (p. 1)

Organizaciones como las Naciones Unidas, se han destacado en la construcción de la regulación de los conflictos internacionales y verificación de la normativa previamente descrita, priorizando la consolidación de sociedades estables y pacíficas, determinando por medio del consenso, la emisión de resoluciones y la gestión de cambios en las normativas o protocolos de acciones de manutención de la seguridad interna de sus Estados miembros. Para la construcción de un plano internacional interconectado por medio de agendas para el desarrollo sostenible y mecanismos para la resolución pacífica de controversias. Sin embargo, el desarrollo de los escenarios políticos, junto con la construcción de los Estados y sus instituciones, han consolidado grupos al margen de ley o individuos con nuevas visiones de la esfera política local y mundial. Los cuales, por medio del uso de la fuerza, causan una disrupción negativa en la evolución de la guerra, el desarrollo de los conflictos y la configuración de las prácticas que determinan los actos de violencia.

Tras los compromisos anteriores, Estados como Colombia, anexaron a su agenda pública una serie de objetivos que permitieran, a partir del fortalecimiento de sus fuerzas de seguridad, atender nuevas amenazas que han ampliado sus concesiones y alcance, tras lo surgimientos de agrupaciones al margen de la ley, individuos u otros actores, los cuales ante el desarrollo político y su influencia en el desarrollo de la ciudadanía, ha constituido escenarios de violencia por medio del surgimiento de crisis, afectaciones a los derechos fundamentales de la población víctima entre otras acciones, que han priorizado al terrorismo como un problema público prioritario.

En el plano internacional, hitos históricos como los ocurridos durante el 9-11, han visibilizado una problemática que, si bien presenta orígenes previos de esta fecha en la historia de la humanidad, este puede considerarse, como el punto de partida del terrorismo actual, el cual bajo el uso de instrumentos de presión política o ruptura del estatus quo en el desarrollo de las dimensiones políticas actuales, busca generar cambios sociales y políticos por vías violentas.

Una aproximación al concepto de terrorismo en el territorio.

Para abordar el estudio del terrorismo, sus características y su aplicación en la regulación del Estado colombiano, es necesario hacer un análisis histórico de su evolución con base en la influencia que este ha tenido frente al desarrollo del conflicto armado interno. Para esto, el presente capítulo abordará un estudio del alcance por medio del análisis de los conceptos que se tienen de la práctica y sus aplicaciones en el caso colombiano.

Entre las definiciones que destacan al terrorismo, se encuentra la expresada por la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, la cual lo establece como:

> (…) actos criminales con fines políticos concebidos o planeados para provocar un estado de terror en la población en general, en un grupo de personas o en personas determinadas», y que esos actos son «injustificables en todas las circunstancias, cualesquiera sean las consideraciones políticas, filosóficas, ideológicas, raciales, étnicas, religiosas o de cualquier otra índole que se hagan valer para justificarlos. (OHCHR, 2011., p. 11)

Las principales características que se pueden abstraer de la definición, permiten establecer que el terrorismo o la catalogación de un acto terrorista es el fin de las acciones emprendidas y su influencia en las esferas políticas, es decir, los actos terroristas requieren causar un impacto en el desarrollo político de los Estados para ser categorizados como tal, y

estos deben buscar directamente o indirectamente cambios en el desarrollo y constitución de las instituciones públicas. Por otra parte, los actos de terrorismo presentan un cambio determinante en el desarrollo de la administración legitima de la fuerza, en un sentido de guerra regular, esta facultad recae en los Estados las cuales se manifiestan a través de sus instituciones y fuerzas de seguridad, sin embargo para el desarrollo del terrorismo, un individuo puede hacer uso de la fuerza y la violencia para garantizar un fin político, complejizando el desarrollo y las acciones construidas en el derecho de la guerra justa, ya que en su aplicación los grupos o individuos terroristas constituyen una amenaza que desdibuja las fronteras entre los derechos de la ciudadanía, los no combatientes y los protocolos que se tenían dispuestos para el manejo de conflictos.

De otro lado, y según la legislación colombiana, el terrorismo puede definirse como:

> Mientras subsista turbado el orden público y en estado de sitio todo el territorio nacional, el que provoque o mantenga en estado de zozobra o terror a la población o a un sector de ella, mediante actos que pongan en peligro la vida, la integridad física o la libertad de las personas o las edificaciones o medios de comunicación, transporte, procesamiento o conducción de fluidos o fuerzas motrices valiéndose de medios capaces de causar estragos incurrirá en prisión de diez (10) a veinte (20) años y multa de diez (10) a cien (100) salarios mínimos mensuales, sin perjuicio de la pena que le corresponda por los demás delitos que se ocasionen con este hecho.
> Si el estado de zozobra o terror es provocado mediante llamada telefónica, cinta magnetofónica, video, cassette o escrito anónimo, la pena será de dos (2) a cinco (5) años y la multa de cinco (5) a cincuenta (50) salarios mínimos mensuales (República de Colombia, 1980, Art 187).

Según lo anterior, y bajo el análisis de la normatividad colombiana, una de las principales características del terrorismo, parte del establecimiento de un estado de terror o bajo condiciones que atenten en contra de los derechos y calidad de vida de la población en términos de la amenaza a su seguridad humana el desarrollo económico y social de la población. De igual forma, este establece que su manifestación puede categorizarse desde la acción directa y presencial, así como mediante las acciones perpetradas en los campos digitales.

Ante lo anterior, se podría establecer entonces que, los principales elementos que componen al terrorismo, se circunscriben en el la infusión del terror a una o más víctimas, con la finalidad de compartir una ideología o pensamiento que implique la reestructuración de la normatividad de un Estado y las figuras e instituciones que lo componen, destacando que el terrorismo es una práctica etérea que no requiere el exclusivo uso de la fuerza, sino que esta puede involucrar otros actos o conductas delictivas para su sostenibilidad en espacios determinados.

Del mismo modo, diversos autores en el estudio de la definición del terrorismo han determinado que esta es una estrategia que puede partir de una ideología, en la que convergen los siguientes elementos:

- El uso o amenaza del uso de la fuerza.
- Tal uso o amenaza es un medio de combate o elemento en una estrategia para lograr ciertos objetivos.
- El propósito es inducir un estado de miedo en las víctimas.
- La fuerza se usa sin consideración alguna, o bien no se ajusta al uso de las normas humanitarias.
- La publicidad de los actos es un elemento esencial.

Esto quiere decir que bajo el estudio de los diversos casos y definiciones que presenta el terrorismo a nivel nacional e internacional, este converge en una serie de características que

determinan las conductas catalogadas como actos de terrorismo; es por eso que a continuación se caracterizarán las principales variables que constituyen actos como acciones de terrorismo y su influencia en la seguridad y cumplimiento de los derechos fundamentales de la población que pueda ser víctima de dichos actos.

Análisis de la evolución del ciberterrorismo como amenaza de tipología nacional

El terrorismo cibernético como una amenaza a la estructura de seguridad y defensa nacional tiene debe analizarse con una concepción praxeológica que se interconecte con el avance tecnológico del internet. Tal y como se llegó a observar en las posturas conceptuales del marco teórico, hay argumentación suficiente para definir dos aspectos característicos del terrorismo cibernético.

El primero es que su rápida dispersión, difusión y evolución ha ido a la par de los nuevos descubrimientos en materias de conectividad. Es por eso que un ciber ataque de 1999 no se puede comparar con una afectación en el escenario digital tipo *cloud*.

Ahora, aunque diferentes, los dos ataques dependen del componente tecnológico. De ahí que el segundo aspecto sea la naturaleza de la amenaza cibernética. Al respecto, debe examinarse que el medio tecnológico de difusión o ataque siempre será estático. Esto no quiere decir que el componente tecnológico ralentice su evolución; todo lo contario, esta afirmación debate el proceso evolutivo de lo tecnológico, y sitúa como factor de cambio la intención – objeto del ciber atacante. En otros términos, la evolución del ciber terrorismo se ha dado en dos facetas: cambios tecnológicos y transmutación intencional del actor delincuencial.

Para comprender cómo ha evolucionado este tipo de terrorismo, el proceso de investigación acude a tres parámetros explicativos. El primer parámetro describe la expresión *uso de internet con fines terroristas* propuesto en el informe de la Oficina de las Naciones Unidas Contra la Droga y el Delito. El segundo distingue y caracteriza la relación que hay entre

ciber ataques y evolución *tech*. El tercero explica cómo la tecnología ha facilitado la implementación de acciones con miras y objetivos terroristas, a partir de una práctica común: la utilización de medios tecnológicos para el ejercicio del terrorismo una figura estructural de coacción y coerción.

