

Carlos Ramírez Castañeda

Perspectiva Investigativa del Ciberterrorismo desde el Análisis de Contexto

Investigative Perspective on Cyberterrorism from a Contextual Analysis

Resumen

El ciberterrorismo es un fenómeno que debe ser abordado desde diferentes aristas. Aunque se gestó en el entorno digital, no quiere decir que su alcance e impacto se restrinja únicamente a este contexto, pues las repercusiones son directas y palpables en el mundo material. Analizaremos al ciberterrorismo con una óptica de impacto en la perfilación y contextualización de todo lo que engloba al ciberterrorista, algunos de los modus operandi y casos históricos de impacto, así como las visiones y matices que deja en cada acción. El poder contar con un panorama más amplio y enfatizar la evolución constante de este fenómeno, así como la importancia de un enfoque multidisciplinario basado en ciberseguridad, dándole la debida relevancia a la cooperación internacional en materia legislativa y educación digital para mitigar sus efectos y fortalecer la resiliencia humana y digital ante las diversas amenazas emergentes, las cuales avanzan a pasos agigantados, permitirá analizar el contexto y adaptación de los ciberterroristas, sin perder así el acervo histórico que merece un punto de comparación para lograr una mejor y mayor comprensión.

Palabras clave: Ciberterrorismo, Perfilación, Análisis, Contexto, México

Abstract

Cyberterrorism is a phenomenon that must be addressed from different angles. Although it originates in the digital environment, this does not mean that its scope and impact are restricted solely to this context, as the repercussions are direct and palpable in the physical world. We will analyze cyberterrorism from an impact perspective, profiling and contextualizing everything that cyberterrorists encompass, some of their modus operandi and historical cases of impact, as well as the visions and nuances left in each action. Having a broader overview and emphasizing the constant evolution of this phenomenon, as well as the importance of a multidisciplinary approach based on cybersecurity, giving due importance to international cooperation in legislation and digital education to mitigate its effects and strengthen human and digital resilience in the face of various emerging threats, which are advancing by leaps and bounds, therefore, the analysis of the context and adaptation of cyberterrorists is essential, without losing the historical heritage that deserves a point of comparison to achieve a better and greater understanding.

Keywords: Cyberterrorism, Profiling, Analysis, Context, Mexico

Carlos Ramírez Castañeda, Docente e Investigador Fiscalía General del Estado de Michoacán.

Para citar este artículo: Ramírez, C. (2025), Perspectiva investigativa del ciberterrorismo desde el análisis de contexto, Revista Internacional de Estudios sobre Terrorismo, n°15, pp.31-44.

Recibido

11/07/2025

Aceptado

03/09/2025

1. Introducción

Basta con recurrir a internet para poder encontrar un universo de información en el que a veces resulta complicado diferenciar entre contenidos legítimos y cosas que parecieran sacadas de una novela de ciencia ficción. Internet llegó disruptivamente como una tecnología que logró el posicionamiento como una herramienta de comunicación inmediata y expedita, reinando a lo largo y ancho del mundo, permitiendo el contacto entre personas sin importar fronteras o barreras geográficas, ideologías, géneros, pensamientos. Hoy en día, Internet es el punto clave del funcionamiento en distintas escalas sociales.

De la premisa anterior podemos partir hacia diversos análisis de las conductas cibercriminales, desde perspectivas jurídicas y técnico-informáticas, las cuales son abordadas de manera abundante. Sin embargo, se olvida una bifurcación que ramifica en las perspectivas sociales y psico-criminológicas sobre la temática que relaciona este cuadrante de características relacionadas al ciberterrorismo.

En este artículo analizaremos lo que podría ser el trasfondo o contexto en el ciberterrorismo, a partir de una perfilación criminológica, así como su comparación con otras ramas relacionadas a la ciberseguridad y la cibercriminalidad.

Entre las múltiples ventajas del uso de internet se encuentran desde los avances científicos hasta el aprovechamiento que logran tener los grupos terroristas alrededor del mundo para lograr un posicionamiento en su causa. En este sentido, las necesidades que enfrentan los cuerpos de seguridad, ciudadanía, empresas y usuarios en general requieren un abordaje de análisis sobre el contexto para lograr una mejor y mayor comprensión en pro de la prevención.

Cabe resaltar que el terrorismo en sus distintas modalidades, está presente en todos los países, en algunos casos más marcado y visible que en otros y para ello basta con hacer una catarsis de los hechos históricos en regiones de todo el mundo, que son claro ejemplo de cómo la tecnología e internet se convierten en los principales puntos de convergencia para el control social. De aquí es donde requerimos vislumbrar las contemplaciones de contexto relacionadas directamente al ciberterrorismo y así dejar un precedente.

