

*Maestría en Estudios Internacionales*

# **El papel de las TICs en la radicalización terrorista: El caso del Estado Islámico y los lobos solitarios**

**Autoría:** Singer González, Sofía Milagros

**Año:** 2025

## **¿Cómo citar este trabajo?**

Singer González, S. (2025) "*El papel de las TICs en la radicalización terrorista: El caso del Estado Islámico y los lobos solitarios*". [Tesis de maestría. Universidad Torcuato Di Tella]. Repositorio Digital Universidad Torcuato Di Tella  
<https://repositorio.utdt.edu/handle/20.500.13098/13545>

El presente documento se encuentra alojado en el **Repositorio Digital de la Universidad Torcuato Di Tella** bajo una licencia Creative Commons Atribución-No Comercial-Compartir Igual 4.0 Internacional

**Dirección:** <https://repositorio.utdt.edu>



UNIVERSIDAD TORCUATO DI TELLA  
Departamento de Ciencia Política y Estudios Internacionales  
Maestría en Estudios Internacionales

**El papel de las TICs en la radicalización terrorista:  
El caso del Estado Islámico y los lobos solitarios**

Alumna: Sofía Milagros Singer González  
Tutor: Jorge Battaglino

Firma del/la tutor/a

Abril, 2025

## DECLARACIÓN JURADA

En cumplimiento de las reglas de ética universitaria de la Universidad Torcuato Di Tella establecidas en el Reglamento de Estudios de Posgrado, certifico que esta tesis es mi propio trabajo original, basado en mi estudio y/o investigación personal y que he reconocido todo el material y las fuentes utilizadas en su preparación citándolos correctamente.

Certifico, además, que toda idea tomada de libro, artículo, tesis, ponencia, documento de trabajo o cualquier otra fuente, en forma impresa o electrónica, se menciona específicamente haciendo referencia a su origen, que me he asegurado de que sea absolutamente claro qué ideas son propias y cuáles se toman de esas fuentes, y que las citas textuales se indican entre comillas.

También certifico que este trabajo/tesis (o partes significativas del mismo) no se ha presentado previamente para su evaluación en ninguna otra unidad académica de la Universidad o en otra institución, excepto cuando se haya otorgado un permiso específico, y que no he copiado ni plagiado, ni en parte ni en su totalidad, el trabajo de otras personas.

Declaro conocer que, de conformidad con el Reglamento de Estudios de Posgrado de la UTDT, el incumplimiento de las reglas de ética universitaria podrá llevar a la instrucción de un procedimiento disciplinario en mi contra.

## ***Abstract***

*Este trabajo investiga cómo el Estado Islámico (ISIS) ha utilizado las tecnologías de la información y la comunicación (TICs), particularmente las redes sociales, para radicalizar y reclutar individuos, especialmente a los "lobos solitarios" desde 2014 hasta 2017.*

*La hipótesis central es que el uso estratégico de las TICs por parte de ISIS ha transformado radicalmente la escena de la seguridad internacional. La investigación se centra en analizar cómo ISIS ha aprovechado las características de las redes sociales para construir una narrativa digital atractiva, dirigida principalmente a jóvenes marginados, y cómo ha utilizado estos espacios virtuales para facilitar la conexión entre ellos, ampliando su alcance, y llevándolos a la radicalización y la violencia a escala global. Se evidencia que las TICs, han contribuido a la emergencia de una nueva generación de terroristas, los "lobos solitarios", que actúan de manera autónoma pero inspirados por la ideología de grupos terroristas, desde cualquier parte del mundo.*

*Asimismo, se examina el impacto de esta estrategia en la seguridad de los Estados y de los ciudadanos, así como los desafíos que plantea para las políticas de seguridad tradicionales, y se destaca la necesidad de desarrollar nuevas estrategias coordinadas internacionalmente para hacer frente a la amenaza que representan.*

palabras clave: terrorismo, radicalización, lobos solitarios, yihadismo, redes sociales, una virtual, extremismo, prevención, globalización, seguridad internacional.

## **Tabla de contenidos**

### **CAPÍTULO 1: INTRODUCCIÓN**

|                                                  |    |
|--------------------------------------------------|----|
| 1.1 Planteamiento del problema .....             | 1  |
| 1.2 Justificación e importancia del estudio..... | 3  |
| 1.3 Objetivos de la investigación.....           | 4  |
| 1.4 Pregunta de investigación e hipótesis.....   | 7  |
| 1.5 Metodología y enfoque teórico.....           | 9  |
| 1.6 Estructura de la tesis.....                  | 18 |

### **CAPÍTULO 2: FUNDAMENTOS TEÓRICOS Y CONCEPTUALES**

|                                                                  |    |
|------------------------------------------------------------------|----|
| 2.1. Definición y evolución del terrorismo.....                  | 19 |
| 2.2 El caso del Estado Islámico (ISIS).....                      | 22 |
| 2.3. Radicalización y terrorismo digital.....                    | 24 |
| 2.4. Lobos solitarios: características y perfil psicológico..... | 25 |
| 2.5. La seguridad internacional en la era digital.....           | 28 |

### **CAPÍTULO 3: EL USO DE LAS TICs POR PARTE DE ISIS**

|                                                                      |    |
|----------------------------------------------------------------------|----|
| 3.1. Contexto y surgimiento de ISIS en el ámbito digital.....        | 31 |
| 3.2. Estrategias de comunicación y propaganda en redes sociales..... | 31 |
| 3.3. Plataformas utilizadas y su impacto.....                        | 39 |

### **CAPÍTULO 4: RADICALIZACIÓN Y MOVILIZACIÓN DE LOBOS SOLITARIOS**

|                                                                                                                  |    |
|------------------------------------------------------------------------------------------------------------------|----|
| 4.1. De la narrativa digital a la acción violenta:<br>Factores de vulnerabilidad y atracción de los jóvenes..... | 41 |
| 4.2. Lobos solitarios radicalizados en redes.....                                                                | 42 |

|                                                                                                          |    |
|----------------------------------------------------------------------------------------------------------|----|
| 4.3. Impacto en la seguridad de los Estados y ciudadanos:                                                |    |
| ISIS in America.....                                                                                     | 45 |
| 4.4 Manifestaciones de la radicalización: ataques inspirados por ISIS en Estados Unidos (2014–2017)..... | 52 |

## **CAPÍTULO 5: ANÁLISIS DE LA ESTRATEGIA DIGITAL DEL ESTADO ISLÁMICO.**

|                                                                                         |    |
|-----------------------------------------------------------------------------------------|----|
| 5.1. Resumen de hallazgos principales.....                                              | 54 |
| 5.2.Estrategia Comunicacional de ISIS en Twitter: Objetivos, Audiencias y Tácticas..... | 58 |
| 5.3 Nota metodológica.....                                                              | 61 |
| 5.4. Limitaciones del análisis.....                                                     | 62 |

## **CAPÍTULO 6: CONCLUSIONES Y RECOMENDACIONES**

|                                                                          |           |
|--------------------------------------------------------------------------|-----------|
| 6.1. Limitaciones de las políticas de seguridad tradicionales            |           |
| El papel de las plataformas digitales y la regulación de contenidos..... | 64        |
| 6.2. Implicaciones para la seguridad global.....                         | 64        |
| 6.3. Propuestas para abordar la radicalización digital:                  |           |
| Cooperación internacional en la lucha contra el terrorismo digital.....  | 66        |
| 6.4. Reflexión final.....                                                | 70        |
| <b>BIBLIOGRAFÍA .....</b>                                                | <b>72</b> |

## **ANEXO**

## CAPÍTULO 1: INTRODUCCIÓN

### *1.1. Planteamiento del problema*

Y.O.D.O. *“You only die once. Why not make it martyrdom”*

Aunque sea difícil de creer, la frase expuesta aquí arriba, representa un eslogan utilizado por los grupos terroristas extremistas. A través de ella se puede ver cómo mediante la utilización de un lenguaje simple y cercano se difunden ideas que transmiten, infunden e incluso contagian sentimientos particulares que tienen el objetivo de acercar a los individuos a los grupos terroristas.

Este eslogan encapsula la esencia de la propaganda radical fundamentalista terrorista del Estado Islámico que tuvo como objetivo radicalizar y movilizar a individuos dispuestos a sacrificar sus vidas en nombre de una causa extremista en la que creen. El apelar a emociones como el miedo, la ira y la búsqueda de un propósito, intentan deshumanizar al "otro" y de esta manera justificar ciertas acciones violentas que estos grupos puedan cometer. La eficacia de este tipo de mensajes hoy en día, se ve amplificada por el uso de las redes sociales que facilitan su difusión a gran escala y permiten la creación de comunidades virtuales donde los individuos radicalizados pueden encontrar un sentido de pertenencia.

Cada uno de los que se adhiere a una ideología extremista tiene sus propias motivaciones, razones, así como debilidades e inseguridades. La frase "YODO" actúa como un detonante emocional que puede resonar en aquellos que se sienten marginados, desconectados o aislados en sus propios mundos.

En última instancia, la frase también representa la amenaza significativa que son los lobos solitarios para la seguridad global. Este tipo de mensajes pueden incitar a individuos a cometer actos terroristas y desestabilizar sociedades, al promover la violencia y el odio e infundiendo miedo y terror, principal objetivo de estos grupos terroristas extremistas.

El informe “ISIS in America” publicado en el New York Times y realizado dentro del Program on Extremism de The George Washington University, señala que ya para diciembre 2015, había más de 300 personas de nacionalidad estadounidense o que al menos viven en dicho país consideradas simpatizantes activos de ISIS en las redes sociales, difundiendo propaganda e interactuando con personas de ideas afines. El compromiso real de los simpatizantes con ISIS varía significativamente, desde los que simplemente se sienten inspirados por su mensaje hasta los que acaban dando el salto del mundo virtual a la militancia real. (New York Times, 2016)

Si tomamos a Dubet en su libro *La época de las pasiones tristes*, podemos ver cómo los sentimientos de ira y resentimiento acceden a la esfera pública de la manera más cruda y directa. La capacidad de decir públicamente las propias emociones y opiniones hace de cada uno de nosotros un militante de su propia causa. (Dubet, 2020).

En este caso, la causa de un otro que se toma como propia. Son los grupos terroristas quienes utilizan estos sentimientos de resentimiento para aprovechar y fomentar mensajes que se caracterizan por una visión del mundo donde los otros son vistos como responsables de las propias desgracias, de todos nuestros males, fomentando una mentalidad paranoica y aislamiento social. Esto luego se refleja en la política contemporánea, donde la desconfianza y el odio hacia el otro distinto a un nosotros,

se han convertido en elementos centrales del discurso terrorista extremista.

## ***1.2. Justificación e importancia del estudio***

Tomando la frase de Grunewald, Chermak & Frieilich (2013), los ataques terroristas realizados por lobos solitarios suelen considerarse la forma más desconcertante e impredecible de terrorismo dado que es muy difícil darse cuenta cuándo, cómo y por qué una persona se radicalizó y llevó a cabo el ataque.

Este tipo de investigaciones es de vital importancia dado que se debe comprender la relevancia de las amenazas presentadas por los grupos terroristas y cómo si esto no se detiene, sumado al avance de las tecnologías de información en la actualidad, se puede llegar a que dicha amenaza escale de manera sin precedentes. Con tal solo pensar en el uso que estos grupos pueden darle a la inteligencia artificial, es suficiente para entender la gravedad del asunto.