La explicación del primer parámetro comienza con la siguiente afirmación:

> Desde finales de la década de 1980, Internet ha demostrado ser un medio de comunicación sumamente dinámico, que llega a un público cada vez mayor en todo el mundo. El desarrollo de tecnologías cada vez más sofisticadas ha creado una red con un alcance verdaderamente mundial y barreras al acceso relativamente bajas. La tecnología de Internet hace que resulte fácil para una persona comunicarse con relativo anonimato, rapidez y eficacia, a través de las fronteras, con un público casi ilimitado (UNODC, 2013, p. 4).

Esta afirmación confirma lo que se trató en el marco teórico, y es que, a mayor acceso y conectividad, mayor probabilidad o propensión al riesgo. Véase que la incursión formal del internet en 1980 vino acompañada de acciones contextuales cuya animadversión radicó en la utilización de internet con fines delictivos (Ver figura 1)

Figura 1 Forma de virus en 1980

Fuente: información recuperada de Avast (2022)

Es decir que no se habla de ciber terrorismo o de ciber amenazas por la complejidad que contienen sus códigos de función, sino por el uso de la red como un medio para realizar acciones criminales.

Eso reitera la primera idea expuesta, la cual explica que el terrorismo cibernético no cambia y/o avanza por su evolución macro-tecnológica, pues la intención de los ciber atacantes varia, cambia y determina cuál será el uso que debe darse a un sistema de información, herramienta digital o escenario virtual.

La premisa expuesta se confirma cuando se explora el documento El Uso de Internet con Fines Terroristas. De acuerdo con el documento y con la UNDOC (2013), uno de los primeros usos dados a la red y que planteó como fin el terrorismo fue la propaganda inter mediática.

Esta propaganda comenzó con la demostración de actos violentos en contra de un grupo poblacional específico y finalizó con la difusión de narrativas terroristas cuyo fin primario era convencer al actor poblacional o reclutarlo. De hecho, esta última acción es considerada otro de los fines ligados al terrorismo cibernético.

La propaganda digital difundida en internet y la cual tiene como fin influenciar la conciencia colectiva es una acción de naturaleza ciber que empieza a tomar fuerza desde 2003 (Enghelberg, 2003), año en el que se registró un número aproximado de 1.787 videos extremistas que buscaban difundir terror en el escenario poblacional. Este tipo de incidencias, es decir, de amenazas emergentes, dio vida a la configuración de nuevos enfoques securitistas como el de *seguridad multidimensional*, propuesto por primera vez en la Declaración de Bridgetown (Organización de Estados Americanos, 2003).

La propaganda como un instrumento de difusión de *retórica extremista* (UNDOC, 2013), fue el principio de esa concepción ciber terrorista que empezaría a evolucionar paralelo a los sistemas de información. Una versión similar, es decir, una postura conceptual allegada a la versión de UNDOC (2013) es de la que propone Enghelberg (2003) al reconocer que las actividades de grupos extremistas a principios del siglo XXI hallarían en el terrorismo cibernético una forma fácil, económica y audaz para retransmitir un mensaje o intención.

Esa combinación de lo tecnológico con lo cibernético y terrorismo, desde la perspectiva de Enghelberg (2003) forma un escenario hostil caracterizado por diferentes componentes asimétricos.

Así los términos, el terrorismo cibernético no se reconocería únicamente como un arma empleada por avanzados grupos terroristas cuyo conocimiento tecnológico es amplio, sino también por insurgencias tradicionales que vieron en el ciber espacio un escenario de afectación que produce mayores impactos y que reduce la cantidad de riesgos prominentes.

Seguido a la propaganda, viene el tema de la incitación. Con incitación, UNDOC (2013) refiere a acciones retransmitidas a través de propaganda que llevan a un actor social a desarrollar acciones físicas, disruptivas, de naturaleza terrorista. Este punto de vista es interesante si se tiene en cuenta que se está hablando de hibridad.

Al respecto, en la investigación que titula Terrorismo e información: análisis de los videos de Al-Qaeda, Agejas, (2004) realiza un estudio de las amenazas en contra de periodistas y de población civil, producto de la incidencia de Al-Qaeda en sociedades europeas. Uno de los aspectos más relevantes, hallados en la revisión de las piezas gráficas, es la incitación del grupo terrorista, para que sus fieles, colaboradores u otro tipo de actor social que sienta afinidad lleve a cabo acciones violentas, cuya característica sea disrupción mediática.

Se observa entonces, que el terrorismo cibernético desde la propaganda y la incitación toma el precepto de lo cibernético no como un arma *ad hoc*, sino como un medio difusivo. Tal particularidad viene a verse en sus primeros años, es decir, cuando la difusión de videos a través de la red se volvió accesible e incluso, con la tecnología 3G permitió el ingreso a sistemas de información que retransmitían piezas gráficas a velocidad considerable.

Ahora, las informaciones registradas en esta primera parte concretan grosso modo que el ciber terrorismo en sus primeras instancias tiene que explorarse, no desde el enfoque tecnológico o cibernético, sino más bien desde los usos procedentes que se dieron ante el rápido crecimiento de la red y por supuesto, desde el avance del internet con sistema de información, y el aumento sucesivo de nuevos usuarios digitales.

Habiendo delimitado esta primera parte a una explicación con la que se llega a describir que el terrorismo cibernético presenta dos facetas, el uso de internet y la creación macro-tecnológica e ciber amenazas, se pasa a la siguiente parte del estudio la cual compete al análisis evolutivo de las ciber amenazas, pero a partir de esa sujeción constante entre el uso de los sistemas de información, la red y el rápido avance de la tecnología.

Para comprender esta parte, hay que aclarar que la hiper conectividad traída a colación con la globalización tecnológica, y trajo consigo nuevas amenazas cibernéticas, la cuales, al emerger con mayor número y potencia crean un espectro geográfico del terrorismo cibernético poco estudiado con la óptica de la geopolítica.

En la investigación que titula Análisis de los ciber ataques realizados en América Latina, Izaguirre (2018), habla de los riesgos en el ciberespacio. Llama la atención que el 90% de esos riesgos tienen relación con la objetividad humana. No hay ciber amenazas o acciones que encajen en el marco del terrorismo cibernético con autonomía, determinación o capacidad para la selección de blancos estratégicos.

Todo lo contrario, Izaguirre (2018) da a entender que el terrorismo cibernético ha evolucionado por la voluntad humana y por la intención de sus actores precursores. Siendo así, esta postura permitiría plantear una hipótesis de frente al análisis evolutivo de las acciones que comprenden un posible acto de ciber terrorismo. Dicha hipótesis explica que la evolución del ciber terrorismo ha hallado en la intención de los actores criminales, en su alcance tecnológico y la facilidad de acceso y difusión, un arma que poco a poco va interviniendo en los campos de acción cibernética que presenta una sociedad, así como también en sus nuevas invenciones. De ahí que el terrorismo cibernético del 2003 no se asimile con el de 2022, el cual actúa bajo la premeditación de inteligencia artificial.

La perspectiva que propone Izaguirre (2018) explica el tema cibernético desde un enfoque sistemático. En otros términos, en cuanto más sistema de información existan más oportunidades tendría un ciber terrorista para atacar.

Así como Izaguirre (2018), Cano (2018) explica que la rápida evolución de las amenazas cibernéticas y por dende, de las acciones terroristas tecnológicas se debe a la concepción de nuevos componentes tipo tech. Cano (2018) explica que hay factores como el incremento de la velocidad de conexión e incluso la asociatividad delictiva de los ciber atacantes, que incrementan la posibilidad de afectación.

Aunque su postura no solo se centra en el ciberterrorismo pues también se enfoca en el ciber delito, sus aportes sí resultan ser apropiados para entender dos puntos de vista. Primero, el ciber terrorismo encontró en la deficiencia de los sistemas de seguridad y defensa cibernética

una oportunidad para, en algunas ocasiones, superar las estrategias públicas diseñadas para contener el avance y alcance de las acciones terroristas – cibernéticas.