2. Comprendiendo el ciberterrorismo

El ciberterrorismo corresponde a un complejo que implica el uso de tecnologías de la información y la comunicación (TIC) para llevar a cabo ataques bajo una premisa tecnológica, destinados a causar, infundir miedo, pánico y daños derivados a nivel mundial, pues internet no conoce fronteras. Sin embargo, muchas veces se logra dentro de una demarcación o región geográfica matizada por situaciones políticas, sociales imperantes. Los contrastes en el ciberterrorismo son notables en términos de motivaciones, ideología, métodos, impacto y consecuencias directas, así como colaterales. A continuación, mencionaremos algunos casos históricos y ejemplos más recientes

para ilustrar estos contrastes:

- Ataques de Estonia en 2007: Una serie de ciberataques paralizaron los servicios gubernamentales, financieros y mediáticos de Estonia. Estos ataques fueron atribuidos a Rusia y se cree que estaban relacionados con una disputa política sobre un monumento en Tallin. Los ataques destacaron la vulnerabilidad de las infraestructuras digitales del país y la forma en la que los conflictos geopolíticos podían escalar también en el ámbito digital.
- Operación Aurora en 2009: Este ataque cibernético fue atribuido a China y tenía como objetivo a numerosas compañías tecnológicas y empresas de defensa a nivel seguridad nacional. Se cree que el propósito detrás de este ataque fue el ciberespionaje, robo de propiedad intelectual y con ello revelación de secretos comerciales, lo que puso en relieve cómo los estados podían utilizar el ciberterrorismo con fines económicos, estratégicos y de posicionamiento.
- Stuxnet en 2010: El malware Stuxnet fue descubierto en 2010 y se cree que fue desarrollado por gobiernos de países en Occidente para sabotear una central nuclear iraní. Este caso puso de manifiesto cómo los estados podían utilizar el ciberterrorismo como una herramienta para frenar el desarrollo de armas nucleares de otros países, abriendo un debate sobre las implicaciones éticas y jurídicas sobre el uso de herramientas digitales (Buxton, 2022).
- Ataques a la red eléctrica en Ucrania: En 2015 y 2016, Ucrania sufrió una serie de ataques cibernéticos que dejaron a regiones enteras sin energía eléctrica durante horas¹. Estos ataques se consideraron un claro ejemplo de cómo el ciberterrorismo podía tener un impacto directo en la infraestructura crítica de un país, causando interrupciones masivas en los servicios públicos (CCDCOE, s.f.).

Por otro lado, de forma más reciente podemos listar algunos de los ataques en los que el uso de herramientas digitales se matiza a través del terror y control social:

- Uso de ransomware²: En la última década, los ataques de ransomware han aumentado significativamente. Grupos criminales utilizan malware³ para cifrar los sistemas de sus víctimas y exigen un rescate a cambio de la clave de descifrado. Ejemplos notables incluyen el ataque a la empresa Colonial Pipeline en Estados Unidos en 2021, que afectó al suministro de combustible en varias regiones del país. Estos ataques resaltan cómo los actores no estatales pueden causar estragos a gran escala con motivaciones principalmente financieras (Easterly, 2023).

1 Este acontecimiento también se conoció como “Blackout”.

2 “El ransomware es un tipo de malware que retiene los datos o el dispositivo confidenciales de una víctima, amenazando con mantenerlos bloqueados, o peor, a menos que la víctima pague un rescate al atacante” (Kosinski, s. f., párr. 1).

3 “Malware es un término que abarca cualquier tipo de software malicioso diseñado para dañar o explotar cualquier dispositivo, servicio o red programable. Los delincuentes cibernéticos generalmente lo usan para extraer datos que pueden utilizar como chantaje hacia las víctimas para obtener ganancias financieras. Dichos datos pueden variar desde datos financieros, hasta registros de atención médica, correos electrónicos personales y contraseñas. La variedad de información que puede verse comprometida se ha vuelto ilimitada” (McAfee, s. f., párr. 1).

- Operaciones entre naciones y desinformación: Algunos países se involucran en operaciones cibernéticas para influir en la opinión pública y desestabilizar a otros gobiernos. El caso de la presunta interferencia rusa en las elecciones presidenciales de Estados Unidos en 2016 y 2020 es un ejemplo destacado de cómo el ciberterrorismo puede ser utilizado para minar la confianza en los sistemas democráticos y socavar la estabilidad política.
- Amenazas persistentes avanzadas (APT) chinas: China ha sido acusada de llevar a cabo ciberataques sostenidos y altamente sofisticados contra objetivos gubernamentales, militares y corporativos en todo el mundo. Estos ataques suelen estar dirigidos a la obtención de información estratégica y tecnológica para el beneficio del estado. Ejemplos incluyen el robo de información relacionada con el desarrollo de cazas furtivos y tecnología militar avanzada (America's Cyber Defense Agency, s.f.)
- Amenazas emergentes de IA: A medida que la inteligencia artificial avanza, surgen preocupaciones sobre cómo podría ser utilizada en ciberataques. Desde el desarrollo de malware más inteligente hasta la automatización de ataques dirigidos, la integración de la IA en el ciberterrorismo podría aumentar significativamente el alcance y la eficacia de los ataques.