Es muy difícil estimar cuántos simpatizantes y lobos solitarios fueron inspirados o reclutados a través de las redes sociales, pero, incluso si ISIS haya reclutado un pequeño porcentaje de personas, significa un gran peligro para las sociedades.

Al estudiar las estrategias de los grupos terroristas, en este caso de ISIS, y su intento de expandir su causa a través de los medios virtuales, podemos comprender sus fortalezas y debilidades y de esta manera planear cómo anticipar y prevenir futuras situaciones similares o de otros grupos terroristas extremistas que puedan tomar estos recursos a su favor.

Para combatir esta amenaza, es necesario desarrollar estrategias integrales que aborden tanto las causas centrales de la radicalización como las manifestaciones más visibles

del extremismo violento. Esto se va a dar no sólo con estrategias de seguridad y defensa, sino también es necesario un proceso de educación para la ciudadanía.

Esto permitirá a los gobiernos, las agencias de seguridad y las plataformas y compañías tecnológicas desarrollar estrategias más efectivas para combatir el terrorismo así como con una correcta educación, tener ciudadanos más integrados, reflexivos y tolerantes que no sean permeables ni influenciables a estos ideales.

A su vez, la importancia de esta investigación radica en que los resultados de la misma podrían servir de base para la elaboración de políticas públicas que regulen el uso de las redes sociales y otras plataformas digitales sociales, con el objetivo de prevenir la difusión de contenido extremista y proteger a sus ciudadanos, en especial a los niños y jóvenes dentro del mundo virtual.

Al comprender las tácticas utilizadas por los grupos terroristas, podemos educar a la población sobre los riesgos de la radicalización y fomentar una ciudadanía digital crítica. Esto es fundamental para fortalecer la resiliencia de las sociedades frente a la propaganda extremista. La proliferación de información falsa, las burbujas de filtro y la polarización en las redes sociales representan amenazas a la calidad de la deliberación dentro de estos ámbitos virtuales.

Para esto, es central garantizar la protección de la privacidad y de los datos de los usuarios, y ver dónde están fallando estos grandes medios y compañías de tecnología.

### ***1.3. Objetivos de la investigación***

Esta investigación tiene como objetivo general analizar cómo el Estado Islámico (ISIS) ha utilizado las tecnologías de la información y la comunicación (TICs), particularmente

las redes sociales, para radicalizar y reclutar individuos, con especial énfasis en los "lobos solitarios", y evaluar el impacto de esta estrategia en la seguridad internacional entre 2014 y 2017.

Para ello, se examinarán las estrategias digitales empleadas por ISIS para la difusión de su ideología extremista, la construcción de narrativas digitales atractivas y la segmentación de sus mensajes hacia jóvenes marginados y vulnerables. Además, se estudiará cómo la radicalización en entornos digitales ha impactado la seguridad internacional, modificando las dinámicas del terrorismo y desafiando los enfoques tradicionales de seguridad y lucha antiterrorista.

La investigación evaluará las respuestas internacionales ante esta amenaza y explorará la necesidad de desarrollar estrategias innovadoras y coordinadas para mitigar el uso de las TICs con fines terroristas, con el objetivo de fortalecer la seguridad global y reducir el riesgo de nuevos procesos de radicalización en línea.

Su relevancia radica en el hecho de que ISIS ha sido pionero en el uso de herramientas digitales para difundir su ideología y captar nuevos miembros, lo que ha transformado la naturaleza del terrorismo en el siglo XXI.

La radicalización digital ha dado lugar a una nueva generación de terroristas "autónomos" que operan fuera de las estructuras tradicionales, complicando la identificación y prevención de ataques.

Los Estados han enfrentado dificultades para adaptar sus estrategias de seguridad a este nuevo escenario, lo que subraya la necesidad de respuestas más eficaces.

Para comprender el fenómeno del terrorismo digital y su impacto en la seguridad internacional, esta investigación se estructura en torno a una serie de objetivos específicos que permiten abordar la problemática de manera integral. En primer lugar, se examinará el papel de las tecnologías de la información y la comunicación (TICs) en la estrategia de expansión de ISIS, analizando cómo estas herramientas han facilitado la difusión de su ideología y el reclutamiento de nuevos seguidores. A continuación, se identificarán las principales plataformas digitales empleadas por el grupo terrorista, evaluando su alcance y efectividad en la propagación de contenido extremista.

Posteriormente, se analizarán los métodos y técnicas utilizadas por ISIS para la radicalización en redes sociales, con un enfoque especial en la segmentación del mensaje hacia jóvenes marginados y vulnerables, quienes representan el grupo más susceptible a la captación. En este marco, se explorará el fenómeno de los "lobos solitarios", describiendo sus características sociológicas y psicológicas, así como su conexión con la propaganda digital del grupo. A través del estudio de casos concretos, se buscará evidenciar cómo estos individuos, inspirados por la narrativa extremista en línea, han llevado a cabo ataques sin una relación orgánica con la estructura central de ISIS.

Asimismo, se evaluará el impacto de la radicalización digital en la seguridad internacional, examinando los desafíos que este fenómeno plantea para los Estados y sus estrategias de lucha contra el terrorismo. Se verán las respuestas y medidas adoptadas por los gobiernos y organismos internacionales, con el objetivo de determinar su eficacia y detectar posibles limitaciones en su implementación. Finalmente, se propondrán estrategias de prevención y regulación para mitigar el uso de las TICs con fines terroristas,

destacando la importancia de la cooperación internacional y el rol de las plataformas digitales en la moderación de contenido extremista.

Con estos objetivos, la investigación busca proporcionar un análisis detallado y fundamentado sobre la relación entre el terrorismo y la tecnología, así como generar aportes para el desarrollo de nuevas estrategias de seguridad adaptadas a las dinámicas del terrorismo digital en el siglo XXI.

#### ***1.4. Pregunta de investigación e hipótesis***

Dada la laguna de seguridad generada en el espacio cibernético, la pregunta que surge de esta investigación es: ¿Cómo el Estado Islámico utilizó las TICs especialmente las Redes sociales para su modelo de radicalización de individuos y potencial reclutamiento del terrorismo fundamentalista, especialmente en el caso de los lobos solitarios? La propuesta es analizar cómo dicha organización hizo uso de las herramientas tecnológicas y del espacio virtual y su vacío regulatorio para radicalizar y ganar adeptos a través de la difusión de ciertos mensajes.

ISIS, supo cómo distribuir mensajes a través de sitios de medios digitales, tales como Facebook, Twitter (X)<sup>1</sup>, Instagram y Telegram, haciéndose de los datos de los usuarios para desarrollar distintas estrategias de captación, adoctrinamiento, adiestramiento, financiación y preparación de ataques terroristas, aprovechando las insuficientes capacidades estatales alcanzadas hasta ahora. Las redes sociales permiten a los individuos subir sus actividades y al mismo tiempo descargar información desde cualquier lugar y en cualquier momento. Además, horizontaliza la jerarquía del grupo

---

<sup>1</sup> De ahora en adelante se nombrará a la plataforma X como Twitter.

terrorista volviéndolo más impredecible. Por otro lado, el uso de estas plataformas y de los datos recopilados de los usuarios de Internet habilita un nuevo plano en el que actuar y cometer los actos terroristas: el ciberespacio.

### Hipótesis

El Estado Islámico empleó de manera estratégica las Tecnologías de la Información y la Comunicación (TIC), especialmente las redes sociales, para identificar, radicalizar y posteriormente reclutar a individuos vulnerables, fomentando su adhesión al terrorismo fundamentalista contribuyendo a la noción de un “enemigo común”.

En este trabajo nos referiremos al concepto reclutamiento terrorista como el proceso por el cual organizaciones terroristas atraen y convencen a otros individuos extremistas para unirse a sus filas y participar en actividades terroristas ya sea de manera coordinada y conjunta, o de manera individual y aislada. Este proceso implica una serie de estrategias y tácticas diseñadas para captar nuevos miembros y expandir la influencia del grupo terrorista.

La organización terrorista logró convertir a Internet en uno de sus principales soportes de propaganda. Este espacio les ofrece un alcance global y una acción inmediata para formar una red de comunicación.

De esta manera, podemos abordar esta cuestión tanto como un problema de seguridad para los Estados, como de los ciudadanos (Seguridad Humana). Todas estas nuevas amenazas tienen mucho más impacto en la población civil que en los militares. No sólo se debe lidiar contra los terroristas en un plano físico (que también es favorecido por las estrategias de cooptación), sino que también en uno virtual.

Este espacio permite conectar a lobos solitarios y distintos núcleos de seguidores con las células terroristas, aun cuando éstos no se correspondan al lugar geográfico donde se encuentren estos grupos, generándoles un sentido de pertenencia. Para este nuevo tipo de amenaza todavía no se tiene una respuesta acorde.

### ***1.5. Metodología y enfoque teórico***

Este proyecto busca ser un estudio ideográfico o investigación de inferencia descriptiva.

Durante el desarrollo de esta investigación se utilizan los conceptos centrales de terrorismo y lobos solitarios, así como también las nociones de la transformación de los medios de comunicación de Habermas y su efecto en la radicalización de los individuos.

Las redes sociales permitieron al grupo terrorista identificar posibles individuos con características psicológicas y sociales que los hacían más vulnerables a la radicalización. Luego, fueron muy hábiles en crear narrativas persuasivas a través de contenidos extremistas y propagándolo, logrando construir comunidades virtuales radicalizadas y proporcionando a los potenciales reclutas las herramientas y la motivación necesarias para llevar a cabo ataques violentos de manera autónoma.

Dichas redes aceleran este proceso al proporcionar un entorno donde los individuos pueden ser expuestos a una constante inundación de propaganda extremista. Permiten una comunicación altamente personalizada, y junto con la interacción con otros individuos radicalizados, refuerza las creencias extremistas y facilita la transición hacia la violencia. Al aprovechar las necesidades humanas fundamentales, los mensajes extremistas pueden resonar con individuos que buscan sentido de pertenencia o identidad. (McElreath et al, 2018)

Esta investigación busca analizar cómo interactúan los usuarios entre sí y con los contenidos presentes en las redes sociales, (comentarios, compartidos, reacciones). Si existen patrones de interacción específicos entre los reclutadores y los potenciales reclutas, y principalmente las narrativas creadas en las redes: análisis de historias, ideas y mensajes que ISIS utiliza para atraer y radicalizar a individuos.

Se analizarán las principales narrativas utilizadas para radicalizar a los individuos (narrativas de victimización, de “comunidad”, etc.) así como las técnicas que se utilizan (apelación a las emociones, uso de testimonios, simplificación de mensajes). De esta forma podremos ver cómo estas contribuyen a la construcción de una imagen del "otro" que justifica la violencia como forma de radicalización.