Segundo, el ciber terrorismo halló en el desconocimiento y brecha tecnológica un rápido canal de avance, movimiento y afectación. La brecha tecnológica es un punto de discusión que se dará cuando esta investigación se centre en el proceso evolutivo del ciber terrorismo en Colombia. Por el momento es necesario comprender esto:

> Cierto es que los criminales van siempre por delante de las fuerzas de seguridad, por lo que otra de las circunstancias que correría a favor de Al-Qaeda iba a ser la denominada brecha tecnológica. Esta circunstancia originaría los primeros cambios a finales de la década de los noventa, provocando que los servicios de seguridad e inteligencia no pudieran hacer frente a la ingente cantidad de tráfico de datos circulando a una velocidad vertiginosa por toda la Red. Así, incluso con el mayor sistema de interceptación y vigilancia de las telecomunicaciones e Internet (incluyendo el correo electrónico), puesto en marcha por algunas agencias de seguridad, no se pudieron evitar los atentados de Al-Qaeda del once de septiembre (11-S) en los EE. UU., o los ataques terroristas posteriores (Estarellas, 2011, p. 12).

Matriz de caracterización de eventos

De acuerdo con lo anteriormente expuesto, donde podemos evidenciar que la contextualización de eventos en cuanto a terrorismo convencional o delito y ciberterrorismo o ciberdelito, es muy compleja en razón a que se debe analizar desde diversas aristas; se plantea la siguiente matriz de caracterización de eventos con la finalidad de poder comparar los diferentes factores que se pueden evidenciar en algunos casos y de esta forma poder delimitar el evento.

Figura No 2 Matriz de caracterización de eventos

MATRIZ DE CATEGORIZACION DE EVENTOS							
EVENTO:		CASO TIMOTHY WILSON: Explosion Carro bomba Hospita en Belton (Missouri), motivado por la animosidada racial - religiosa - antigubernamental, ya que este sujeto suponia que los Juidos utilizaban la pandemia para realizar la toma del poder, este sujeto era el administador de un grupo en telgram "The Order" y tenia vinculos en telegram con dos organizaciones Neonazis "NSM" y "VSD"					
CIUDAD:		MISSOURI					
FACTORES			VALOR	TERRORISMO CONVENCIONAL	CIBERTERRORISMO	DELITO	CIBERDELITO
AMBIENTE VIRTUAL	MEDIOS TECNOLOGICOS	APLICACIONES VARIADAS	1	0	1	0	1
		SOFTWARE	1	0	1	0	1
	MÉTODOS	ATAQUES CIBERNETICOS	1	0	1	0	1
		INTELIGENCIA ARTIFICIAL	1	0	1	0	1
		MANIPULACIÓN REDES SOCIALES	1	0	1	0	1
		FAKENEWS	1	0	1	0	1
		MANIPULACIÓN INFORMACIÓN PERSONAL E INSTITUCIONAL	1	0	1	0	1
		MANIPULACIÓN DE SOFTWARE	1	0	1	0	1
VÍCTIMAS	NUMERO INDISCRIMINADO	MUERTES	1	1	1	1	1
		VIOLACION DE DERECHOS HUMANOS	1	1	1	1	1
		SEGURIDAD HUMANA	1	1	1	1	1
		LIMITACIÓN DE SERVICIOS ESENCIALES	1	1	1	1	1
	INDIVIDUAL	MUERTES	1	0	0	1	1
		VIOLACION DE DERECHOS HUMANOS	1	0	0	1	1
		SEGURIDAD HUMANA	1	0	0	1	1
		LIMITACIÓN DE SERVICIOS ESENCIALES	1	0	0	1	1
FINES	IDEOLÓGICOS	PROPÓSITOS FUNDAMENTALISTAS	1	1	1	0	0
		IMPOSICIÓN PERSPECTIVAS (Derecha - Izquierda)	1	1	1	0	0
	POLÍTICOS	DESESTABILIZACIÓN DEL ESTADO	1	1	1	0	0
		TOMA DEL PODER - INSURGENCIA	1	1	1	0	0
	ECONÓMICOS	ACUMULACIÓN RIQUEZA	1	0	0	1	1
		SECUESTRO	1	1	1	1	1
		EXTORSIÓN	1	1	1	1	1
		EXPANSIÓN NARCOTRÁFICO	1	0	0	1	1
USO DE LA FUERZA	INTIMIDACIÓN	MEDIOS FÍSICOS	1	1	1	1	1
		MEDIOS VIRTUALES	1	0	1	0	1
	VIOLENCIA	FÍSICA	1	1	1	1	1
		PSICOLÓGICA	1	1	1	1	1
		INTELECTUAL	1	1	1	1	1
GENERACIÓN DE MIEDO	POBLACIÓN	AFECTACIÓN COLECTIVA (AUDIENCIA)	1	1	1	1	1
	INDIVIDUO	AFECTACION DE CARÁCTER PERSONAL	1	0	0	1	1
TOTALES				15	24	18	27

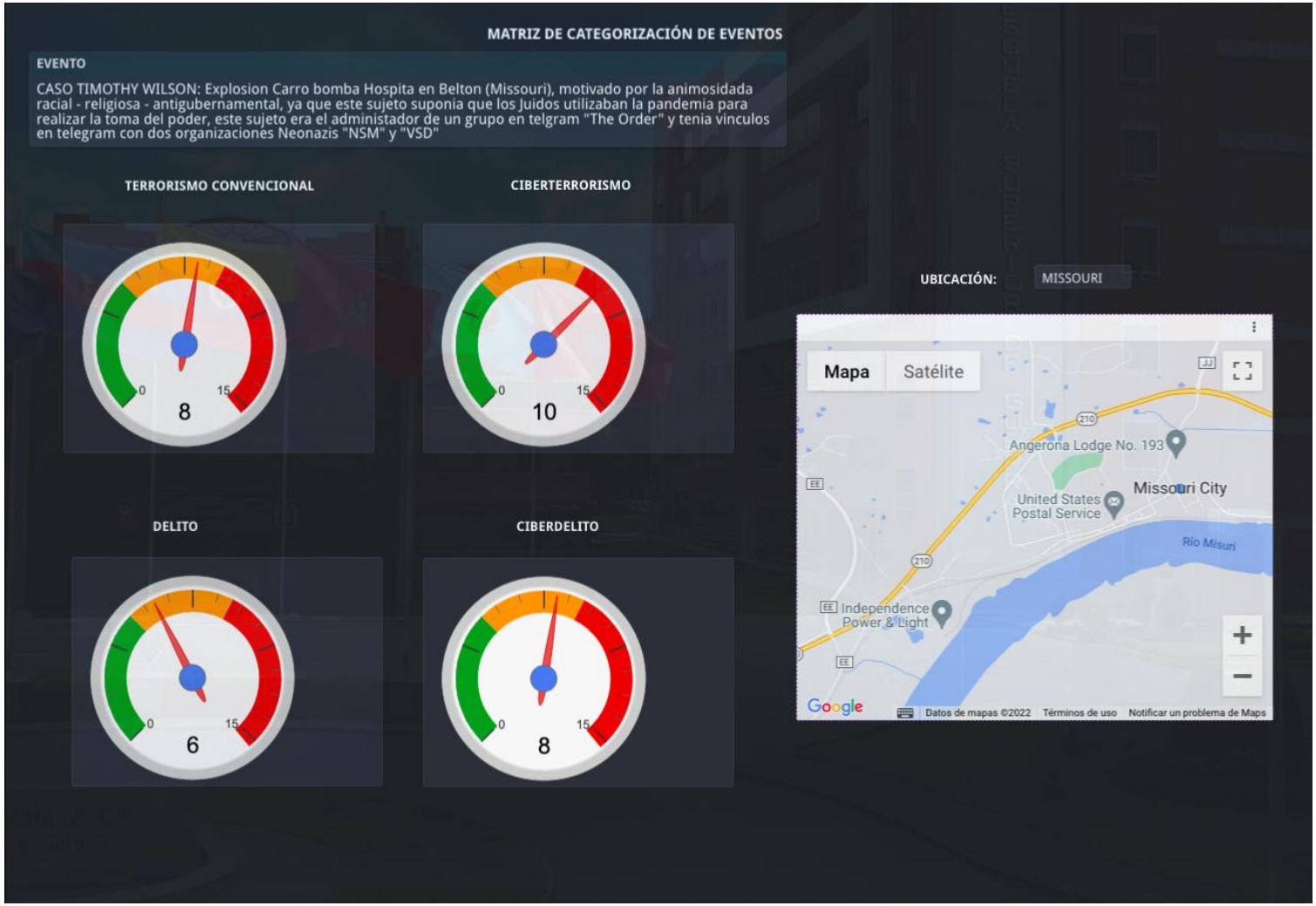
Fuente: Elaboración propia

Dentro de esta matriz podemos observar los diferentes factores que permiten evidenciar o diferenciar la materialización de un evento especifico como el terrorismo convencional, ciberterrorismo, delitos y ciberdelitos; posteriormente podemos evidenciar la columna de valor la cual permite asignar el número uno (1) cuando se logra evidenciar la aplicación de alguno de los factores relacionados o cero (0) cuando no se evidencia la aplicación de los mismos, estos valores nos permite identificar cual es el evento que probablemente se está materializando.