La mancuerna tecnológica que tenemos que comprender en un primer momento es la que se logra entre la tecnología y los factores de impacto psicosocial, al momento de llevar a la realidad posterior del plano digital a todas esas afectaciones palpables que dejan huella.

La evolución tecnológica no es un hecho aislado, es un punto aprovechado por el terrorismo para magnificar sus impactos y simplificar sus esfuerzos.

3. Factor humano

Dentro del ciberterrorismo debemos reconocer que no todo es puramente digital al involucrar herramientas desarrolladas para lograr una finalidad, ya que detrás de ello hay un humano o grupo de humanos que se encargan del manejo de la tecnología. Algunos ejemplos de este tipo de acciones son los siguientes:

- Activismo y hacktivismo: Grupos hacktivistas, como Anonymous o Guacamaya, han llevado a cabo ataques cibernéticos para promover causas sociales y políticas. Estos grupos a menudo atacan sitios web y plataformas en línea para difundir mensajes y exponer información sensible. Si bien sus motivaciones pueden estar impulsadas por ideales, sus métodos pueden causar daños colaterales y generar debates sobre los límites de la protesta digital.
- Grupos extremistas: Algunos grupos terroristas hace años comenzaron a utilizar el ciberespacio como una herramienta para reclutamiento, propaganda y coordinación. Estado Islámico, por ejemplo, ha utilizado las redes sociales y plataformas en línea para reclutar seguidores y propagar su ideología. Aunque estos grupos pueden no tener la capacidad técnica de llevar a

cabo ataques cibernéticos sofisticados, su presencia en línea sigue siendo una preocupación importante en términos de radicalización y desestabilización⁴.

- Guerra cibernética: Las tensiones entre estados pueden manifestarse en forma de ciberespionaje y ciberataques de alto nivel. Con lo anterior podemos ver cuerpos de cibersoldados preparados para la guerra cibernética, algo que se ha visto reflejado en el conflicto bélico de Rusia y Ucrania, donde se ha desplegado una gran cantidad de operaciones digitales de escala e impacto con daños reales en las naciones desde el 2022 y hasta la fecha aún con consecuencias latentes.

En última instancia, el ciberterrorismo sigue evolucionando y presentando una amplia gama de desafíos en términos de seguridad y ciberseguridad, allegada a otros temas como la diplomacia, la ética y la legislación. La comunidad internacional debe colaborar para desarrollar estrategias de prevención y respuesta efectivas para abordar esta amenaza en constante cambio, no solamente de temas digitales si no hacia un factor humano que permita conocer del contexto en pro de la prevención.

El ciberterrorismo está presente con matices de diverso y variado impacto, con ello podemos mencionar algunos ejemplos claros para la comprensión del grado de daño que se podría ver reflejado en el mundo material. Bajo la premisa anterior cabe mencionar que hay que hacer mucho hincapié en la conciencia para los usuarios al permitirles conocer que a pesar de que algo se gesticione en el ciberespacio o a través de tecnologías y en un primer momento no es tangible, puede tener consecuencias irreversibles en el mundo real, en el mundo tangible. Por ello, a continuación, se describen con más detalle los impactos en diferentes escalas:

Impacto Social. Uno de los principales factores de los que se vale el ciberterrorismo, el cual está relacionado con su nombre es el miedo y pánico. Muchos de los ciberataques de manera técnica o ataques digitales con el uso de plataformas pueden generar sensaciones de temor en la población, ya que la interrupción de servicios esenciales o la exposición de datos sensibles pueden socavar la confianza en las instituciones y sistemas que dependemos para nuestra vida cotidiana.

En los últimos años vemos incluso un nuevo factor, el control a través del miedo, pues no es necesario recurrir a herramientas sofisticadas, quizá una publicación que pareciera real o es real (según sea el contexto) puede generar que poblaciones enteras tengan miedo a salir de sus hogares. Así ocurre con el caso del narcotráfico en México, donde a través de plataformas de redes sociales se difunden mensajes con fotografías tomadas de plazas públicas para que la población sienta temor (Contreras, 2023).