Para ello, se creó un marco teórico que puede ser representado a través del diagrama de flujo que se puede visualizar a continuación:

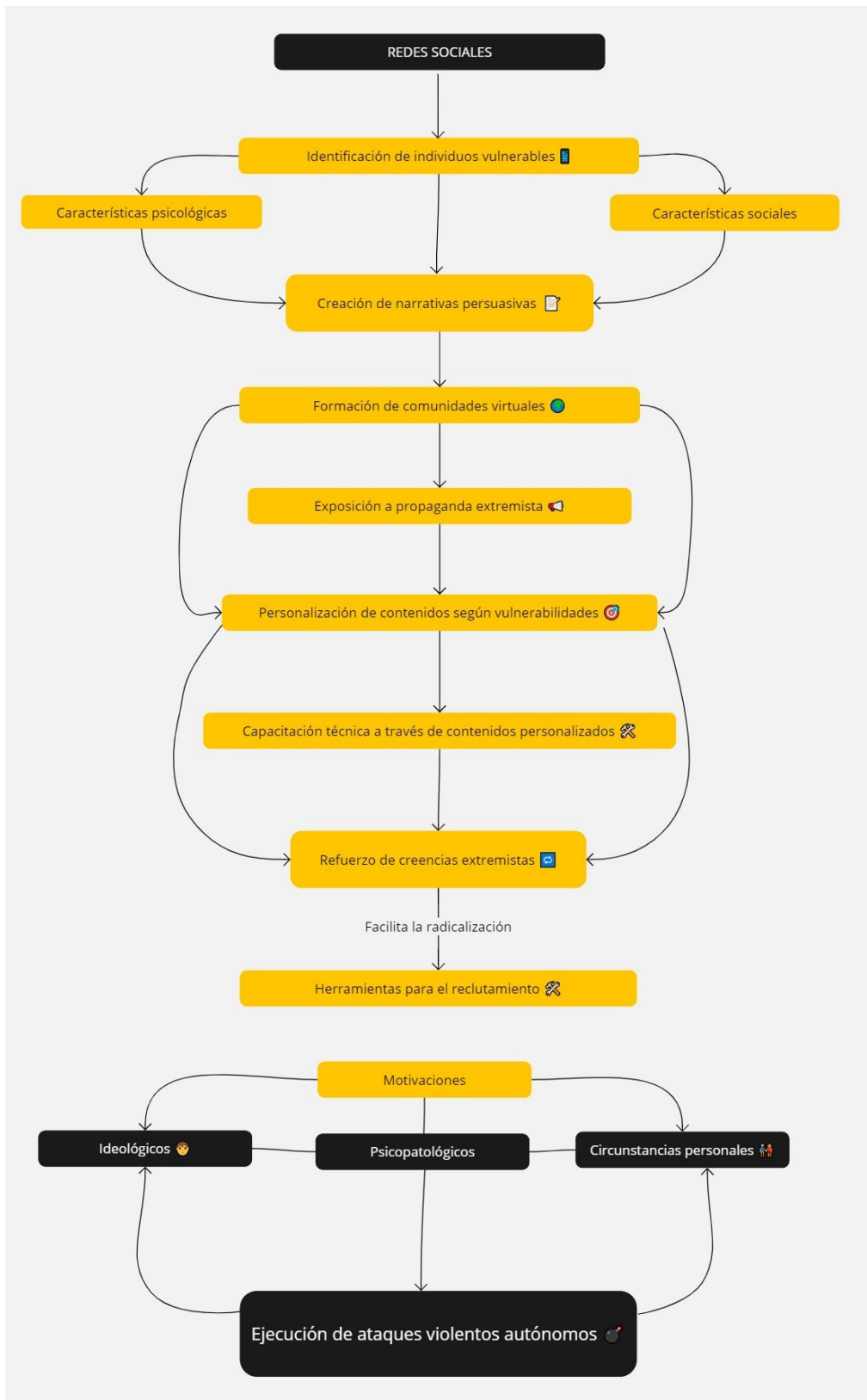


Figura 1: Diagrama de elaboración propia

### Operacionalización de las variables y validación

Se analizará cómo el Estado Islámico interactúa con los usuarios a través de los posts, comentarios, mensajes privados y otras formas de comunicación en el marco de las redes sociales. Para los fines de este trabajo, se tratará de analizar las siguientes variables:

- Plataformas de redes sociales. Definición operacional: Se considerarán como plataformas de redes sociales aquellas herramientas digitales que permiten la creación de perfiles de usuario, la interacción social y la difusión de contenido en línea.

Según los autores analizados hasta el momento y expuestos en el Estado del arte, en el caso del Estado Islámico se utilizaron las siguientes: Twitter/X, Facebook, Telegram, Instagram, Youtube, etc.)

Se verá cuáles fueron los medios digitales utilizados por ISIS para difundir su mensaje y reclutar seguidores.

#### *Indicadores:*

- Identificación de las plataformas más utilizadas: ¿Qué plataformas de redes sociales fueron utilizadas principalmente por ISIS para el reclutamiento? A través del análisis de investigaciones previas, y monitoreo de dichas plataformas, se identificarán las plataformas más utilizadas por el Estado Islámico para difundir su mensaje y reclutar seguidores.
- Análisis de la evolución en el tiempo: Se evaluará cómo el uso de estas

plataformas ha evolucionado a lo largo del tiempo, identificando posibles cambios en las estrategias de comunicación del grupo.

- Contenidos difundidos. Definición operacional: Se entenderá como contenido difundido cualquier material publicado en las plataformas de redes sociales, incluyendo textos, imágenes, videos, audios y otros formatos multimedia.

*Indicadores:*

- Clasificación del contenido: Se clasificará el contenido según su tipo (propaganda, testimonios, llamados a la acción, etc.) y su formato (texto, imagen, video). ¿Qué tipo de contenido se difunde? (videos, imágenes, textos, memes, etc.)
- Uso de hashtags y etiquetas: Se estudiará el uso de hashtags y etiquetas para categorizar el contenido y facilitar su difusión.
- Análisis del lenguaje y tono: ¿Cuál es el tono y el lenguaje utilizado, y el mensaje transmitido en las publicaciones de ISIS en redes sociales? Se analizará el lenguaje utilizado, el tono de los mensajes (amenazas, promesas, apelaciones emocionales), y la retórica empleada para persuadir a los seguidores.
- Identificación de temas recurrentes: Se identificarán los temas principales abordados en el contenido, como la yihad, la opresión, la promesa de un paraíso, etc.
- Análisis de la evolución de los mensajes: Se evaluará cómo los mensajes

han evolucionado a lo largo del tiempo, adaptándose a las nuevas circunstancias y a las audiencias.

Se analizarán publicaciones o posteos en las redes, especialmente tweets, pero durante la investigación se han observado memes, videos, testimonios, entre otros contenidos que muestren cómo el grupo terrorista comparte propaganda, testimonios de combatientes, casos exitosos de reclutamiento, entre otros.

- Mensajes transmitidos. Definición operacional: Se considerarán los mensajes transmitidos como las ideas principales y los objetivos que el Estado Islámico busca comunicar a través de su contenido en las redes sociales.

*Indicadores:*

- Identificación de los objetivos: Se identificarán los objetivos principales de la comunicación del Estado Islámico, como la legitimación de la violencia, la difusión de la ideología y la incitación al odio, así como también el posible reclutamiento de nuevos miembros.
- Identificación de los grupos objetivo: Se identificarán los grupos a los que se dirigen los mensajes (jóvenes, descontentos, etc.).

| Variable    | Definición Operacional                         | Indicadores                                                                      |
|-------------|------------------------------------------------|----------------------------------------------------------------------------------|
| Plataformas | Herramientas digitales para interacción social | Twitter, Facebook, Telegram, etc.                                                |
| Contenido   | Material publicado en las plataformas          | Textos, imágenes, videos, etc.                                                   |
| Mensajes    | Ideas principales transmitidas                 | Legitimación de la violencia, difusión de ideología, posible reclutamiento, etc. |

Figura 2: Tabla de elaboración propia

### Selección del universo de casos

El caso que se toma para analizar el uso de las TICs, particularmente las redes sociales, para radicalizar y reclutar individuos, especialmente a los "lobos solitarios" desde 2014 hasta 2017, es el caso de Estados Unidos. Este estudio se centra en el caso de Estados Unidos durante este período, debido a su importancia como objetivo principal de ISIS o como gran representante de Occidente.

Este periodo en particular es elegido dado que coincide con el auge del Estado Islámico y su intensa actividad propagandística en redes sociales, tanto que se produjeron varios ataques terroristas inspirados en ISIS en Estados Unidos y otros países occidentales, lo que evidencia la efectividad de sus tácticas de radicalización y posterior reclutamiento en línea. Esto hizo que durante ese período se convirtiera al tema en uno de interés internacional, generando una mayor atención académica y mediática sobre el fenómeno, especialmente para Estados Unidos, quien lleva años luchando contra el terrorismo global.

La evolución de las estrategias de difusión del Estado Islámico en redes sociales ha sido notable. Inicialmente, el grupo se concentró en foros en árabe, protegidos con contraseña ofreciendo un espacio seguro para la radicalización. A pesar de que estos foros siguen existiendo, en nuestro trabajo no serán incluidos, primeramente porque no podríamos tener acceso a ellos y luego porque no se cuenta con una comprensión del idioma árabe, por lo que se relevaron únicamente datos en inglés.

La relevancia del caso de Estados Unidos se puede ver a continuación con las siguientes cifras. La designación del ISIS como organización terrorista por parte de Estados Unidos criminalizó cualquier forma de apoyo a este grupo. En 2016, el FBI reportó

más de 90 casos de estadounidenses involucrados con ISIS, muchos de los cuales planeaban ataques o buscaban unirse al grupo. Estos individuos, de diversos orígenes pero predominantemente jóvenes y hombres, se radicalizaron en gran medida a través de las redes sociales. Algunas de estas personas fueron acusadas de planear atentados en Estados Unidos en nombre de ISIS. Otros fueron acusados de prestar apoyo y asistencia a la organización (Lichtblau, 2016).

McElreath et al retoman a Green (2017) para dejar representadas ciertas estadísticas con relación al caso norteamericano. Algunos de estos individuos reportados por el FBI intentaron viajar, o facilitar el viaje de otros, con el objetivo de unirse a ISIS, mientras que otros proporcionaron dinero o equipamiento a miembros del grupo terrorista. Como señala Green, su edad media era de 25 años, aproximadamente el 75% eran ciudadanos estadounidenses y el 90% eran hombres. Al menos el 33% se había convertido al islam, y aproximadamente el 25% eran personas de ascendencia árabe. A pesar de las diferencias demográficas, la mayoría tenían algo en común: alrededor del 90% de los incidentes estaban relacionados con las redes sociales, a menudo con conversaciones en línea con supuestos reclutadores, ya fueran encubiertos o reales (McElreath et al., 2018).

#### Selección del método de observación

En cuanto a la metodología, este trabajo presenta un carácter cualitativo. A continuación se presentan las diferentes técnicas de recolección de datos utilizadas:

- Trabajo de fuentes primarias: Contenidos producidos directamente por el Estado Islámico: Análisis de contenido de Tweets
- Recuperación de fuentes primarias a través de fuentes secundarias:

- Análisis de material e información digital: análisis de notas de prensa relacionadas a la temática a estudiar, de artículos e investigaciones donde se hayan recuperado fuentes primarias valiosas para la investigación, así como información digital obtenida de portales informativos.
- Análisis de discurso junto con entrevistas hechas por académicos.

Para los fines de esta investigación entonces se realizará un análisis cualitativo del contenido de las fuentes, trabajándolo por categorías, identificando palabras clave, temáticas recurrentes y similitudes en las narrativas utilizadas dentro de las redes sociales por parte del grupo terrorista dentro del período estudiado.

Esta categorización se hará de acuerdo a:

Temática: Propaganda, reclutamiento, justificación de la violencia, vida en el califato, etc.

Simbología/Visuales: Uso de imágenes, videos, símbolos, etc.

Tono: Amenazante, persuasivo, emocional, motivacional, etc.

Lenguaje: Uso de términos religiosos, referencias históricas, apelaciones a la identidad, etc.

A través de un análisis temporal se podrá comparar cómo las narrativas y el contenido de los mensajes se fue modificando para amoldarse al público objetivo. Como se menciona anteriormente se prestará atención al uso de recursos y símbolos, así como de terminología similar e imágenes adoptadas para poder identificar y establecer patrones en la forma de comunicación ISIS.