Igualmente es importante resaltar que algunos de los factores desplegados en la matriz de caracterización de eventos pueden afectar de forma simultánea a dos o más eventos como lo podemos observar en la Figura No 2, pero hay algunos factores determinantes que nos permite establecer la caracterización.

Con la finalidad visualizar los resultados obtenidos, se genera una interfaz agradable para que los datos sean fáciles de comprender mediante una mesa de trabajo (Dashboard) online que permite reflejar la descripción, ubicación y resultados de la matriz de caracterización de eventos, felicitando dentro del análisis de los factores la contextualización de los eventos.

Figura No 3 Resultados de la matriz de caracterización de eventos



Fuente: Elaboración propia

Como podemos observar en la figura No 3, se realizó una simulación de ejemplo, con el fin de explicar cómo se visualiza el reporte que genera la mesa de trabajo (DasHboard), donde se logró evidenciar la aplicación de diez (10) factores, los cuales afectan de forma simultánea a los cuatro eventos, pero hay ciertos factores determinantes que nos van a permitir establecer cuál es el evento con mayor afectación.

De acuerdo con lo anterior se puede visualizar los siguientes aspectos; una descripción detallada y la ubicación mediante un mapa; así mismo cada uno de los eventos posee un reloj de medición los cuales nos permitirán realizar un análisis cuantitativo con el fin de determinar la caracterización del evento, en razón a que el evento con mayor afectación nos va a permitir distinguir cual es el evento que probablemente se haya desarrollado; para el ejemplo anterior, el evento con mayor afectación el del ciberterrorismo.

CAPÍTULO IV

Factores que han influido en la evolución del ciberterrorismo: año 2010 al año 2021

Utilización de medios tecnológicos de información

El desarrollo tecnológico constituyó como una de las soluciones con mayor transformación en los últimos años; principalmente en las grandes ciudades del mundo, donde su importancia se halla en la evolución de infraestructuras y de conglomerados sociales, gracias a los avances derivados de la IV Revolución Industrial.

Fenómenos como la globalización e introducción a sistemas electrónicos con inteligencias artificiales, redes de comunicaciones, entre otros adelantos tecnológicos, no solo hicieron visible el potencial de evolución de sistemas económicos integrados con nuevas tecnológicas, si no que, a su vez consolidaron espacios para el desarrollo de grupos criminales que, por medio del ciberterrorismo, ejecutaban acciones cibernéticas para generar caos, produciendo así escenarios contextuales inestables.

Frente a lo anterior, los gobiernos señalaron el fenómeno como un problema de seguridad y defensa nacional, pues facilitó la difusión de información en tiempo real, con menor costo logístico y sin mecanismos para comprar su origen o veracidad. Tal fenomenología convirtió espacios de comunicación como las redes sociales en escenarios de naturaleza hostil, en los cuales hay desagregación mediática de ideas, ideologías y corrientes sociológicas inclinadas al terrorismo.

El ciberterrorismo ha permitido que diversos estudios académicos como los presentados por Hernández, Torrero y Hernández (2014) diversifiquen su impacto negativo entre el actor poblacional, bajo el enfoque de transformación estructural de la conducta social por medio de una integración a una cultura de masas, la cual se define como una transformación a un conjunto de normas, costumbres, pensamiento, formas de comportamiento o el mismo entendimiento o integración de la información que lo rodea. (p. 117) mediante la integración de narrativas ideológicas que transformen las conductas de la población y fomenten rasgos

extremistas o lesivos para determinadas instituciones o grupos sociales. Detonando así actos violentos como los citados por Naciones Unidas a continuación:

> Timothy Wilson, quien, el 24 de marzo de 2020, recibió un disparo de la Oficina Federal de Investigaciones de los Estados Unidos (FBI) en Kansas City cuando planeaba detonar una bomba en un hospital que atendía a pacientes con coronavirus. Wilson participó activamente en al menos dos canales neonazis de Telegram y mantuvo comunicación con un soldado de infantería del ejército que quería planear un ataque a una importante red de noticias estadounidense y discutió sobre apuntar a un candidato presidencial demócrata. El último comentario en línea de Wilson fue un mensaje antisemita sobre el origen de COVID-19. (Naciones Unidas, 2020, p. 12).

Demostrando que, bajo escenarios de incitación al odio, comunicación de información sin controles de veracidad o dispuestas para el convencimiento o reclutamiento de personas a grupos terroristas, la agenda pública nacional presenta una nueva serie de amenazas que atentan contra el desarrollo social, el cumplimiento de la oferta pública nacional y la consolidación de espacios pacíficos y de cumplimiento de derechos fundamentales.

En el caso colombiano podemos evidenciar que los diferentes grupos que intervienen dentro de conflicto interno (Disidencias FARC - ELN) utilizan los mismos mecanismos de difusión, con el fin de generar una desestabilización del gobierno como uno de sus fines políticos, ya que estas herramientas son eficaces en la difusión de información a gran cantidad de audiencia, utilizando identidades virtuales que no les genere ningún vínculo que ponga en riesgo su organización.

Lo anterior, se puede evidenciar en el 2017, cuando las Fuerzas Armadas Revolucionarias de Colombia (FARC) lanzaron una campaña de marketing en medios digitales

para alterar su actividad criminal frente a diversos escenarios y públicos, entre los que se destacan actores internacionales, los cuales engloban un grupo poblacional que al no encontrarse presente en los actos de violencia o no contar con la información correcta para tomar una postura acorde con los crímenes realizados por estos grupos. Como se demostró en artículos informáticos de medios extranjeros como la BBC durante el 2017.

Este tipo de propaganda (ver anexo A), demuestra que los grupos al margen de la ley, por medio de planes estructurados de posicionamiento y marketing, pueden distorsionar la realidad nacional, concentrando la información en una perspectiva incompleta que pueda hacer ver que sus acciones se encuentran justificadas, que requieren del apoyo de diversos actores y que el Estado colombiano es el verdadero enemigo.

Ante esta estrategia, se podría hablar de una evolución de los discursos nacionalistas que concentran su accionar en la lucha frente a un enemigo en común, el cual debe ser derrotado en el menor tiempo posible para preservar "un interés nacional", esta abstracción en los grupos al margen de la ley en el Estado colombiano, se han configurado como una estrategia característica de los escenarios de violencia y terrorismo, en la que se destaca el uso directo de la fuerza para atentar en contra de una población, sus derechos o su territorio, sino que mediante una postura alejada de las armas, con banderas y un ambiente de violencia, adaptan espacios del uso de la fuerza suave, para introducir discursos populistas que escalen en la percepción que se tiene de estos grupos al margen de la ley característico de los últimos años de conflicto.

Este tipo de control social presenta las condiciones ideales para ejecutar acciones terroristas tal y como lo explican Méndez, Gendler y Lago (2015) al debatir que:

> (…) la globalización permite que diversos grupos generen estados de conmoción o terrorismo sin importar su nacionalidad de origen, por medio de las redes sociales, estos presentan la posibilidad de generar intervenciones transnacionales en favor

de grupos o actividades delictivas, las cuales generan una complicación de las condiciones de inseguridad en un territorio determinado (p.14)

Destacando de lo anterior que, los estados de conmoción no se limitan a los ocasionados por acciones violentas, sino que su alcance ha evolucionado a estados de incertidumbre y especulación en donde un grupos de actores y ciudadanos, al verse inmersos por información falsa y perspectivas que omiten información relevante para tomar posturas políticas y sociales acordes a la realidad interna de un territorio, presentan una vulnerabilidad en la seguridad humana, causando que los afectados directos e indirectos se encuentren vulnerados en nuevos ambientes de derechos, como el acceso a la información y uso responsable de las TIC´S, al adaptar el terrorismo a los nuevos desarrollos humanos.