Los ataques gestados a través del ciberterrorismo a gran escala pueden erosionar la confianza en el gobierno, las empresas, las instituciones. La falta de seguridad percibida en el ciberespacio puede tener efectos duraderos en la confianza hacia el público, atrayendo la desconfianza que va deteriorando el tejido social. Lo anterior puede ser incluso utilizado como herramientas para influir

⁴ Otros grupos que se pueden mencionar en este sentido son grupos de guerra como las FARC en Sudamérica y grupos de narcotraficantes en México.

en procesos políticos y socavar la estabilidad de los gobiernos⁵. La difusión de información falsa, la manipulación de elecciones y la exposición de información comprometedora pueden tener un impacto directo en la política interna y las relaciones internacionales.

Impacto digital. Los ataques dirigidos a infraestructuras críticas, como redes eléctricas, sistemas de agua, nucleares, telecomunicaciones y servicios de salud, pueden causar daños significativos. La interrupción de estos servicios esenciales puede tener efectos devastadores en la vida de las personas y la economía de un país. Algunos daños colaterales pueden resultar en la pérdida de datos personales, financieros y empresariales. Esto puede conducir a la explotación financiera, la usurpación o suplantación de identidad y la exposición de secretos industriales, lo que puede tener consecuencias a largo plazo para las personas y las organizaciones afectadas.

Los ataques diversifican en pérdidas económicas significativas para las naciones y empresas en particular. Asimismo, la interrupción de operaciones comerciales, la degradación de la reputación de una empresa y los costos de recuperación pueden tener un impacto negativo en la economía en general. Para labores de ciberespionaje es usual que los ciberterroristas focalicen en información sensible y a la vez estratégica.

Impacto a escala global. El ciberterrorismo con sus consecuencias directas y colaterales contribuye directamente a la desestabilización global, con ataques que pueden exacerbar tensiones internacionales y llevar a conflictos diplomáticos o incluso militares. Visto desde otra perspectiva, cuando los actores son los países, se puede utilizar el ciberterrorismo como una herramienta para influir en las relaciones internacionales. Los ataques cibernéticos entre naciones pueden generar tensiones y alterar las dinámicas geopolíticas, derivando en conflictos bélicos.

El ciberterrorismo resalta la importancia de la cooperación internacional en materia de ciberseguridad. La comunidad global debe establecer normas y acuerdos para abordar los desafíos únicos presentados por el mismo y promover un ciberespacio más seguro. Aunque esto último pareciera una utopía, se requieren esfuerzos para lograr un primer paso firme entre naciones.

Tal como lo hemos dicho, existen diversos matices y enfoques de impacto, desde lo social y lo político, hasta lo económico o el aspecto digital. Estos impactos pueden ser profundos y duraderos, afectando tanto a individuos como a naciones enteras. La prevención y mitigación del ciberterrorismo requieren una respuesta global coordinada y un enfoque multidisciplinario.

5 Como ya se ha comentado antes, las últimas elecciones en Estados Unidos son ejemplo de ello.

4. Terror digital

Al hablar de miedo o terror, tenemos que hacer mención al ciberterrorismo, a su contexto presente y existente tras él, para así partir hacia un entendimiento post análisis.

El terror digital es una estrategia utilizada en el ciberterrorismo para manipular y difundir el miedo, la desinformación y la propaganda a través de medios digitales con el objetivo de alcanzar diversas metas, como la radicalización, la movilización de seguidores y la desestabilización social. Esta táctica se ha vuelto cada vez más efectiva debido a la omnipresencia de la tecnología y la interconexión global a través de Internet y las redes sociales. A continuación, mencionaremos algunas de las estrategias utilizadas como punto de impacto.

4.1. Manipulación mediática

Los grupos ciberterroristas pueden utilizar medios digitales para difundir información falsa y desinformación con el propósito de sembrar el caos, minar la confianza en las instituciones y difundir su ideología extremista. Pueden aprovechar las plataformas de redes sociales, sitios web falsos y foros en línea para difundir su narrativa y así incentivar a que algunos se sumen a su causa y otros más no realicen acciones por miedo. A menudo se construyen narrativas que explotan temas sensibles y controversiales, como la religión, la política y la discriminación. Utilizan estas narrativas para atraer a individuos vulnerables y manipular sus emociones, lo que puede conducir a la radicalización y esa tendencia llevarla a matizar en un acto que impacte en el mundo material (Waldmann, 2010).

En un proceso de radicalización se busca la creación de una identidad y para ello se pueden usar las redes sociales y otros medios digitales para crear esa pertenencia en línea que confluya con los individuos que buscan pertenecer a algo más grande que ellos mismos. Esto puede conducir a una mayor participación con entes más radicales. En este sentido, llegamos a un aspecto de análisis para la construcción del contexto ciberterrorista: la suma de personas a una causa hace que esta misma se mantenga presente y vigente. Aquí reside la importancia por la que los grupos de ciberterroristas buscan continuamente personas o medios y herramientas digitales de las que valerse, tales como las siguientes.