## ***1.6. Estructura de la tesis***

Esta tesis está organizada en cinco capítulos luego de la introducción (Capítulo 1), estructurados de manera lógica para abordar la problemática planteada y responder a la hipótesis central. El capítulo 2 desarrolla el marco teórico y conceptual, introduciendo los principales elementos necesarios para comprender el fenómeno investigado, como la evolución del terrorismo, los procesos de radicalización en entornos digitales y los desafíos que enfrenta la seguridad internacional en la era de las tecnologías de la información y la comunicación (TICs). El capítulo siguiente se enfoca específicamente en el uso de las TICs por parte del Estado Islámico (ISIS), examinando cómo esta organización ha empleado redes sociales y otras herramientas digitales para la difusión de propaganda, el reclutamiento de nuevos miembros y la radicalización de individuos, a través de estrategias cuidadosamente diseñadas en diversas plataformas. Durante el capítulo 4 se analizan las formas de radicalización individual vinculadas a la narrativa digital de ISIS, prestando especial atención a los “lobos solitarios”, motivados por el discurso extremista. En este capítulo se incluyen ejemplos empíricos que muestran el impacto concreto de estas dinámicas en la seguridad global. El capítulo 5 presenta los hallazgos más relevantes de esta investigación y propone recomendaciones orientadas a la elaboración de estrategias más eficaces para prevenir y contrarrestar la radicalización en el entorno digital. Finalmente, el último capítulo explora los principales desafíos que estas nuevas formas de radicalización representan para las políticas tradicionales de seguridad, evaluando tanto sus limitaciones como las respuestas emergentes.

## CAPÍTULO 2: FUNDAMENTOS TEÓRICOS Y CONCEPTUALES

### *2.1. Definición y evolución del terrorismo*

#### *Qué se entiende por terrorismo*

La falta de una definición universalmente aceptada del terrorismo ha generado controversia en torno a su conceptualización, pues el término es frecuentemente utilizado con fines políticos y estratégicos. Como señala Boaz Ganor (2002), “el terrorismo es, ante todo, un problema de definición; sin un consenso claro sobre su significado, resulta difícil desarrollar estrategias efectivas para combatirlo”.

Hay numerosas definiciones para hacer referencia al fenómeno del terrorismo, pero en este trabajo entendemos por terrorismo al fenómeno a través del cual ciertos individuos cometen actos de violencia con el fin de infundir miedo o terror a otro grupo, dirigido hacia civiles no armados y realizado por un cálculo estratégico y propósito político empleado tanto por actores estatales como no estatales y en tiempos de guerra y de paz. (Jackson, 2007)

Jackson (2008) enfatiza la dimensión discursiva del terrorismo, argumentando que la manera en que se define el término responde a intereses políticos y que la etiqueta de “terrorista” suele ser utilizada estratégicamente por los Estados para justificar ciertas acciones militares o políticas represivas. Argumenta que el terrorismo no es sólo un acto de violencia, sino también una construcción social discursiva utilizada para justificar ciertas acciones políticas reflejando narrativas de poder y conflicto.

McElreath et al, sugieren que ya no es sólo el terrorismo doméstico o ciudadanos extremistas quienes ponen en peligro a las sociedades en general, ahora también el

terrorismo internacional supone amenaza, especialmente inspirando un ataque a nivel interno a través de la radicalización de un ciudadano o residente (McElreath et al., 2018).

Dado que el terrorismo se manifiesta de distintas maneras, es necesario diferenciar entre el terrorismo perpetrado por actores no estatales y el terrorismo de Estado.

El terrorismo de Estado se refiere al uso sistemático de la violencia por parte de un gobierno para intimidar, reprimir o eliminar a sectores de la población considerados una amenaza para su autoridad. A diferencia del terrorismo tradicional, que suele ser llevado a cabo por actores no estatales, en el terrorismo de Estado los perpetradores son agencias gubernamentales, fuerzas de seguridad o grupos paramilitares con apoyo estatal, e implica el uso sistemático del terror por parte de gobiernos contra su propia población o contra otros Estados.

Según Noam Chomsky (2002), “el terrorismo de Estado es con frecuencia el más destructivo y, sin embargo, el menos reconocido, debido a que quienes lo practican también controlan las narrativas internacionales sobre el terrorismo”.

Las principales características del terrorismo de Estado incluyen:

- Violencia dirigida contra la propia población junto con represión sistemática de opositores políticos, minorías étnicas o grupos sociales considerados subversivos.
- Uso de la intimidación y el miedo como estrategia de control. Esto incluye desapariciones forzadas, torturas, ejecuciones extrajudiciales y censura.
- Legitimación a través del aparato estatal: La violencia es justificada mediante

leyes, decretos o discursos oficiales que presentan a las víctimas como una amenaza para la estabilidad del país.

- Uso de agentes estatales y organizaciones clandestinas para ejecutar actos de violencia con impunidad.

En la mayoría de los casos de terrorismo de Estado como la Alemania Nazi (1933-1945), las dictaduras militares en América Latina entre 1970 y 1980 como así también el *apartheid* en Sudáfrica en el siglo XX, se refleja cómo el terrorismo de Estado ha sido utilizado para consolidar el poder político, eliminar la disidencia y perpetuar regímenes autoritarios.

Este tipo de terrorismo plantea un desafío fundamental para la seguridad internacional, ya que muchos Estados que combaten el terrorismo convencional han sido responsables de prácticas terroristas contra su propia población. Por ejemplo, en la Guerra contra el Terrorismo posterior al 11 de septiembre de 2001, Estados Unidos ha sido acusado de aplicar tácticas de terrorismo, como la tortura en Guantánamo y las ejecuciones extrajudiciales con drones en el Medio Oriente (Jackson, 2018).

Con el auge de grupos como Al-Qaeda en los años 90, el terrorismo dejó de estar vinculado a luchas nacionales y se convirtió en un fenómeno transnacional, con ataques de gran impacto como el 11 de septiembre de 2001 en Estados Unidos. Richard Barret (2017) señala que "el terrorismo contemporáneo ha evolucionado de organizaciones jerárquicas a redes descentralizadas que operan a escala global". (Barrett, 2017).

Este cambio estructural ha estado impulsado por dos factores clave como la globalización

y el acceso a nuevas tecnologías de comunicación, que han permitido la coordinación de ataques sin necesidad de una base territorial, así como la ideología del extremismo religioso, que ha sido instrumentalizada por grupos como Al-Qaeda e ISIS para movilizar seguidores en distintas partes del mundo.

El terrorismo ha evolucionado desde una táctica empleada por movimientos políticos locales hasta una amenaza transnacional con impacto global. A medida que las estrategias terroristas han cambiado, también lo han hecho los enfoques de seguridad internacional, que deben adaptarse a nuevos desafíos como la radicalización digital y el ciberterrorismo.

En este contexto, los debates sobre la definición del terrorismo siguen abiertos, ya que el término sigue siendo utilizado con fines políticos y estratégicos. Sin embargo, la tendencia actual apunta a un modelo descentralizado, donde el uso de las TICs ha facilitado la propagación del extremismo y ha generado nuevos desafíos para la seguridad global.

### ***1.2 El caso del Estado Islámico (ISIS)***

Hasta 2016, ISIS demostró no solo una violencia extrema, sino una capacidad de resistencia que sorprendió a muchos observadores internacionales. A pesar de su tamaño relativamente pequeño, propagó la ideología extremista a escala mundial a través de las redes sociales con eficacia y éxito. (Hoffman, 2017).

Para comprender el fenómeno del Estado Islámico, nos remontaremos a sus inicios. Para ello, el siguiente estudio hace referencia al texto de Springli y Curvale (2021)

Al Qaeda, fundada a fines de la década de 1980 en el contexto de la resistencia afgana

contra la invasión soviética, se convirtió en un movimiento yihadista global que buscaba establecer un califato islámico. Su ideología, basada en el salafismo yihadista, justificaba el uso de la violencia para alcanzar sus objetivos. En un primer período, marcado por la formación de Al Qaeda y los atentados del 11-S, el movimiento consolidó su presencia en el escenario internacional. Posteriormente, con la muerte de Osama bin Laden y la Primavera Árabe, el yihadismo experimentó una fase de descentralización y diversificación.

El Estado Islámico (EI), también conocido como ISIS (Estado Islámico de Irak y Siria) o ISIL (Estado Islámico de Irak y el Levante), tiene sus orígenes en la insurgencia iraquí tras la invasión estadounidense en 2003. El grupo precursor de ISIS, Jama'at al-Tawhid wal-Jihad, fue fundado en 1999 por el militante jordano Abu Musab al-Zarqawi. En 2004, al-Zarqawi juró lealtad a Al-Qaeda y renombró su grupo como Al-Qaeda en Irak (AQI).

Tras la muerte de al-Zarqawi en 2006, AQI se fusionó con otros grupos insurgentes para formar el Estado Islámico de Irak (ISI). La organización sufrió importantes derrotas entre 2007 y 2011 debido a la surge estadounidense y a la cooperación de tribus suníes en su contra. Sin embargo, el grupo aprovechó la retirada de las tropas estadounidenses en 2011 y la inestabilidad política en Irak y Siria.

Fue en 2013, bajo el liderazgo de Abu Bakr al-Baghdadi, que ISI se extendió a Siria y se autodenominó Estado Islámico de Irak y el Levante (ISIL o ISIS). El 29 de junio de 2014, al-Baghdadi proclamó la creación de un califato, el Estado Islámico, y se declaró califa, gobernando sobre los territorios capturados en Irak y Siria. Esta proclamación marcó un punto crucial en la historia del grupo, atrayendo a militantes

de todo el mundo y llevando a una intervención militar internacional en su contra.  
(Springli y Curvale, 2021).

### ***2.3. Radicalización y terrorismo digital***

#### ***El proceso de radicalización***

Hay una gran cantidad de literatura que al analizar el fenómeno del terrorismo comparten la idea que detrás de los individuos que integran dicha organización, se da un proceso de radicalización tanto de la religión como de su propia persona.

McElreath et al hacen un repaso por distintos autores para intentar describir a qué se entiende por radicalización (McElreath, 2018):

La literatura especializada en radicalización revela un panorama complejo y multifacético. Autores como Coolseat (2011), Hudson, Loza y Windsor (2018), y McElreath et al. (2018) han destacado la ausencia de un consenso unívoco en torno a las causas subyacentes a este fenómeno. La radicalización para estos autores, emerge como resultado de la intersección de múltiples factores sociales, económicos, políticos, psicológicos y religiosos, que se entrelazan de manera dinámica y compleja. Ekici (2009), así como también Moghaddam (2005) y Sageman (2008), subraya el papel fundamental de las necesidades psicosociales, como la identidad, la pertenencia y la afiliación, la desigualdad, la injusticia y la exclusión social en la predisposición a la radicalización, mientras que autores como Midhio, Ismadi y Waluyo (2017) enfatizan el papel central de la ideología y la violencia en la configuración de trayectorias radicales. Kruglanski et al. (2014) proponen un modelo acumulativo que subraya la importancia de la motivación, la ideología y el contexto social en la génesis

y desarrollo de la radicalización. (McElreath, 2018)

## ***2.4. Lobos solitarios: características y perfil psicológico***

### *Concepto y perfil de los lobos solitarios*

A lo largo de los años se ha escrito mucha bibliografía sobre qué quiere decir el término “lobo solitario”.