De acuerdo con lo analizado anteriormente, es preciso destacar la vulnerabilidad que presenta la ciudadanía frente a grupos terroristas que transmiten información alterada mediante la utilización de las redes sociales como medio de difusión, las cuales bajo la influencia de estos mensajes puede ser motivada o manipulada para causar actos violentos premeditados en contra de la población civil y organismos de seguridad del Estado, con el fin de obtener un fin político; o patrocinar grupos al margen de ley por medio de recursos, sin saber las implicaciones violentas o los fines de estos recursos en la vulnerabilidad de los afectados directos.

Por tal razón, el desarrollo del conflicto y uso de herramientas de control de la información, estados de especulación o manipulación social, complejizan la determinación de la participación e influencia de Grupos Armados Organizados (GAO) o los Grupos Armados Organizados Residuales (GAO-r), ya que la utilización de herramientas tecnológicas permite generar identidades virtuales falsas, cuyo fin es proteger sus identidades reales, para no exponer a sus organizaciones delictivas y evitar cualquier tipo de vínculos al sistema judicial.

Por último, es preciso establecer que uno de los desafíos para el Estado Colombiano en el desarrollo de la Estrategia de seguridad y defensa nacional, es integrar sistemas de control

de información y conocimientos tecnológicos, que facilite el estudio y anticipación de posibles ataques terroristas que pudieran ser gestionados mediante medios digitales; si bien el Estado Colombiano presenta mecanismos para la atención a delitos cibernéticos, en importante que el Estado Colombiano enfoque su esfuerzos en la ciberseguridad y ciberdefensa, ya que con los avances tecnológicos y la integración de nuevos sistemas de comunicación como también de canales digitales, se puede evidenciar que mencionadas herramientas cada vez están siendo más utilizados por estas organizaciones al margen de la ley que hacen parte del conflicto interno colombiano, como también podemos evidenciar un aumento considerable en el blanco audiencia de estos medios de difusión.

Por tal motivo se requiere de un constante fortalecimiento a los cuerpos de seguridad del Estado no solo para que haga frente a las amenazas actuales, sino que a su vez, permita la prevención de amenazas futuras a la seguridad ciudadana.

CAPÍTULO V

Principales factores que contribuyeron a la evolución del ciber terrorismo: tecnología, conocimiento y globalización

El ciberterrorismo es la representación digital de amenazas que plantean inestabilizar a grandes escalas Estados y organizaciones (Gordon y Ford, 2002); la escalada digital de los mismos, así como la apertura del internet a todos los sectores de la sociedad ha suscitado el nacimiento de grupos revolucionarios cibernéticos, cuya bandera o ideología busca enseñar "verdades" o robar secretos para poder utilizarlos en contra de la gobernabilidad de un Estado o para presionar y coaccionar a empresas a pagar millonarios sobornos para no develar secretos (Weimann, 2004).

Ahora bien, al considerar el ciberterrorismo como una amenaza del mundo moderno, surge una pregunta de investigación, ¿Cuáles son los factores que contribuyen a la evolución de la amenaza cibernética?, de una u otra forma siempre ha existido la gran interrogante que busca justificar como surge este fenómeno y cuál es el alcance o que es lo que buscan los famosos criminales digitales.

El primer factor de análisis es la tecnología; la historia del hombre está rodeada de hechos históricos que han representado un avance significativo en la evolución del mismo, desde la invención de la rueda en la prehistoria, hasta la invención de vehículos eléctricos, el ser humano siempre ha innovado en la búsqueda de optimizar y facilitar los trabajos que desarrolla a diario; en esta incansable sed de crecimiento, surge en el año 1943 el primer ordenador del mundo ENIAC, que suscitaba el primer paso hacia el modernismo en la recolección de datos e información (Molero, 2015).

Los conflictos internacionales, la ambición del ser humano por acortar distancias y por conectar al mundo hizo que para el año de 1957 la URSS lanzara el primer satélite al espacio (SPUTNIK 1) (Lubert, 2017), en consecuencia, la Agencia de Proyectos para la Investigación Avanzada de Estados Unidos por sus siglas en ingles ARPA, inicia con un programa en

conjunto al departamento de defensa americano, que buscan la protección y la interconectividad de los sectores del estado (Abbate, 1994).

Es en 1969, cuando se empieza a conocer las capacidades de la red ARPA para interconectar a un ordenador con una línea telefónica, y pocos años después conectar a cerca de 50 universidades americanas; para el año de 1983 se da un gran salto hacia lo que conocemos como internet al ser conectada a múltiples servidores del gobierno americano (Abbate, 1994). La evolución tecnológica en este aspecto denota como el nacimiento y evolución de los computadores, y la creación y posterior desarrollo del internet como una red global que intercomunica a todas las personas alrededor del mundo, sería el canal sobre el cual los delincuentes cibernéticos encontrarían formas de realizar ataques en el mundo moderno.

Otro factor fundamental ha sido la evolución del conocimiento en el ser humano, a través de los siglos, se han marcado eras en las que mentes brillantes han buscado sobresalir y dejar legados que trasciendan la historia, desde filósofos como Sócrates, Aristóteles y Platón hasta genios físicos y matemáticos como Einstein y Hopkins, todos han marcado un punto de inflexión en la historia que han dejado como parte relevante en la evolución del ser humano (Jammer, 2006), la teorización de varios conceptos que siempre han buscado explicar el origen de las cosas ejemplifican como el conocimiento a través de los siglos ha evolucionado y hoy en día parece ser más fácil de adquirir.

En este punto, se puede observar la primera correlación directa que existe entre tecnología y conocimiento, porque la una depende de la otra de sobremedida, el crecimiento en el conocimiento de las personas suscito que la tecnología mundial creciera y evolucionaria y esta a su vez de forma reciproca devuelve conocimiento al ser humano que esta sediento por saberlo todo, es aquí donde el internet es fundamental porque a través de esta red que conecta al mundo se encuentra acceso a conocimiento como tal vez nunca se había visto anteriormente; sin embargo, aquí es donde también empieza el riesgo, porque el conocimiento puede traer

consecuencias positivas o en muchos otros casos peligrosas para quienes usan la red mundial de internet.

El conocimiento es poder, y esta frase ha quedado grabada en la mente del ser humano a través de los siglos (Popkewitz, 1997), de hecho, una el conocimiento que adquieren los denominados Hackers, es tal que pueden poner en peligro la estabilidad de un estado un claro ejemplo fue Julián Assange quien en el año 2010 filtro material clasificado del ejército norteamericano sobre la realidad de la guerra de Afganistán, esto, suscito una serie de crisis mundial que denoto como una persona con conocimiento y con alcance a internet podría poner en jaque a una potencia mundial como la norteamericana.

El tercer factor que ha influenciado el nacimiento del ciberterrorismo, es la globalización, está a su ve enmarca los dos conceptos anteriormente analizados, en razón a que la misma demuestra cómo el mundo se ha conectado a través de la búsqueda de conocimientos y de la industrialización con tecnologías modernas que faciliten la vida del hombre (Pascual, 2006). Sin embargo, la globalización también implica que las economías del mundo estén interconectadas y que por ende existan mayores relaciones entre la población mundial.

Ahora bien, la incidencia que tienen estos tres conceptos en auge del ciberterrorismo es notoria, el nacimiento de las tecnologías específicamente el computador y el uso del internet ha crecido desaforadamente, de igual manera las universidades han fortalecido los denominados “tanques de pensamiento”, en donde grupos de investigadores científicos trabajan a diario por ampliar los conocimientos y mejorar la calidad de vida de las personas, y finalmente el intercambio de conocimientos, productos, bienes y servicios es una realidad latente en un mundo globalizado que a través de la industria y la tecnología ha logrado disminuir las brechas y conectar a los más de 7.7 billones de personas que habitan al planeta tierra.

El ciberterrorismo surge entonces como una forma de obtener poder, a través de métodos convencionales como es la obtención de información (conocimiento) a través de internet (tecnología) que busque afectar a una economía (globalización); en otras palabras, el crecimiento de estas tres aristas anteriormente explicadas permite la evolución de un nuevo concepto que logra la inestabilidad de los estados y que amenaza a las económicas de los países más poderosos del mundo (Gamón, 2018).