Plataformas de redes sociales. Ofrecen una plataforma efectiva para que los ciberterroristas recluten nuevos miembros. Pueden utilizar perfiles anónimos o falsos para contactar y radicalizar a individuos en línea, ofreciendo información distorsionada y creando un sentido de comunidad (Cyber Zaintza, s.f.).

Contenido multimedia. El uso de contenido multimedia impactante, como videos de propaganda, imágenes gráficas y discursos extremistas, puede tener un poderoso efecto en la atracción de nuevos adeptos. Estos materiales pueden ser diseñados para apelar a las emociones y fomentar la adhesión a la causa terrorista.

Técnicas de ingeniería social. Los ciberterroristas pueden utilizar técnicas de ingeniería social para manipular psicológicamente a las personas y hacer que realicen acciones que normalmente no harían. Esto puede incluir la persuasión para unirse a grupos extremistas, participar en actividades ilegales o llevar a cabo ataques.

Videojuegos. La utilización de videojuegos como medio para reclutar adeptos para el ciberterrorismo es un fenómeno preocupante que ha ganado atención en los últimos años. Aunque no todos los videojuegos están asociados con el ciberterrorismo, algunos grupos extremistas han aprovechado estas plataformas interactivas para atraer a individuos jóvenes y vulnerables hacia sus agendas. Dentro de los videojuegos, los ciberterroristas pueden introducir propaganda, ya sea a través de mensajes en el juego, imágenes o incluso videos. Esta propaganda puede promover ideologías extremistas, glorificar actos de violencia o presentar narrativas distorsionadas.

4.2 Desestabilización y caos social

Del efecto terror llegamos al efecto del caos, al mero estilo de narrativa filosófica en el que la devastación se hace presente, jugando un papel clave la desestabilización, la cual es la suma de los factores anteriormente mencionados.

Al difundir mensajes de odio, polarización y discriminación, los ciberterroristas pueden contribuir a la división social y étnica. Estos mensajes pueden provocar conflictos internos y debilitar la cohesión de la sociedad. Hemos visto a lo largo de la historia levantamientos en pro de causas sociales para derrocar regímenes (Khader, 2012) y otros casos más en donde logran desestabilizar sociedades.

Para este último supuesto se pueden utilizar plataformas en línea para coordinar ataques físicos o digitales. Esto puede incluir la planificación de ataques terroristas, ataques cibernéticos o el fomento de disturbios y protestas violentas.

El terror como parte digital en el ciberterrorismo es una estrategia multifacética que busca influir en la opinión pública, radicalizar a individuos y desestabilizar la sociedad utilizando medios digitales y redes sociales. La rapidez y la amplitud de la comunicación en línea hacen que esta táctica sea poderosa y desafiante de contrarrestar, y subraya la importancia de la educación digital y la ciberseguridad.

5. Análisis y contexto

El análisis de contexto es fundamental en la comprensión y la prevención del ciberterrorismo. Para abordar este tema, es necesario considerar tanto las unidades o elementos involucrados en el análisis como las técnicas de perfilación y los métodos utilizados para identificar posibles amenazas, con el fin de tener un parámetro de prevención antes de que se matice en un resultado material irreversible.

Para lo anterior se necesita un enfoque multidisciplinario, tal como comentábamos al principio, para poder identificar y discernir, entre otras, las amenazas cibernéticas, las motivaciones, las técnicas y herramientas o las vulnerabilidades. Todas ellas las vamos a comentar a continuación.

Cuando hablamos de amenazas cibernéticas nos referimos a las actividades y actores que representan una amenaza para la seguridad cibernética. Esto incluye individuos, grupos, organizaciones y estados que buscan llevar a cabo ataques cibernéticos con fines maliciosos, en este caso ciberterroristas. En cuanto a las motivaciones, comprender aquellas existentes detrás de los ataques cibernéticos es crucial para identificar a los actores y sus objetivos. Sus fines pueden ser políticos, económicos, ideológicos o simplemente maliciosos. Por otra parte, analizar las técnicas y herramientas utilizadas en ataques cibernéticos puede proporcionar información sobre la sofisticación de los actores y su nivel de conocimiento técnico. Por último, identificar las vulnerabilidades en sistemas y redes es esencial para prevenir ataques cibernéticos. Esto implica comprender las debilidades potenciales que podrían ser explotadas por los actores maliciosos, esto en una escala un poco más técnica pero aplicable al contexto.