Hay ciertos autores que consideran que este término es errado ya que no se puede decir que sean solitarios dado que el individuo es influenciado por su entorno. Los "lobos solitarios" pueden inspirarse en una determinada organización terrorista y verse a sí mismos como sus servidores, aunque nunca hayan sido reclutados formalmente ni hayan recibido formación, o ayuda de ningún tipo de dicha organización. Buscan reivindicar su autoría en los atentados que cometen dado que aspiran a ser reconocidos por ello y por la organización terrorista.

Retomaremos el texto de Ganor (2021), “Understanding the motivations of Lone Wolf terrorists” para recopilar distintas definiciones del término “lobo solitario” hasta llegar a la elegida para este trabajo.

Según Gartenstein-Ross y Barr (2021), los "verdaderos" lobos solitarios son personas que cometen ataques terroristas sin haber tenido nunca contacto de ningún tipo (online o en persona) con grupos extremistas yihadistas, por lo que el término lobos solitarios es errado para hacer referencia a la mayoría de los individuos radicalizados que cometen ataques. Otro autor que retoma Ganor es Daniel Byman quien señaló que la mayoría de las veces no se puede determinar qué tan solo y aislado el lobo solitario se encuentra. Al igual que Gabriel Weimann quien sugiere que "los terroristas 'lobos

solitarios' no están completamente fuera de contacto", ya que se comunican a través de la "Dark Web", Byman cree que forman o crean pequeñas “manadas virtuales”. Dentro de estos espacios, se encuentran y se les ofrecen una gran cantidad de recursos para aprender y llegar a ejecutar ataques. (Ganor, 2021)

Para los propósitos de Ganor, el autor define al fenómeno de los lobos solitarios como uno en el que “un terrorista individual perpetra un atentado por su cuenta o con la ayuda o participación de otras personas, pero sin ninguna conexión operativa con ninguna organización terrorista específica. Señala que por más de que el terrorista haya estado en contacto con otros (en línea o en persona) y se haya inspirado en una organización terrorista específica, o incluso si se veía a sí mismo como un adherente/operativo de la misma, mientras que ninguna organización terrorista haya actuado/ participado en ninguna de las fases del atentado (inicio, planificación, preparación, financiación o logística del atentado), se considerará un atentado de "lobo solitario". (Ganor, 2021, pág.4)

Ganor y Merari proponen una tipología de motivaciones que subyacen a las acciones de los 'lobos solitarios', dividiéndolas en tres categorías principales: ideológicas, psicopatológicas y relacionadas con circunstancias personales.

Dentro de la categoría ideológica, los autores identifican una amplia gama de motivaciones, que incluyen el nacionalismo, el fascismo, el comunismo, el anarquismo y otras ideologías menos comunes. En cuanto a las motivaciones psicopatológicas, destacan factores como el sentimiento suicida, problemas de salud mental, experiencias traumáticas, crisis personales, creencias relacionadas con la vida después de la muerte, entre otros. Finalmente, la categoría de circunstancias

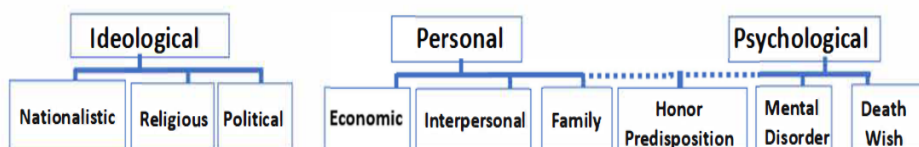
personales abarca una variedad de factores, como motivos económicos, religiosos, crisis interpersonales, problemas familiares, búsqueda de reconocimiento social y el deseo de aventura.

Para el autor, los motivos anteriores o una combinación de estos puede llevar a un "lobo solitario" a perpetrar un atentado, y diferirá para cada persona. El peso de cada motivo varía en función de cada caso y de las circunstancias personales del terrorista, así como su estructura mental, su exposición a la incitación, etcétera. (Ganor, 2021, pág 5 y 6)

En su texto, el autor presenta dos modelos para poder comprender las motivaciones de los lobos solitarios que serán presentados a continuación.

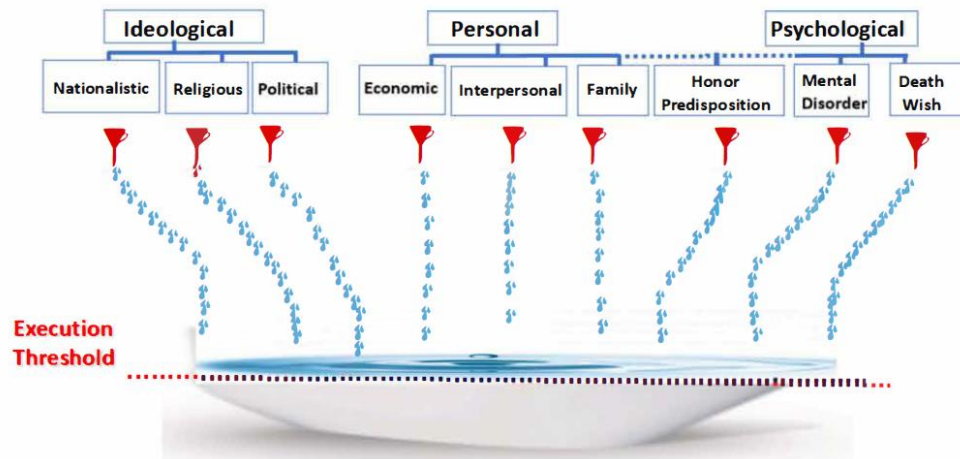
Para visualizar la toma de decisiones de los lobos solitarios nos dice que imaginemos el ataque como un recipiente (una bañera) que se va llenando con los diversos grupos y subgrupos de motivaciones antes mencionados. A este se referirá como "bathtub model o "modelo de la bañera". Estos motivos van llenando la "bañera de motivación", y es recién cuando la bañera está llena, que se desborda y se produce un ataque. Este desbordamiento refleja la maduración de la decisión terrorista de atentar. (Ganor, 2021, pág 6).

Figure 1: "The Bathtub" Model - Typology of "Lone Wolf" Motives



**Figura 3<sup>2</sup>**

**Figure 2: The “Bathtub Model” – “Lone Wolf” Attack Execution Threshold**



**Figura 4<sup>3</sup>**

El autor nos dice que el umbral de ejecución es el límite máximo en el cual el lobo solitario pudo contenerse. Este modelo es único a cada persona y dinámico dado que puede ir cambiando dependiendo su ambiente, contexto, exposición a las distintas motivaciones y resiliencia del atacante. (Ganir, 2021, pág 7).

Habiendo definido los principales conceptos, vamos a pasar a las herramientas utilizadas por ISIS para llevar a cabo su radicalización virtual y potencial reclutamiento.

## **2.5. La seguridad internacional en la era digital**

La seguridad internacional ha experimentado una transformación significativa con el avance de las tecnologías de la información y la comunicación (TICs). La

<sup>2</sup> Ganor, Op. cit, 6.

<sup>3</sup> Ganor, Op. cit, 6.

digitalización ha expandido el panorama de riesgos y ha permitido la emergencia de nuevas amenazas transnacionales. En este contexto, el uso de redes sociales y otras plataformas digitales por parte de grupos como el Estado Islámico ha demostrado cómo el terrorismo puede adaptarse a la era digital, empleando herramientas de comunicación para difundir ideologías extremistas, captar nuevos reclutas y planificar ataques de manera descentralizada.

La facilidad con la que ISIS y otras organizaciones extremistas pueden difundir su mensaje a nivel global a través de plataformas digitales ha permitido la creación de redes descentralizadas de simpatizantes y combatientes. El anonimato y la accesibilidad de internet han hecho que la radicalización sea más difícil de detectar y combatir. Las plataformas de redes sociales, como Twitter, Telegram y YouTube, han sido utilizadas para difundir propaganda, compartir manuales sobre la planificación de atentados y facilitar la comunicación entre extremistas. Esto ha generado una complejidad adicional para los organismos de seguridad, que deben rastrear y neutralizar amenazas en un entorno digital dinámico y en constante evolución.

Estos ataques desafían las nociones tradicionales de guerra y seguridad, ya que pueden ser perpetrados de manera remota, con costos reducidos y sin necesidad de intervención física en el territorio del enemigo, paralizando servicios esenciales y generando caos económico y social.

Otra amenaza emergente es el uso estratégico de la desinformación como arma de manipulación política y social. Grupos extremistas y actores estatales han empleado tácticas de guerra híbrida mediante la difusión de noticias falsas, campañas de desinformación y manipulación de redes sociales para polarizar sociedades y debilitar

la estabilidad de los Estados. Ejemplos de esta estrategia incluyen campañas de desinformación dirigidas a influir en procesos electorales, fomentar divisiones internas en sociedades democráticas o desacreditar gobiernos e instituciones internacionales. El caso del Estado Islámico es paradigmático en este sentido, ya que ha utilizado videos y publicaciones en redes sociales para reclutar combatientes y justificar sus acciones ante una audiencia global.

Frente a estas amenazas, los Estados han desarrollado estrategias de ciberseguridad y cooperación internacional para combatir el terrorismo digital. Organizaciones como la ONU, la OTAN, han promovido iniciativas para rastrear y dismantelar redes terroristas en el entorno digital, así como para prevenir el financiamiento del terrorismo a través de criptomonedas y otras plataformas financieras.

Sin embargo, la lucha contra el terrorismo en internet plantea desafíos significativos en términos de soberanía, privacidad y derechos digitales. Las políticas de vigilancia masiva y la regulación de contenidos en redes sociales han generado debates sobre los límites entre la seguridad nacional y la libertad de expresión, lo que dificulta la implementación de medidas efectivas sin afectar derechos fundamentales.

Las grandes plataformas digitales han sido criticadas por la proliferación de contenido extremista en sus plataformas. Aunque han implementado medidas de moderación y eliminación de cuentas vinculadas a grupos terroristas, estos esfuerzos a menudo son insuficientes debido a la rapidez con la que los extremistas adaptan sus estrategias y crean nuevas cuentas para seguir difundiendo propaganda. La falta de un marco regulatorio internacional uniforme dificulta una respuesta coordinada y eficaz frente al terrorismo digital.

## **CAPÍTULO 3: EL USO DE LAS TICs POR PARTE DE ISIS**

### ***3.1. Contexto y surgimiento de ISIS en el ámbito digital: el salto a la estrategia digital***

Mientras que Al-Qaeda utilizó páginas web y foros cerrados en la década de 2000, ISIS llevó la propaganda terrorista a una nueva dimensión al emplear redes sociales y plataformas interactivas (Barrett, 2017). Según Winter (2017), ISIS entendió el potencial de las redes sociales como una herramienta de guerra psicológica y expansión global.

A partir de 2014, con la proclamación del califato en Mosul, ISIS inició una campaña digital agresiva para: legitimarse como un Estado funcional con estructura política, militar y social, difundir su ideología extremista, atraer seguidores y desmoralizar a sus enemigos mediante la difusión de ejecuciones y actos de violencia extrema.

Durante este período, ISIS no solo utilizó redes sociales abiertas como Twitter y Facebook, sino que también desarrolló foros internos, aplicaciones móviles y revistas digitales para consolidar su mensaje.

Según Oppermann (2019), "la narrativa digital de ISIS fue clave para su expansión, ya que permitió la construcción de una identidad global que trasciende las barreras geográficas y lingüísticas".