En conclusión, el auge del ciberterrorismo tiene un origen convencional a través de la evolución del conocimiento, la tecnología y la globalización del mundo moderno, este nace también como una forma de protesta y en muchos otros casos con fines económicos personales, sin embargo el ciberterrorismo no tiene blancos determinados, porque puede afectar a cualquiera, los riesgos a los que se enfrenta un mundo globalizado con una amenaza de este tipo, es el poder que puede ejercer sobre las personas, que eventualmente pide traducirse en violencia y muertes, en otras palabras el ciberterrorismo puede terminar desencadenando una catástrofe mundial si no es controlado efectivamente por la sociedad.

CAPÍTULO VI
Triangulación de resultados

Hasta esta parte de la investigación se llevó a cabo un análisis conceptual y exploratorio de los planteamientos correlacionados con el proceso evolutivo del ciber terrorismo ente 2010 y 2021. Diferentes factores salieron a colación. Entre ellos, las categorías de estudio: tecnología, conocimiento y globalización.

Desde el parámetro de lo tecnológico, hay una concepción clásica que describe el fenómeno como el resultado de un amplio y rápido proceso evolutivo en materia tecnológica. Acá, es necesario aceptar que la tecnología, de facto, se convirtió en un obstáculo para los organismos de seguridad y defensa, no porque estos últimos estuvieran fuera de su alcance, sino porque su domino demandó un nuevo tipo y/o nivel cognoscitivo de la guerra (Halder, 2011).

La tecnología como dinamizante para la co-creación de estrategias de ciber defensa o ciber protección es a su vez un factor generador de desventajas. Mírese la siguiente afirmación para continuar con esta explicación: “hoy, las nuevas tecnologías, usadas militarmente, pueden ayudar a que se lleven a cabo acciones terroristas de consecuencias inimaginables. De hecho, ya no se trata de una amenaza, sino de una realidad incipiente que no puede más que agravarse en el futuro” (Medero, 2008)

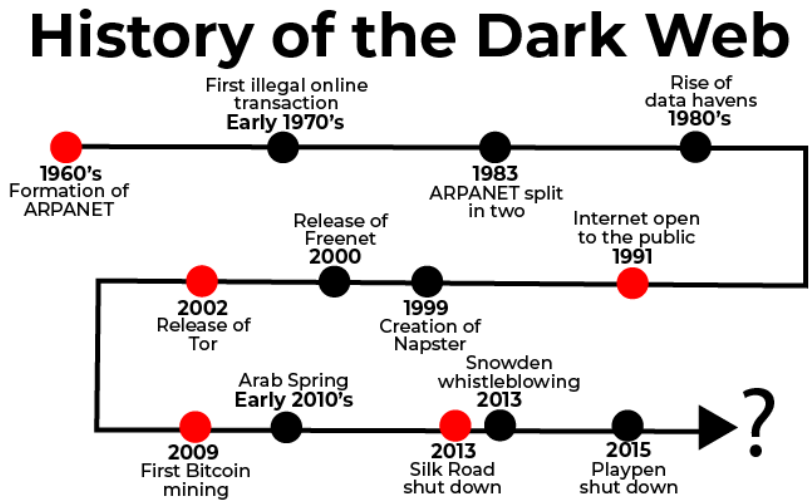
El terrorismo cibernético evoluciona a la par de factores contextuales interrelacionados con el desarrollo humano. Ese es un hecho que quedó claro con la distinción de los tres factores conexos al proceso de evolución: tecnología, conocimiento e hiper conectividad.

Al hablar de evolución también hay que hablar de métodos y medios, y es allí, en esa discusión, en donde el ciberterrorismo cobra relevancia, pues un eje transversal para los tres factores es el dominio conceptual y experimental aplicativo de los parámetros funcionales.

Esto quiere decir, que si bien la globalización productora de hiper conectividad y la tecnología son talantes base para concertar posibles hechos ciber-terroristas, el conocimiento como vector cognoscitivo es fundamental a la hora de entrelazar el objetivo delictivo con los sistemas de información (Mazari et al, 2018).

Un ejemplo básico pero adecuado para comprender la importancia del conocimiento en el proceso evolutivo del ciber terrorismo es la implementación de la "Deep web" (de ahora en adelante DW). Según Vilić (2017), la evolución de este espacio en el que no hay track o huellas digitales, y en donde se efectúan transacciones y operacionales ilegales, se da a partir de arduos procesos de investigación y experimentación que interconectaron tanto un sistema de información en funcionamiento como un planteamiento cognoscitivo, quizá experimental, pero avanzado para la época. La figura nº 2 presenta una línea temporal de evolución para la DW:

Figura 4 Línea de tiempo Deep Web



Fuente: información recuperada de Kastner (2020)

El conocimiento para el desarrollo de software interconectados a la DW es fundamental; previo a la arquitectura tecnológica y costos de inversión, el dominio epistemológico en campos como la programación y creación de códigos y algoritmos toma un papel primario. Por ejemplo, el navegador TOR, también llamado "The Onion Route" permite la navegación de los

usuarios en espacios digitales sobrepuestos en internet, hecho tal que omite un factor primario: la dirección IP[1].

Los alcances en este tipo de tecnología, que primero requieren conocimiento experimental para su creación y luego conocimiento para su manejo, generaron un escenario amplio, cuyo margen de acción permite a diferentes usuarios interactuar sin restricción o marco regulatorio alguno. Esto, a su vez provocó la aparición de fenomenologías delictivas complejas, poco conocidas, eventualmente aventajadas por la clandestinidad que ofrece este tipo de sistemas.

El conocimiento se convierte entonces en el principal factor evolutivo del terrorismo cibernético. El segundo factor es la tecnología. Para analizar esta postura hay que observar la siguiente afirmación:

> Cuando hablamos de ciberterrorismo lo hacemos en sentido amplio y hablamos tanto de las acciones terroristas perpetradas a través de Internet como de todas aquellas gestiones o actuaciones que realizadas en este medio sirven de puente para poder llegar a realizar acciones terroristas de todo tipo de índole. El terrorismo en la actualidad no se puede entender sin el uso de las tecnologías cibernéticas es decir el ciberterrorismo es una problemática que afecta a la seguridad mundial. Las Naciones han desarrollado estrategias jurídicas para castigar y prevenir este tipo de delitos, que ponen en entre dicho la seguridad nacional (Gamon, 2018, p. 12).

Lo tecnológico y cognoscitivo van de la mano. Esta es una ecuación que se evidenció con el trabajo de investigación. Ahora, una de las problemáticas de contexto que de facto aventaja al ciber terrorismo no corresponde al tecnológico como tal, sino a las brechas tecnológicas que hay entre los Estados.

[1] La dirección IP es la etiqueta que explora y reconoce la interfaz.

Esas brechas dinamizan al ciberterrorismo, pues producen gaps cognoscitivos, los cuales afectan el proceso proteccionista que presentan los organismos de seguridad y defensa nacional cibernéticos. En tal medida, la tecnología como factor dinamizante si es el segundo componente, pero lo que realmente beneficia a los actores terroristas cibernéticos es la brecha cognoscitiva entre los ciber atacantes y los organismos encargados de que crear sistemas defensivos. La figura que se presenta a continuación permite entrever los componentes que conforman esa brecha tecnológica:

Figura 5 Brecha tecnológica

Fuente: información recuperada de Aponte (2016)

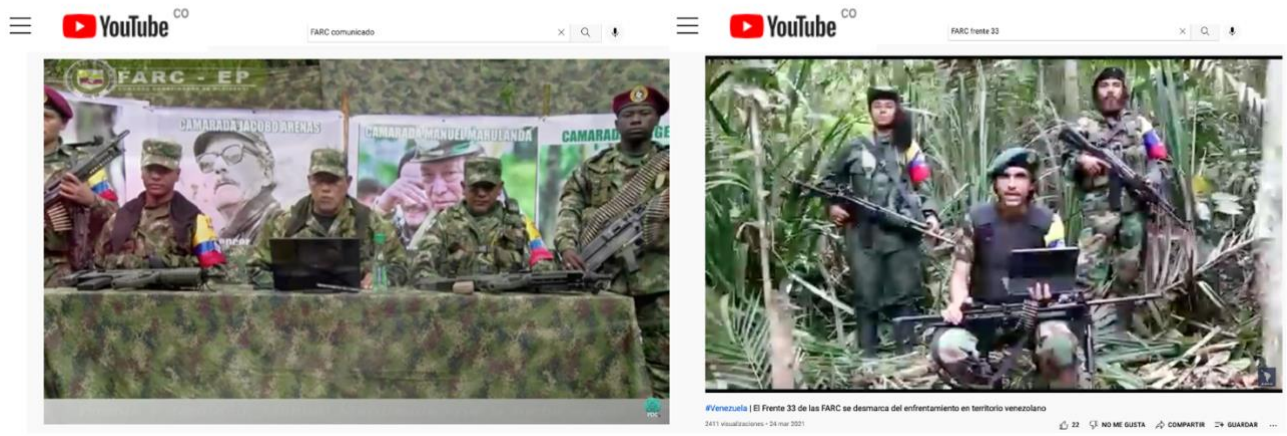
El tercer elemento fundamental, es la globalización conexa a la hiper conectividad. En tal sentido, es necesario explicar que la producción de conocimiento en materia ciber junto con el desarrollo tecnológico, formó un núcleo expansivo en el que las comunidades internacionales quedaron hiper conectadas.