6. Profiling en el ciberterrorismo

El profiling⁶ o perfilación en el ciberterrorismo implica la creación de perfiles de los actores involucrados y sus características. Esto se hace con el objetivo de identificar patrones, comportamientos y motivaciones que puedan ayudar a prevenir o mitigar ataques. En este sentido, en 2019 los investigadores Macdonald, Jarvis y Lavis. En su estudio: “Cyberterrorism Today? Findings from a follow-on survey of researchers”, refuerzan la relevancia de analizar los componentes ideológicos y conductuales dentro del ciberterrorismo. A partir de una encuesta realizada a especialistas en 2017, los autores muestran un consenso creciente en torno a ciertos rasgos esenciales de este fenómeno: la motivación política o ideológica, el uso de medios digitales como instrumento o blanco y la generación de miedo en la sociedad como efecto principal. Del mismo modo, los investigadores prevén que la amenaza del ciberterrorismo se percibe en aumento y que distintos actores (incluyendo Estados y organizaciones terroristas) pueden estar involucrados. Frente a ello, resaltan la necesidad de medidas preventivas, como el fortalecimiento de infraestructuras, la cooperación internacional y la educación en ciberseguridad, antes que recurrir a respuestas excepcionales o drásticas (Macdonald, Jarvis & Lavis, 2019).

De igual manera encontramos esta terminología en apartados digitales similares (AT Internet, s.f.). Algunos aspectos clave del profiling para el ciberterrorista son:

Características demográficas. Esto incluye factores como la edad, la nacionalidad, la educación y el género de los individuos involucrados. Estos aspectos pueden proporcionar pistas sobre sus posibles motivaciones y entorno social.

6 “Vicente Garrido define el perfil criminal o criminológico (profiling) como la disciplina de la ciencia forense que se ocupa de analizar las huellas del comportamiento en una escena del crimen con el objeto de proveer información útil a la policía para la captura de un delincuente desconocido” (Garrido, 2012, p. 11).

Habilidades técnicas. Evaluar las habilidades técnicas de los actores es crucial para comprender su nivel de experiencia y el tipo de amenazas que pueden representar.

Historial de actividades. Analizar el historial de actividades en línea puede revelar patrones de comportamiento y preferencias. Esto puede ayudar a identificar si un individuo está involucrado en actividades sospechosas o extremistas.

Comunicaciones y contactos. Examinar las comunicaciones y los contactos en línea puede proporcionar información sobre las redes y grupos en los que un individuo está involucrado. Esto es fundamental para rastrear posibles colaboraciones y asociaciones.

Análisis de lenguaje. La evaluación del lenguaje utilizado en publicaciones en línea puede proporcionar pistas sobre las creencias ideológicas y las intenciones de los individuos. Esto incluye el uso de términos extremistas, discursos de odio y retórica violenta.

Patrones de conexiones. Identificar patrones de conexiones entre individuos y grupos en línea puede revelar las redes y alianzas en el ciberespacio. Esto es esencial para rastrear la difusión de ideas y la colaboración en actividades extremistas.

Análisis de contenido multimedia. Examinar imágenes y videos compartidos en línea puede revelar simbología extremista, glorificación de la violencia o evidencia de actividades ilícitas.

Técnicas de reconocimiento. Los ciberterroristas pueden llevar a cabo técnicas de reconocimiento en línea para identificar objetivos potenciales. Esto puede incluir la recopilación de información sobre infraestructuras críticas o individuos clave.

Análisis de comportamiento de grupo. Observar cómo los grupos interactúan en línea puede ayudar a entender cómo se difunden las ideologías extremistas, cómo se movilizan los miembros y cómo se planifican actividades.

Dentro de toda la metodología a implementar durante y después de la construcción de un profiling para el ciberterrorista, podemos mencionar algunas técnicas a tener en consideración dentro del proceso de análisis de contexto, entre las cuales encontramos:

Monitoreo de dark web. Muchas actividades extremistas y ciberterroristas ocurren en la “dark web”⁷. Monitorear estos espacios puede proporcionar información valiosa sobre la planificación y ejecución de ataques.

7 La “Dark Web” es una parte de Internet que no está indexada por los motores de búsqueda tradicionales y que requiere navegadores especializados, como Tor, para acceder a ella. Se caracteriza por el anonimato de sus usuarios, lo que la convierte en un espacio donde se pueden realizar tanto actividades legítimas como ilegales.

Inteligencia cibernética. Implica la recolección y el análisis de datos relacionados con amenazas cibernéticas. Esto puede incluir el monitoreo de foros en línea, redes sociales y comunicaciones cifradas.

Análisis de comportamiento. Observar patrones de comportamiento en línea puede ayudar a identificar actividades sospechosas o inusuales que podrían estar relacionadas con el ciberterrorismo.