### ***3.2. Estrategias de comunicación y propaganda en redes sociales***

*Internet como método de radicalización: ¿Por qué esta modalidad importa?*

La estrategia del Estado Islámico fue la de distribuir una ideología fundamentalista medieval, utilizando instrumentos de la era moderna, como lo son el Internet y las

redes sociales, para su difusión. La planificación de esta estrategia ha servido, en su momento, para potenciar el poderío militar de ISIS, y actualmente se constituye como una de las pocas herramientas disponibles para seguir fundamentándose políticamente frente a los extremistas.

La comunicación de ISIS se basó en una estrategia multimodal que combinaba narrativas emocionales, violencia simbólica y mensajes dirigidos a diferentes audiencias. Según Ingram (2018), la propaganda de ISIS se estructuró en varios niveles:

- Mensajes de atracción: en el cual se glorifica el califato como un destino ideal.
- Mensajes de identidad o pertenencia: ISIS como el único representante legítimo del Islam, diferenciándose de otros grupos y Estados musulmanes.
- Mensajes de confrontación: Justificación de la violencia contra los "enemigos del Islam" y deshumanización de sus adversarios en todos los niveles.

Su objetivo ya no se centra en llevar a cabo grandes ataques por sus propios medios, como sí lo hicieron anteriormente en Europa o Medio Oriente, sino inspirar acciones que terminan siendo ejecutadas por "lobos solitarios".

Este fenómeno de lobos solitarios tiene larga data, en los cuales terroristas individuales perpetúan ataques sin la orden ni la guía, soporte o financiación de las organizaciones terroristas. La habilidad de las organizaciones radica en ser parte de la “comunidad” virtual, esparcir su propaganda y mensajes e inspirar a los lobos solitarios a realizar estos ataques terroristas. (Ganor, 2021). Dichos ataques a su vez suelen ser realizados y difundidos donde hay audiencias masivas. No se realizan en aislamiento. Los lobos solitarios no quieren permanecer en el anonimato sino ser reconocidos por dicho

ataque. Aquí se puede ver el sentimiento de martirismo que se expresa en la frase que abre la sección de la introducción.

### *El rol de las redes sociales*

Como vimos, el auge de las redes sociales ha creado el caldo de cultivo perfecto para la radicalización digital.

Sageman (2008) introduce el concepto de redes sociales como un elemento clave en la movilización de individuos radicalizados, destacando además la importancia de sentimientos como la indignación moral y la empatía.

Las redes sociales tales como Facebook, Twitter, Instagram, Telegram, así como los chats dentro de videojuegos, los foros o blogs, los comentarios en la plataforma Youtube, entre otros, les otorgan grandes ventajas a los grupos terroristas dado que pueden lograr:

- a) Publicar mensajes sin revisión ni censura.
- b) Reducir el tiempo de transmisión de la información, transmitiendo cantidades masivas de información en fracciones de segundo.
- c) Minimizar el costo económico de la comunicación.
- d) Extender la información a una amplia mayoría de la población del planeta, ampliando su dimensión y alcance.
- e) Comunicación directa y sin intermediarios con su “público” potencial.
- f) Menor control gubernamental.

Aquí podemos ver el concepto de “aldea global” de McLuhan en la cual se difuminan las fronteras y las barreras geográficas. Aquí, las personas pueden llegar a adoptar una idea de pertenencia a una comunidad global a través de las posibilidades de interconexión que internet y estas redes sociales les proveen. (McLuhan, Powers, 1996)

Por todas estas ventajas, las redes sociales se convirtieron en el medio más eficiente para que los grupos terroristas expandieran sus mensajes ya que contaba con una organización descentralizada, un ambiente multicultural, y una escala antes no vista.

Tomando a Lind, el uso de las redes sociales opera como una plataforma de operaciones psicológicas. Para el autor, “las operaciones psicológicas llegarán a ser el arma dominante en la forma de intervención en los medios de comunicación y a través de las TIC...los adversarios de la cuarta generación de guerra manipularán los medios para alterar la opinión pública mundial y local para doblegar la voluntad de lucha” (Lind, 1989: 22-26)

Internet posibilita la cohesión global de extremistas que se encuentran por todo el mundo. Retomando a Thevessen del texto de Cano Paños, la llamada “umma virtual” que representa Internet permite a muchos sujetos que se sienten aislados en la sociedad en la que desarrollan sus vidas percibir una sensación de pertenencia a una comunidad de sujetos unidos por una ideología común. En el caso de los jóvenes desilusionados y alienados que habitan en Occidente, esta identificación con una umma de carácter supranacional puede conducir a la larga a un proceso de radicalización política. En este sentido, está fuera de toda duda que sin Internet hubiera resultado imposible conseguir lo que se ha denominado “globalización del terrorismo islamista”. (Cano

Paños, 2008, pág. 76).

Durante su estudio de las redes sociales en la operación estratégica yihadista, Klausen encontró que Twitter estaba siendo utilizado por miembros del Estado Islámico para crear la ilusión de que el grupo era más poderoso de lo que en verdad era. (Klausen, 2015). Acá se puede ver cómo toman este proceso como uno de activismo político.

En la última década, las redes sociales se han consolidado como un espacio privilegiado para la participación política y social de los jóvenes (Awan, 2006). Si bien estos entornos virtuales han sido asociados con la democratización del discurso y la construcción de conocimiento (Castells, 2009), Awan (2006) plantea que también pueden facilitar procesos de radicalización. La creciente familiaridad de las nuevas generaciones con los entornos digitales y la migración de sus prácticas sociales a estos espacios (juegos, redes sociales, etc.) generan nuevas dinámicas que requieren un análisis más detallado sobre los factores que inciden en la radicalización especialmente en línea. (McElreath et al, 2018)

Siguiendo con el texto de McElreath et al, retoman nuevamente a Awan (2006) quien argumenta que estos espacios virtuales, amplifican la retórica radical y predisponen a los individuos a aceptar ideas extremas. Twitter, por ejemplo, es utilizada para difundir propaganda y reclutar nuevos miembros. La capacidad de los usuarios de ocultar su identidad y la facilidad para crear nuevas cuentas dificultan la moderación del contenido y permiten que la radicalización se propague a gran escala. (McElreath et al, 2018) .

Como argumentan Amy Louise Watkin & Joe Whittaker (2017), con la pérdida de territorio ISIS ha demostrado una mayor dependencia hacia plataformas en línea y una

gran adaptabilidad con un salto hacia las plataformas encriptadas.

Thompson nos dice que los grupos terroristas al saber de la dependencia de Occidente en Internet, utilizan este espacio para manipular especialmente a la juventud, radicalizarlos y darles un propósito. (Thompson, 2011)

La tecnología se constituyó como una herramienta clave porque permite reducir el tiempo de transmisión de la información y minimizar el costo económico de la comunicación. A esto se le suma el anonimato de los usuarios de Internet y el casi nulo control por parte de los Estados.

Así, amplía la dimensión y el alcance propagandístico de los grupos terroristas, logrando una comunicación directa y sin intermediarios con su “público” potencial (González Torres, 2018). Y al mismo tiempo permite que el individuo desarrolle una idea de pertenencia a una comunidad global a través de las infinitas posibilidades de interconexión.

### ¿Cómo funciona?

La dependencia de Internet y las redes sociales como medio de reclutamiento y mensajería fue acompañando el desarrollo de ISIS desde 2014. Ya desde aquel año, sus victorias militares en el terreno comenzaron a favorecer su visualización frente a principalmente jóvenes en todo el mundo, contando con una estrategia de atracción de combatientes internacionales.

A partir de esto, ISIS comenzó a enviar mensajes a través de medios sociales digitales, tales como Facebook, Twitter e Instagram, con el objetivo de fomentar la instauración de un califato islámico, radicalizando aún más el conflicto (Cano Paños, 2008). Al

principio, esta estrategia se reducía a ciudadanos del Medio Oriente (Berger y Morgan, 2015); sin embargo, luego se extendió hacia Occidente también, exponenciando el uso de aún más plataformas de la web abierta (como Telegram), así como de la “dark web”, e incluyendo publicaciones en más idiomas, desde inglés principalmente, como español, alemán, francés, ruso, polaco, y chino mandarín.

El medio virtual se utiliza como difusor de la propaganda para legitimar las operaciones terroristas y para ganar apoyo o mostrar las debilidades de sus enemigos.

Específicamente, la metodología consiste en publicar mensajes ideológicos sobre los valores y los objetivos de la organización utilizando conceptos propios de Internet y referencias culturales atractivas para el público (como el uso de memes o el videojuego “Call of Duty”, por ejemplo). Así también, cuando se da un evento global importante, como el Mundial de fútbol, se pudo ver cómo utilizaban hashtags relativos al tema para ganar visibilidad.

El Estado Islámico contaba con una estrategia muy planificada, en tanto selecciona y adapta el tipo de contenido que mejor se ajusta a cada receptor ("narrowcasting"). Desde la selección de las fotos que tienen el potencial de generar un fuerte impacto, especialmente para crear terror entre sus enemigos y ganar la admiración de otros grupos radicales, como por ejemplo los videos de ejecuciones, entre otros. En este sentido, convirtieron a las redes sociales en una plataforma de operaciones psicológicas para manipular percepciones y persuadir a los usuarios a alinear sus sentimientos, y eventualmente sus opiniones, con los intereses de la organización (Cohen Almagor, 2017). Hay una evidente alienación cultural. (ver anexo figura C)

Detrás de esto hay una racionalidad clara en cuanto a su objetivo político, que se puede

visualizar no solamente en la producción de dichos videos, imágenes en alta calidad, con escenografía, producción, montaje. Es una estrategia o intento de hacer política en condiciones de fuerte asimetría de poder y utilizan la tecnología a su favor para competir con sus enemigos.

La avalancha de videos, llamadas a la acción y mensajes ideológicos no sólo posibilitan una presencia constante, inmediata, económica, e impune en el ciberespacio, sino también poder tener un contacto directo con individuos que se encuentran en partes muy lejanas del mundo.

Además, se constituyó como una estrategia alternativa más horizontal, sin jerarquías evidentes. La estrategia controlada por un brazo llamado “Ejército electrónico del Estado Islámico”, dedicado, por un lado, a la mensajería de las redes sociales y, por otro lado, al pirateo y la seguridad (Stern y Berger 2015, 173). Con este fin, en enero de 2014, ISIS anunció la creación del batallón Al-battar Media, un equipo basado en Twitter designado para impulsar la propaganda de ISIS y castigar a sus oponentes (Fernández, 2015).

Más precisamente, ISIS utilizó diversos formatos para captar la atención de su audiencia:

- Videos de alta producción: Material audiovisual de calidad cinematográfica, con gráficos avanzados y efectos especiales.
- Revistas digitales: Dabiq y Rumiyah, diseñadas para legitimar sus acciones y atraer combatientes extranjeros.
- Testimonios de combatientes: Historias de yihadistas occidentales que viajaron a Siria, mostrando una imagen de hermandad y propósito.

- Segmentación de la audiencia: La propaganda de ISIS se adaptó a distintos perfiles, desde combatientes potenciales hasta mujeres y jóvenes musulmanes en Occidente, presentando el califato como un lugar ideal para vivir y luchar.
- Memes y contenido viral: Uso de memes, hashtags y videos cortos para difundir su mensaje entre jóvenes en redes como Twitter y TikTok.

A su vez, ISIS combinó su estrategia de propaganda con el uso de terror psicológico, difundiendo ejecuciones en masa y amenazas dirigidas a gobiernos occidentales.

Según Weimann (2016), "el impacto de estas campañas radica en su capacidad de generar miedo y radicalizar a los espectadores, haciéndolos sentir parte de una causa más grande".