Eso quiere decir que la información fluye más rápido, y por ende los códigos compuestos, base fundamental de un ciber ataque. Pero, la hiper conectividad deja otras lecciones; estas tienen que exponerse desde el campo del ciber terrorismo. Comprender esas lecciones implica ampliar el margen epistémico del concepto ciber terrorismo, específicamente

porque no todas las acciones tienen o presentan relación con lenguajes de programación complejos o utilización de tecnologías disruptivas como la Deep Web o navegadores que ocultan las IP de la interfaz.

Una muestra en ese tipo de terrorismo es la utilización de medios tecnológicos para la difusión de miedo y coerción. Las insurgencias colombianas, así como otros grupos terroristas de la talla del Estado Islámico, son expertas en esa materia (Ver figura 4).

Figura 6 Formas de terrorismo cibernético



Fuente: elaboración propia con información recuperada de You Tube (2022)

La difusión de miedo y coerción es considerada parte del vector "terrorismo convencional" (Sánchez, 2016). Su dispersión, a través de factores tecnológicos, entra a hacer parte de una distinción categórica poco explorada en el proceso evolutivo del terrorismo cibernético. Por esa razón, entre los elementos que coadyuvaron a su evolución entre 2001 y 2021 hay que agregar no solo la hiper conectividad, sino también las formas de uso que emergieron al mismo tiempo que lo hicieron métodos y medios asociados a un nuevo dominio cognoscitivo de la guerra: el ciber escenario.

Recomendaciones

Una vez finalizado el ejercicio de investigación y triangulación, se pasa a la proposición de tres recomendaciones, cada una de ellas conexas al factor de "sugerencia" para la estructuración de futuras investigaciones basadas a las categorías: terrorismo cibernético, utilización de medios digitales y empleo de redes terroristas cibernéticas.

Las recomendaciones son las siguientes:

Primero, es necesario reconfigurar el CONPES 3975 de 2019, incluyendo en el objetivo estratégico "capacitación en temas asociados al precepto Inteligencia Artificial", tres factores de atención: intervención de redes sociales y otros medios tecnológicos que faciliten y/o permitan difusión de mensajes, actuaciones u otro tipo de configuraciones con fines difusivos asociados a grupos terroristas; también hay que incluir la implementación de políticas de prevención y predicción de mensajes terroristas con capacidad híper mediática y, finalmente, la formulación de procesos de gestión para materializar el dominio cognitivo en temas ciber.

Segundo, es fundamental potencializar capacidades estratégicas conexas a la Estrategia Intersectorial compuesta por el Comando Cibernético de las FF.MM., Comando Cibernético de la Policía y ColCert[2]. Esa potencialización, que de hecho se propuso en el CONPES 3974 de 2016, debe darse en dos aristas principales: completitud del programa Task Hacker y dinamización de procesos formativos para el capital humano que hace parte de la estrategia inter-sectorial-

Tercero, es imperativo diseñar una estrategia para proteger y resguardar el proceso transformacional que planteó el CONPES 3975. Esa estrategia tiene que basarse a su vez en cuatro elementos clave: cubrimiento totalizado del sistema de ciber defensa sobre empresas y/o compañías que tienen acceso a mega y macro-datos de naturaleza pública; tecnificación

[2] Grupos de respuesta a emergencia cibernéticas de Colombia.

constante de los sistemas de ciber protección y enajenación financiera pública para dar autonomía de inversión al sistema de ciber defensa colombiano.

Conclusiones

El terrorismo cibernético posee aristas diferentes. Su estudio como se pudo observar tiene que abarcar múltiples campos de acción, entre los que está la identificación de actores terroristas cibernéticos los cuales gozan de clandestinidad. Ahora, si se mira el planteamiento con esa necesidad evolutiva, diferentes formas de estudio saldrían a colación.

Para el caso, este ciclo exploratorio comenzó con el análisis teórico del concepto terrorismo. De allí dos deducciones salieron a la luz. Primero, el concepto cambia a la par de factores contextuales como tecnología, hechos e impactos. Segundo, la definición transmuta porque al planteamiento van ingresando nuevos elementos como actores, subsistemas de información e invenciones que facilitan la rápida difusión de información y acciones cibernéticas con genealogías delictivas.

Definido el concepto, se pasó a la fase de los componentes contextuales que influyeron en el proceso evolutivo del ciber terrorismo desde el año 2001 a 2021. Allí se pudo subrayar que el desarrollo tecnológico constituyó uno de los dinamizantes claves para la expansión del terrorismo a través de medios digitales. Sin embargo, y contrario a lo que se cree, el ciber terrorismo y su transmutación – constante- no dependería únicamente del avance *tech*, pues otros dos componentes dinamizarían su alcance: la globalización conexa a la hiper conectividad y el conocimiento.

Fenómenos como la globalización e introducción a sistemas electrónicos con inteligencias artificiales, redes de comunicaciones, entre otros adelantos tecnológicos, no solo hicieron visible el potencial evolutivo de sistemas económicos integrados con nuevas tendencias tecnológicas, sino que, a su vez, consolidaron espacios para el desarrollo de grupos criminales que, por medio del ciberterrorismo, ejecutaron acciones generadoras de caos, produciendo así escenarios contextuales inestables. Como ejemplos se expusieron las insurgencias colombianas, las cuales han desarrollado acciones ciber terroristas, pero a partir

de métodos y medios contrarios a un lenguaje de programación complejo o utilización de subsistemas ciber terroristas clandestinos.

El tercer componente es transversal a la globalización y tecnología: el conocimiento. El dominio cognoscitivo de la ciber guerra y de sus elementos praxeológicos es fundamental para consolidar nuevos espacios de interacción delictiva no considerados con anterioridad. El conocimiento o su ausencia ha abierto brechas estratégicas que ponen en ventaja al actor que domina el campo ciber, pero que también genera desventajas estratégicas y geoestratégicas para el que posee conocimiento insuficiente.

Siendo así y dando respuesta a la pregunta de investigación, se puede afirmar que los elementos que impulsaron la evolución del ciber terrorismo entre 2001 y 2011 son: la tecnología, la globalización e hiper conectividad y el conocimiento experimental en materia ciber.

Referencias

1. Alban, G. P. G., Arguello, A. E. V., & Molina, N. E. C. (2020). Metodologías de investigación educativa (descriptivas, experimentales, participativas, y de investigación-acción). *Recimundo*, *4*(3), 163-173.
2. Amado, I. G. (2007). Ciberterrorismo-Una Aproximación a Su Tipificación como Conducta Delictiva. *Derecho Penal y Criminología*, *28*, 13.
3. Barredo, M. Á. (2016). Redes sociales y ciberterrorismo. Las TIC como herramienta terrorista. *Dialnet*.
4. Carlini, A. (2016). Ciberseguridad: un nuevo desafío para la comunidad internacional. . *Boletín IEEE*, 950-966.
5. Cespedosa Rodríguez, C. (2019). Yihadismo, internet y ciberterrorismo.
6. Cespedosa, C. (05 de 2019). Yihadismo, internet y ciberterrorismo. *Comillas*, 45-54.
7. Conti, M., Dargahi, T., & Dehghantanha, A. (2018). Cyber threat intelligence: challenges and opportunities. In *Cyber Threat Intelligence* (pp. 1-6). Springer, Cham.
8. Echeverria, R. (12 de enero de 2017). El terrorismo cibernético como acto que criminaliza la libertad de expresión: una mirada desde la geo informática. *Trabajao de investigación.* Medellín, Colombia: Repositorio Universidad CES: https://repository.ces.edu.co/bitstream/handle/10946/3008/Terrorismo%20Ciberbético.pdf?sequence=1.
9. Fernández, N. (2018). La letalidad del Ciberterrorismo. *Revista general de la Marina*, 134.
10. Gamon, V. P. (2017). Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad. *Revista Latinoamericana de Estudios de Seguridad*.
11. González-García, F. J. (20 de 07 de 2020). Capacidades prospectivas y de defensa en la lucha contra el Ciberterrorismo. *Relaciones Internacionales*, *29*(58).