Análisis de tendencias. Identificar tendencias emergentes en el ciberterrorismo, como nuevos tipos de ataques o técnicas, es crucial para estar preparados y desarrollar estrategias de prevención.

Análisis de amenazas. Implica evaluar la gravedad y la probabilidad de amenazas cibernéticas específicas. Esto ayuda a priorizar recursos y medidas de seguridad.

Contexto geopolítico. Comprender el contexto geopolítico es esencial, ya que las tensiones y conflictos internacionales pueden tener un impacto en las motivaciones y actividades de los actores cibernéticos.

Inteligencia abierta y cerrada. La inteligencia abierta implica el uso de fuentes públicas, como redes sociales y sitios web, para recopilar información. La inteligencia cerrada se basa en información clasificada o exclusiva de fuentes gubernamentales o corporativas.

Análisis de Amenazas Persistente Avanzada (APT). Las APT son ataques de alto nivel y persistentes. El análisis de APT involucra rastrear los patrones de ataque a lo largo del tiempo y entender las técnicas, tácticas y procedimientos utilizados por los actores para identificar sus objetivos y motivaciones.

Análisis de redes sociales. El análisis de redes sociales implica monitorear plataformas online para identificar la propagación de contenido extremista, la interacción entre individuos y la formación de comunidades en entornos digitales

Del mismo modo, aportes como el de Jiménez Serrano (2012) en el Manual práctico del perfil criminológico o Miranda Díaz (2017) “*Introducción a la perfilación criminal. Visión CriminológicaCriminalística*”, resultan útiles para trasladar la línea de análisis del profiling al ámbito digital. Los autores explican que el perfil criminológico se construye a partir de la identificación de características estables y patrones conductuales repetitivos, considerando elementos como el modus operandi, la firma del delincuente, la geografía criminal y la victimología, los cuales permiten inferir motivaciones, comportamientos y probables escenarios futuros

Aunque principalmente el manual de Jiménez Serrano se centra en el ámbito forense y policial tradicional, su metodología puede aplicarse al ciberterrorismo, donde el “escenario del crimen” se traduce como el entorno digital; el modus operandi en técnicas de ataque (tal como los que ya se

han mencionado a manera de ejemplo como malware, ransomware, APT, entre otros) o difusión de propaganda; la geografía en la localización virtual de foros y redes; y finalmente la victimología en la selección de objetivos estratégicos (individuos, estados, organizaciones, bases de datos, por mencionar algunos). Así, al igual que en el ámbito físico, la perfilación digital permite orientar las investigaciones hacia un enfoque preventivo más que reactivo, anticipando riesgos y reconociendo patrones ideológicos y conductuales de actores extremistas en entornos digitales. En resumen, el análisis de contexto se convierte en una herramienta crítica para comprender y prevenir el ciberterrorismo. El profiling y los métodos de análisis permiten identificar patrones y comportamientos que pueden ser indicativos de posibles amenazas. Esto es esencial para tomar medidas proactivas y proteger la seguridad a distintas escalas, a nivel individual, empresarial, nacional.

La colaboración entre agencias de seguridad, organizaciones internacionales, empresas y la sociedad civil es crucial para combatir el ciberterrorismo. La prevención se basa en compartir información, desarrollar políticas de seguridad sólidas, educar sobre riesgos en línea y promover un entorno digital seguro.

7. Conclusiones

En resumen, el análisis de contexto en el ciberterrorismo se basa en la recopilación y el análisis de información para comprender las amenazas cibernéticas y las motivaciones detrás de ellas. El profiling y los métodos de análisis ayudan a identificar patrones, comportamientos y actividades que podrían indicar la presencia de actores maliciosos. La cooperación y la prevención son esenciales para abordar esta amenaza en constante evolución.

Una necesidad crítica es educar y concienciar a la sociedad sobre las amenazas digitales y el ciberterrorismo. Las personas deben comprender cómo reconocer señales de radicalización en línea, cómo proteger su información y cómo reportar actividades sospechosas. Por su parte, las agencias gubernamentales, las empresas, las instituciones académicas y las organizaciones internacionales deben colaborar para compartir información y recursos. La cooperación entre sectores puede ayudar a prevenir ataques cibernéticos y contrarrestar el ciberterrorismo.

A medida que evolucionan las tácticas de ciberterrorismo, se necesitan constantemente soluciones de ciberseguridad innovadoras. Esto incluye el desarrollo de tecnologías de detección y prevención avanzadas, así como la promoción de buenas prácticas en el diseño de sistemas seguros. En este sentido, los gobiernos deben establecer marcos legales y políticos claros para abordar el ciberterrorismo y castigar a los culpables. Esto implica la definición precisa de ciberdelitos y la colaboración internacional en la persecución de delincuentes cibernéticos.