### ***3.3. Plataformas utilizadas y su impacto***

ISIS ha demostrado una gran capacidad de adaptación tecnológica, migrando constantemente entre plataformas para evitar la censura y mantener su alcance global.

Inicialmente, utilizó plataformas como Twitter y Facebook para difundir su mensaje.

Según Berger y Morgan (2015), en 2014 existían más de 46.000 cuentas activas de ISIS en Twitter, con un alcance masivo en cuestión de minutos.

YouTube también fue utilizado para alojar videos propagandísticos, aunque con el tiempo, las medidas de moderación limitaron su impacto, y fue cuando las plataformas abiertas comenzaron a eliminar contenido de ISIS, que el grupo migró a aplicaciones cifradas como Telegram, WhatsApp y Signal, que le permitieron compartir propaganda de forma privada y sobre todo proteger la identidad de sus miembros.

Además de las redes tradicionales, ISIS exploró el uso de plataformas descentralizadas, foros en la Dark Web y servicios como JustPaste.it, donde podía publicar contenido sin restricciones.

## **CAPÍTULO 4: RADICALIZACIÓN Y MOVILIZACIÓN DE LOBOS**

### **SOLITARIOS**

#### ***4.1. De la narrativa digital a la acción violenta: Factores de vulnerabilidad y atracción de los jóvenes***

ISIS construyó una identidad digital única, proyectándose como un Estado legítimo y poderoso a través de imágenes de victorias militares, ejecuciones de enemigos y promesas de un "paraíso islámico" para sus seguidores. Según Oppermann (2019), esta narrativa digital se basó en los siguientes elementos clave:

Una de las estrategias más efectivas de ISIS fue la captación de combatientes extranjeros a través de internet. Según Barrett (2017), entre 30.000 y 40.000 personas de más de 100 países viajaron a Siria e Irak para unirse a ISIS entre 2014 y 2017.

ISIS utilizó técnicas de marketing digital y manipulación psicológica para atraer jóvenes marginados y radicalizarlos en línea. Estos procesos incluían la interacción personalizada en redes sociales, la producción de revistas digitales: Publicaciones como Dabiq y Rumiya promovían la narrativa de ISIS y tal vez lo más importante para este estudio, la explotación de vulnerabilidades emocionales. En este caso, se identificaba a jóvenes con crisis de identidad, problemas familiares o descontento con sus sociedades para ofrecerles una causa por la cual luchar, quienes luego serían los llamados "lobos solitarios".

Según Oppermann (2019), esta táctica tenía ciertas ventajas para ISIS. La primera ventaja radicaba en el bajo costo que ya mencionamos anteriormente dado que no tenía la necesidad de coordinar operaciones. Esto a su vez significaba un menor riesgo para la

organización que no requería entrenar ni financiar a los atacantes. Por último, la responsabilidad se deslindaba dado que primero era más difícil detectar a los individuos radicalizados antes de que cometieran un ataque y luego conectarlos directamente con el grupo terrorista.

Casos como el atentado en Niza (2016) o el ataque en Manchester (2017) ejemplifican cómo la estrategia digital de ISIS ha logrado inspirar actos de violencia en Occidente sin necesidad de una estructura operativa tradicional.

#### ***4.2. Lobos solitarios radicalizados en redes***

##### *El caso de Twitter (2014-2017)*

Twitter fue la plataforma preferida por el Estado Islámico (ISIS) en sus primeras fases de expansión digital debido a su accesibilidad, la rapidez en la difusión de información y la facilidad para crear múltiples cuentas anónimas tras bloqueos o suspensiones.

ISIS utilizó Twitter de manera estratégica. Difundió miles de mensajes celebrando sus "victorias" militares y promoviendo la idea de que su califato era un Estado legítimo y próspero. Utilizaban imágenes de edificios gubernamentales, mercados y hospitales operando en las zonas bajo su control, junto con hashtags como #Dawla\_Islamiya (Estado Islámico) y #Khilafah (Califato).

##### *Tweet de un simpatizante de ISIS en 2014:*

***"La justicia verdadera solo existe en el Califato. Aquí los musulmanes viven en paz. #IslamicState #Khilafah"***<sup>4</sup>

Este tweet fue extraído del informe The ISIS Twitter Census: Defining and Describing the Population of ISIS Supporters on Twitter, de Berger y Morgan (2015). En este estudio, los autores identificaron más de 46,000 cuentas activas relacionadas con ISIS, muchas de las cuales promovían la imagen del califato como un "paraíso islámico, dirigidas a hablantes de inglés, francés y alemán, promoviendo la idea de un "deber religioso" de unirse al califato.

Gran parte de su estrategia de atracción era mostrar al Estado Islámico como una "alternativa ideal" a Occidente.

*Tweet de una reclutadora de ISIS en 2015:*

***"Hermanos y hermanas, el Califato necesita doctores, ingenieros y soldados. Ven y sé parte de la historia. #HijrahToISIS"***<sup>5</sup>

Así como ISIS fomentaba su califato, exaltando su modo de vida, también utilizó Twitter para difundir videos de decapitaciones y ejecuciones públicas, generando miedo y atrayendo la atención de medios internacionales.

*Tweet de una cuenta vinculada a ISIS en 2015 (suspendida posteriormente):*

***"Este es el destino de los cruzados y sus espías. Que Alá maldiga a los enemigos del***

---

<sup>4</sup> Berger, J. M., & Morgan, J. (2015). The ISIS Twitter Census: Defining and Describing the Population of ISIS Supporters on Twitter. The Brookings Institution.

<sup>5</sup> Ibíd. Este tweet fue rastreado a una joven británica conocida como Sally Jones, quien fue una de las principales reclutadoras occidentales para ISIS.

***Califato. #IslamicState"***<sup>6</sup> - Tweet acompañado de imágenes de rehenes antes de su ejecución.

La utilización de la religión como medio de adoctrinamiento constituye un componente crucial del modelo administrativo de ISIS. Estos fundamentan sus premisas en que los gobiernos de las naciones musulmanas de Medio Oriente son corruptos, irreligiosos y están profundamente influenciados por Estados Unidos y otras potencias occidentales. El Estado Islámico respalda su aplicación de la violencia y su involucramiento en la yihad, atribuyendo a Estados Unidos y a otras naciones occidentales de supuestamente desencadenar una guerra contra el Islam. La implementación de la violencia en estas entidades se presenta como imprescindible para proteger el islam.

En relación con el fomento del terror, uno de los casos que más resonó mundialmente fue el asesinato del periodista James Foley en 2014, donde ISIS publicó un video en Twitter titulado "Un mensaje a América", mostrando su decapitación. Lugo de dicho acontecimiento, Twitter debió bloquear miles de cuentas. (The New York Times, 2014).

A su vez, en el siguiente tweet de un miembro de ISIS se puede ver cómo el grupo terrorista alentaba ataques individuales en Occidente

***"La yihad no tiene fronteras. Ataca en cualquier lugar y con cualquier***

---

<sup>6</sup> Winter, C. (2015). The Virtual 'Caliphate': Understanding Islamic State's Propaganda Strategy. Quilliam Foundation. Este estudio documenta cómo ISIS utilizó Twitter para publicar imágenes y videos de ejecuciones de prisioneros y advertencias a los gobiernos occidentales.

*arma. #AllahuAkbar"*<sup>7</sup>

En dicho caso, se puede observar cómo miembros de la organización recurren a Internet o a las redes sociales para conseguir apoyo para su causa.

#### ***4.3. Impacto en la seguridad de los Estados y ciudadanos: ISIS in America***

Considerando que ISIS en la actualidad se encuentra territorialmente desarticulado y que su capacidad de acción ha disminuido notablemente, para el Estado Islámico una de las pocas maneras de generar algún tipo de impacto en suelo norteamericano fue enviando mensajes propagandísticos y radicalizadores a través de las redes.

Por la enorme dependencia de las redes sociales en Estados Unidos y en Occidente en general, los individuos que residen en dichas áreas son considerablemente más propensos a la radicalización y al reclutamiento en internet. Estos colectivos emplean Internet y las redes sociales para alterar las reclamaciones de los jóvenes desorientados, radicalizarlos y otorgarles un propósito.

Retomando el caso estadounidense, haciendo referencia al informe “ISIS in America: From Retweets to Raqqa”, elaborado por Lorenzo Vidino y Seamus Hughes y publicado en diciembre de 2015 por el Program on Extremism de la George Washington University, ninguna de las personas mencionadas dentro del mismo, acusadas de planear ataques había recibido instrucciones específicas de ISIS en el extranjero, según la evidencia presentada en documentos legales y públicos analizados por The New York Times y el Centro de Seguridad Nacional de la Universidad de

---

<sup>7</sup> Fuente: SITE Intelligence Group (2016). Islamic State's New Propaganda Techniques: A Shift in Messaging and Targeting.

Fordham. Pero el rol que jugó la organización fue el de fomentar la radicalización de estas personas a través de discursos alienantes, tanto para que quieran desarrollar un ataque de pequeña o mediana escala en suelo extranjero, como para que deseen viajar para unirse a la lucha armada.

Durante esta sección y como complemento del análisis empírico, se incorporan a continuación una serie de publicaciones reales extraídas de cuentas verificadas vinculadas al ecosistema de propaganda del Estado Islámico (ISIS) entre 2014 y 2017. Estos tweets fueron seleccionados por su relevancia simbólica y su capacidad de ilustrar los mecanismos discursivos a través de los cuales ISIS logró movilizar individuos en territorio estadounidense.

Todos los tweets analizados en esta sección fueron extraídos del informe “ISIS in America”. Este trabajo representa uno de los relevamientos más detallados sobre la forma en que ciudadanos estadounidenses fueron expuestos, radicalizados o movilizados a través del contenido digital difundido por el Estado Islámico, ofreciendo evidencia empírica valiosa sobre el vínculo entre propaganda online y acción terrorista en Occidente.

Estos mensajes forman parte de lo que Berger y Morgan (2015) denominaron “propaganda de activación individual”, es decir, contenido orientado no tanto a construir ideología, sino a gatillar la acción concreta de potenciales atacantes autónomos.

Ejemplos clave y su función discursiva:

**@atawaakul** – *“The bro with me and myself have given bay'ah to Amirul Mu'mineen.*

*May Allah accept us as mujahideen. Make dua. #TexasAttack*”<sup>8</sup>

Este tweet expresa una declaración pública de lealtad (bay'ah) a la figura del califa del Estado Islámico, e invoca términos como mujahideen (combatientes) y dua (oración), estableciendo una conexión directa entre fe, pertenencia y acción violenta. Además, menciona un ataque inminente (#TexasAttack).

*@aashiralamriki – “Contact me on Telegram. Brothers only. Inshallah.”*<sup>9</sup>

Este mensaje opera como un puente entre el espacio público (Twitter) y el privado (Telegram), mostrando cómo la captación digital no termina en la exposición al contenido, sino que avanza hacia canales cifrados para planificación y “adoctrinamiento”. La restricción de acceso (“brothers only”) refuerza la lógica de comunidad cerrada y clandestina.

*@abualyousef – “Wants to live under the shade of the caliphate.”*<sup>10</sup>

Aquí se observa una estrategia de autorrepresentación simbólica: la imagen de perfil con rostro cubierto, el nombre árabe, y la ubicación “Islamic State in America” proyectan la construcción identitaria de un individuo radicalizado, alineado con la visión del califato como refugio moral y espiritual.