12. Griset, P., Mahan, S., & Griset, P. L. (2003). *Terrorism in perspective.* California: Sage Publications.
13. Jesús, C. E. (2009). La innovación yihadista: propaganda, ciberterrorismo, armas y tácticas. *Grupo de Estudios Estratégicos y Análisis*, *7416*, 1-8.
14. Juan E. Rubio, C. A. (11 de 2019). Current Cyber-Defense Trends in Industrial Control Systems. *Computers & Security Journal, 87*, 3.
15. Manrique, J. (2021). TERRORISMO CIBERNÉTICO: PERSPECTIVAS DESDE LOS DERECHOS FUNDAMENTALES. . *Revista Argumentum-Argumentum Journal of Law*, 819-848.
16. Mauro Conti, A. D. (2018). Cyberthreat Intelligence: Challenges and Opportunities. *Cyberthreat Intelligence*, 1-5.
17. Medero, G. S. (2015). El ciberterrorismo: de la web 2.0 al internet profundo. *Abaco, 3*(85).
18. Nnam, M. U., Ajah, B. O., Arua, C. C., Okechukwu, G. P., & Okorie, C. O. (2019). The war must be sustained: An integrated theoretical perspective of the Cyberspace-Boko Haram Terrorism Nexus in Nigeria. *International Journal of Cyber Criminology, 13*(2), 379-395.
19. Nye, J. (2013). From bombs to bytes: Can our nuclear history inform our cyber future? *Bulletin of the Atomic Scientists*, 8-14.
20. Poveda Criado, M. Á., & Torrente Barredo, B. (2016). Redes sociales y ciberterrorismo: Las TIC como herramienta terrorista.
21. Reyes, A. (2014). Alcances del "ciber-terrorismo" en la sociedad contemporánea. Santiago, Chile. Recuperado el 02 de 2022, de https://repositorio.uchile.cl/: https://repositorio.uchile.cl/handle/2250/116821

22. Rubio, J. E., Alcaraz, C., Roman, R., & Lopez, J. (2019). Current cyber-defense trends in industrial control systems. *Computers & Security, 87*, 101561.
23. Taylor, R., Fritsch, E., Liederbach, J., Saylor, M., & Tafoya, G. (2019). *Delito cibernético y terrorismo cibernético.* Estados Unidos.
24. Weimann, G. (2010). Terror on facebook, twitter, and youtube. *The Brown Journal of World Affairs*, *16*(2), 45-54.
25. UNODC. (2013). *El uso de internet con fines terroristas.* Nueva York: Publicación de las Naciones Unidas.
26. Enghelberg, H. (2003). *CYBER TERRORISM | The Evolution of CYBER TERRORISM AS A PRECISION-DELIVERY WEAPON AND THE NEW FRONTIER IN 21st.* Telaviv: ENGPUBLISHING.
27. Organización de Estados Americanos. (2003). *Declaración de Bridgetown - enfoque de seguridad multidimensional hemisférica.* Barbados: Publicaciones OEA.
28. Agejas, J. (2004). T errorismo e información Análisis de la emisión de los vídeos de Al-Qaeda. *Capítulo de libro*. Repositorio de la universiad de Universidad Francisco de Vitoria .
29. Izaguirre, J. (2018). Análisis de los ciberataques realizados en América Latina. *Revista de la Universidad Internacional del Ecuador* , 172-181.
30. Cano, J. (2018). Cibercrimen y Ciberterrorismo: Dos Amenazas Emergentes. *Journal Online*, 1-6.
31. Estarellas, J. (2011). Los medios de comunicación de Al-Qaeda y su evolución estratégica. . *Pre-bie- IEEE (Instituto Español de Estudios Estratégicos)*, 1-12.
32. CICR. (2004). ¿Qué Es El Derecho Internacional Humanitario? De Https://Www.Icrc.Org/Es/Doc/Assets/Files/Other/Dih.Es.Pdf

33. Escobar, A. E. (17 De 05 De 2022). Concepto De Terrorismo Y Su Efecto Social. Https://Repository.Urosario.Edu.Co/Bitstream/Handle/10336/4834/1020714761-2013.Pdf?Sequence=3#:~:Text=El%20gobierno%20colombiano.-,El%20concepto%20de%20terrorismo,Terror%20(Lamarca%2c%201985).
34. Morales, T. G. (2012). El Terrorismo Y Nuevas Formas De Terrorismo.
35. OHCHR. (S.F.). Los Derechos Humanos, El Terrorismo Y La Lucha El Terrorismo y La Lucha. Https://Www.Ohchr.Org/Sites/Default/Files/Documents/Publications/Factsheet32sp.Pdf
36. República De Colombia. (1980). Decreto 100 De 1980. R Https://Www.Suin-Juriscol.Gov.Co/Viewdocument.Asp?Id=1705120
37. Zalaquett, J. (S.F.). Conceptualización Del Terrorismo: Un Punto De Vista Normativo. Https://Www.Corteidh.Or.Cr/Tablas/R06856-3.Pdf
38. Hernandez, L. M., Torrero, P. E., & Hernandez, V. C. (2014). Virtualidad, ciberespacio y comunidades virtuales.
39. http://www.upd.edu.mx/PDF/Libros/Ciberespacio.pdf
40. Méndez, A., Gendler, M., & Lago, S. (2015). Movimientos sociales y tecnologías digitales: comunicación y prácticas de resistencia en el mundo global.
41. 2022, de https://www.aacademica.org/anahi.mendez/16.pdf
42. Naciones Unidas. (19 de noviembre de 2020). Las redes sociales, la principal arma terrorista durante la pandemia de COVID-19. https://news.un.org/es/story/2020/11/1484342
43. BBC NEWS. (24 de abril de 2017). Así son los anuncios publicitarios con los que las FARC buscan ampliar su público en Colombia y que algunos rechazan. https://www.bbc.com/mundo/noticias-america-latina-39688741

44. Gordon, S., & Ford, R. (2002). Cyberterrorism?. *Computers & Security, , 21*(7), 636-647.
45. Weimann, G. (2004). Cyberterrorism: How real is the threat? . *United States Institute of Peace.*, (Vol. 119).
46. Molero Prieto, X. (2015). De Ada Byron a Grace Hopper y las programadoras del ENIAC: los bits, en femenino. *novática, 231* , 20-25.
47. Lubert, C. P. (December de 2017). Sixty years of launch vehicle acoustics. . *In Proceedings of Meetings on Acoustics 174ASA , Vol. 31*, No. 1, p. 040004.
48. Abbate, J. E. (1994). From ARPANET to INTERNET: A history of ARPA-sponsored computer networks, 1966-1988. . *University of Pennsylvania.*
49. Jammer, M. (2006). Concepts of simultaneity: From antiquity to Einstein and beyond. . *JHU Press.*
50. Popkewitz, T. S. (1997). Foucault's challenge: Discourse, knowledge, and power in education. . *Teachers College Press.*
51. Pascual, D. S. (2006). Ciberterrorismo en el contexto de la globalización. In Defensa e Internet [Archivo de ordenador]: actas del I Congreso sobre Seguridad, Defensa e Internet: Santiago de Compostela, marzo de 2004. *Servicio de Publicaciones= Servizo de Publicacións.*, pp. 319-351.
52. Halder, D. (2011). Information Technology Act and cyber terrorism: A critical review. *Available at SSRN 1964261*.
53. Medero, G. S. (2008). Ciberterrorismo. La guerra del siglo XXI. *El Viejo Topo*, (242), 14-23.

Lista de Figuras

Lista de Anexos

- **Anexo A:**
    - https://www.ieee.es/Galerias/fichero/docs_opinion/2011/DIEEEO16_2011MediosComunicacionAl-Qaeda.pdf,
    - https://www.bbc.com/mundo/noticias-america-latina-39688741
    - https://www.youtube.com/watch?v=kteCjKQqHlw
    - https://www.youtube.com/watch?v=YyQPiWZRKHY.