Equilibrar la privacidad y la seguridad en línea es un desafío. Las consideraciones sobre la recopilación de datos, la vigilancia y el acceso a la información personal deben ser tratadas cuidadosamente para evitar abusos y vulnerabilidades. Internet y el ciberespacio han traído consigo

tanto ventajas como desafíos, incluido el ciberterrorismo. La evolución de la tecnología ha permitido a actores maliciosos utilizar el ciberespacio para propagar el miedo, la desinformación y la violencia.

El ciberterrorismo es un fenómeno complejo que abarca una amplia gama de actores, motivaciones y técnicas. Los contrastes en términos de métodos y objetivos han creado un panorama diverso y en constante evolución. Asimismo, la manipulación mediática y el terror digital son tácticas utilizadas por los ciberterroristas para radicalizar, reclutar y desestabilizar a través de medios digitales. Las redes sociales y los videojuegos se han convertido en canales para difundir ideologías extremistas.

En última instancia, el ciberterrorismo presenta un desafío global que requiere una respuesta coordinada a nivel internacional. La seguridad cibernética, la legislación y la educación se convierten en pilares esenciales para mantener el equilibrio entre la libertad en línea y la protección contra amenazas cibernéticas.

8. Referencias bibliográficas

America's Cyber Defense Agency (s.f), People's Republic of China Threat Overview and Advisories. AT Internet. (s.f.). Elaboración de perfiles

Basque Cybersecurity Centre. (s.f.). Ciberterrorismo. <https://www.ciberseguridad.eus/ciberglosario/ciberterrorismo> Buxton, O. (14 julio 2022), Stuxnet: ¿Qué es y cómo funciona?, Avast Academy,

CCDCOE. (2015). *Power grid cyberattack in Ukraine*

CISA. (s.f.). *China cyber threat overview and advisories*.

Cyber Zaintza (s.f.), *Glosario de términos de ciberseguridad*.

Contreras, L. (10 agosto 2023), *CJNG anunció presunto toque de queda en Tepotzotlán con narcomensaje*, Infobae.

Conway, M. (2017). Determining the role of the internet in violent extremism and terrorism: Six suggestions for progressing research. *Studies in Conflict & Terrorism*, 40(1), 77–98.

Denning, D. E. (2001). Activism, hacktivism, and cyberterrorism: The internet as a tool for influencing foreign policy. En J. Arquilla & D. Ronfeldt (Eds.), *Networks and netwars* (pp. 239–288). RAND Corporation.

Díaz, D. N. M. (2017). Introducción a la perfilación criminal [PDF]. *Revista CLEU*.

Easterly, J. (7 mayo 2023), *The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years*, America's Cyber Defense Agency.

Gómez Sevilla, J. (2024). Ciberespacio y ciberterrorismo: Una aproximación a los nuevos campos de batalla inmateriales. *Revista Internacional de Estudios sobre Terrorismo*.

IBM. (s. f.). Ransomware. IBM Think.

- Infobae. (2023, agosto 10). CJNG anunció presunto toque de queda en Tepetzotlán con narcomensaje.
- Jarque, J. M. (2005). El País frente a los atentados del 11-S norteamericano: “acriticismo” y alineamiento discursivo con la postura estadounidense.
- Jiménez Serrano, J. (2012). *Manual práctico del perfil criminológico (2.ª ed.)*. Lex Nova.
- Khader, B. (2012). *La primavera árabe: el día después*, Papeles.
- Martineau, M., Spiridon, E., & Aiken, M. (2023). A comprehensive framework for cyber behavioral analysis based on a systematic review of cyber profiling literature. *Forensic Sciences*, 3(3), 452–477.
- McAfee. (s. f.). ¿Qué es el malware?
- Macdonald, S., Jarvis, L., & Lavis, S. (2019). Cyberterrorism today? Findings from a follow-on survey of researchers. *Studies in Conflict & Terrorism*, 42(1–2), 17–45.
- Oficina de las Naciones Unidas contra la Droga y el Delito. (s. f.). Módulo 14: Hacktivismo, terrorismo, espionaje, campañas de desinformación y guerra en el ciberespacio. Serie de Módulos Universitarios: Delitos Cibernéticos.
- Rid, T. (2013). *Cyber war will not take place*. Oxford University Press.
- Tshimuila, J. M., Nkashama, D. K., Muabila, J. T., et al. (2024). Psychological profiling in cybersecurity: A look at LLMs and psycholinguistic features [Preprint]. arXiv.
- Universidad del Rosario. (s. f.). Repositorio institucional: Documento académico
- Waldmann, P. (26 abril 2010), Radicalización en la diáspora: por qué musulmanes en Occidente atentan contra sus países de acogida, Real Instituto Elcano.