*@lionofthed3s3rt (Abu ‘Ukkashah’) – “There is no God but Allah, and Muhammad is His Messenger.”*<sup>11</sup>

---

<sup>8</sup> Vidino, L., & Hughes, S. (2015). \*ISIS in America: From Retweets to Raqqa\*. Program on Extremism, George Washington University. Ver anexo figura D

<sup>9</sup> *Ibid.* Ver anexo figura E

<sup>10</sup> *Ibid.* Ver anexo figura F

<sup>11</sup> *Ibid.* Ver anexo figura G

Este tweet no contiene un llamado explícito a la violencia, pero cumple una función de legitimación ideológica, religiosa y como modo de presencia digital constante.

**@AL\_Amriki7954** – “*My second account: @AL\_Amriki7955*”<sup>12</sup>

La lógica de creación de cuentas múltiples y reactivación tras suspensión evidencia la existencia de estrategias de resistencia a la moderación de contenido, donde cada perfil se convierte en un nodo dentro de un ecosistema resiliente. Estas cuentas, además, interactúan con otras que amplifican sus mensajes a través de shoutouts, de esta manera promocionando a otra cuenta para ayudarla a ganar visibilidad. Es una forma de amplificación digital. Esta táctica se utiliza para evitar el silenciamiento digital ante las suspensiones de cuentas por parte de las plataformas.

### ***Función operativa y psicológica de estos mensajes***

Los tweets aquí analizados no solo transmiten ideas, sino que operan como dispositivos de acción simbólica. Están diseñados para: inspirar (ofreciendo sentido, propósito y una narrativa épica al receptor), movilizar (llamando explícitamente a la acción - atacar o viajar-), conectar (derivando a canales privados donde el proceso de radicalización se intensifica), legitimar (construyendo un marco moral para el uso de la violencia), normalizar (generando familiaridad con símbolos, palabras y estilos del ecosistema yihadista).

Estas publicaciones, aunque breves, condensan un alto poder performativo y ejemplifican cómo ISIS trasladó la radicalización desde los márgenes geográficos hacia los centros urbanos de Occidente, utilizando las redes sociales como infraestructura ideológica y

---

<sup>12</sup> *Ibid.* Ver anexo figura H

emocional.

La edad promedio de los reclutas de combatientes extranjeros en todo el mundo ronda los 27 años (Dodwell, Milton y Rassler, 2016); sin embargo, en EE. UU. estos resultan aún más jóvenes. En el International Journal of Cyber Terrorism, McElreath et Al. sugieren que hay que explorar "el aprovechamiento de las redes sociales por las cuales los individuos simpatizan con causas extremistas y se vuelcan hacia algunas formas de apoyo a la entidad extremista". (2018, p. 27).

La mayoría ni siquiera conoce la religión. Por ejemplo, a la hora de contactar o segmentar audiencias para el Estado Islámico, los individuos que no están muy versados en el Islam pueden ser bastante deseables porque se les podría enseñar versiones más radicales de la religión y ser menos propensos a cuestionarla.

Los oficiales y combatientes de ISIS no sólo difunden y promueven material yihadista, sino que también siguen a sus oponentes. Muchas de las cuentas oficiales de ISIS recuperadas a través de trabajos previos, seguían páginas de agencias estadounidenses como el Departamento de Estado y la CIA, así como de investigadores del terrorismo. Esto no sólo les permite leer lo que «el enemigo» publica y promueve, sino que también les proporciona material de voluntad con fines propagandísticos.

Vemos acá con todo esto, que los mensajes se dirigen a las personas jóvenes y vulnerables, generalmente aisladas y con una percepción alienada de la realidad. En este sentido, ISIS fue particularmente hábil para explotar los sentimientos de ira o ansiedad entre estos jóvenes de manera de fomentar la acción. El contenido de los videos e imágenes de reclutamiento muestra desde una violencia brutal y totalmente explícita contra los infieles e intrusos, hasta la noción de que Occidente perjudica sistemáticamente a los

musulmanes. Todos tienen en común la construcción de un proceso de fomento del odio. Awan (2017), ahondó mucho en este tema, y llegó a la conclusión de que “what we are witnessing is ISIS being able to tap into the minds of young and impressionable people who are more likely to be watching YouTube and using Facebook and Twitter (Awan, 2013). Moreover, this allows groups like ISIS, a direct channel whereby they can play upon individual grievances and dissatisfaction that makes those vulnerable feel as though they are significant and important” (p.139).

### ¿Cómo se ve esto en números?

Las estimaciones del impacto de Internet en el reclutamiento son variadas, pero los expertos sugieren que supera a la modalidad de contacto “en persona” (Center on National Security, 2016).

Siendo relevante en este caso, podemos ver un “word mapping”, extraído del trabajo realizado por Awan en el 2017, de cuáles son las palabras que más frecuentemente aparecieron en Twitter para caracterizar a la organización. Como se mostrará a continuación, el tamaño de letra del “word cloud” representa las palabras que más comúnmente se repitieron en los tweets. Estas incluyeron los términos "hermanos", “levántate”, "reclama", "victoria" y “Jihad”, “lucha”, “Ummah”, “Khalifah” entre otras.

Fig. 6 Word Cloud representing most common reappearing words



La mayoría de estas palabras se destacan por tener influencia directa sobre las acciones de reclutamiento de la organización.<sup>13</sup>

Currently brainwashing little children to enjoy themselves and live in a society without fear.

#khalifa



7 7

[View more photos and videos](#)

A través de este tweet publicado por Abuuthmaan1988, se puede ver cómo se usan nociones “enemigas” que fueron empleadas por diversos gobiernos ante el supuesto "lavado de cerebro" que el Estado Islámico ha empleado en sus admiradores.<sup>14</sup>

Esto también se relaciona con la necesidad de difundir todo en las redes sociales, particularmente entre las últimas generaciones. A pesar de que los miembros/ combatientes de ISIS comparten imágenes de terror y para infundir miedo, también actúan como cualquier otro ciudadano en Twitter. Esto da la sensación y cercanía de que individuos de todas partes del mundo usan las redes sociales de la misma forma. Compartiendo imágenes de su vida diaria: con selfies, fotos con amigos, comiendo, de viaje, etc. Esto hace que a través del uso de las redes sociales se aumente la habilidad para interactuar con personas más allá de los límites geográficos.

<sup>13</sup> Figura 5. Awan (2017).

<sup>14</sup> En el Anexo se muestran ejemplos concretos de este tipo de publicaciones.

A través del análisis de entrevistas a jóvenes que fueron reclutados por ISIS a través de Internet (pero que fueron detenidos antes de cometer cualquier delito), se puede deducir que aquellos jóvenes querían ser recordados y alabados por su ataque, y ser reconocido por el Estado Islámico, al que veían como una comunidad. No se trataba únicamente de afinidad religiosa sino que se trataba de darse visibilidad, de resaltar en un mundo en donde su vida no tenía ningún tipo de impacto. Sin embargo, la mayoría de los jóvenes entrevistados atribuyó responsabilidad al contenido online y, confesó que el contenido era peligrosamente inspiracional y que se adaptaba a todo tipo de audiencias vulnerables.

#### ***4.4 Manifestaciones de la radicalización: ataques inspirados por ISIS en Estados Unidos (2014–2017)***

Resulta necesario presentar una selección de atentados perpetrados en Estados Unidos entre 2014 y 2017 por individuos radicalizados de forma autónoma, cuya motivación estuvo influida —aunque no necesariamente dirigida— por la propaganda digital de ISIS en redes sociales. Estos eventos ilustran cómo el contenido difundido sirvió de inspiración, marco legitimador y catalizador para acciones violentas individuales.

A continuación, se resumen algunos casos a modo de ilustración:

##### **1. Curtis Culwell Center, Texas (3 de mayo de 2015)**

Elton Simpson y Nadir Soofi abrieron fuego en un evento de caricaturas de Mahoma. Posteriormente fueron abatidos en el lugar. Simpson había jurado lealtad al Estado Islámico en Twitter poco antes del ataque. Este caso está incluido

en el informe del FBI sobre terrorismo individual en EE.UU.<sup>15</sup>

## **2. Orlando, Florida – Club Pulse (12 de junio de 2016)**

Omar Mateen mató a 49 personas en un club nocturno LGBTQ+. Durante el ataque llamó al 911 para declarar su lealtad a ISIS. Investigaciones posteriores confirmaron que se había radicalizado mediante el consumo reiterado de propaganda digital.<sup>16</sup>

## **3. Nueva York – Atentado con camioneta (31 de octubre de 2017)**

Sayfullo Saipov utilizó una camioneta para atropellar peatones y ciclistas, dejando varios muertos. Se supo que quiso llevar banderas de ISIS en el vehículo, y justificó su acto con base en videos del grupo terrorista. El FBI clasificó este caso como inspirado por la propaganda digital del Estado Islámico. El subdirector de la policía de Nueva York, John Miller, dijo que el detenido había replicado casi a semejanza las instrucciones que ISIS daba en sus redes acerca de cómo realizar un ataque.<sup>17</sup>

Estos casos no serán objeto de análisis penal/judicial en esta investigación. Su inclusión tiene como objetivo contextualizar la eficacia simbólica de la narrativa digital de ISIS, y demostrar cómo el discurso puede actuar como catalizador de acción en sujetos radicalizados sin necesidad de contacto directo con la organización.

---

<sup>15</sup> Federal Bureau of Investigation (FBI). (2018). \*Lone Offender: A Study of Lone Actor Terrorism in the United States (1972–2015)\*. U.S. Department of Justice.

<sup>16</sup> Callimachi, R. (2016). \*In Orlando, evidence points to ISIS influence, but not direction\*. The New York Times.

<sup>17</sup> U.S. Department of Justice. (2017). \*United States of America v. Sayfullo Saipov\*; CNN (2017). \*NYC attack suspect followed ISIS playbook\*.

## CAPÍTULO 5: ANÁLISIS DE LA ESTRATEGIA DIGITAL DEL ESTADO ISLÁMICO

### 5.1. Resumen de hallazgos principales

El presente trabajo ha permitido demostrar cómo el Estado Islámico (ISIS), a partir del año 2014, modificó de forma radical el panorama del terrorismo global mediante una estrategia de comunicación digital sin precedentes. El análisis evidenció que las TICs, especialmente las redes sociales como Twitter, no solo fueron herramientas complementarias, sino que ocuparon un lugar central y estructurante en los procesos de radicalización, captación y movilización de individuos.

La investigación pone de relieve un desplazamiento paradigmático en la forma de comprender la amenaza terrorista: ya no estamos ante un terrorismo vertical y jerárquico, sino ante un fenómeno descentralizado, narrativo y emocionalmente eficaz, cuya principal escena es el espacio virtual. En este nuevo escenario, la figura del "lobo solitario digital" emerge como el síntoma más visible de esta transformación: individuos radicalizados en la intimidad del entorno digital, sin vínculos orgánicos con organizaciones terroristas, pero movilizados por una narrativa que los interpela, los convoca y les ofrece sentido.

Entre los ejemplos más ilustrativos se encuentran los tweets previamente analizados en el capítulo 4, donde se promovía la yihad global con frases como:

- *“La yihad no tiene fronteras. Ataca en cualquier lugar y con cualquier arma. #AllahuAkbar”*
- *“Hermanos y hermanas, el Califato necesita doctores, ingenieros y soldados. Ven*

*y sé parte de la historia. #HijrahToISIS”*

Estos tweets respaldan los argumentos centrales de la tesis y permiten visualizar con mayor claridad el alcance psicológico y simbólico de la propaganda digital. Así, se refuerza la idea de que la radicalización no es meramente ideológica, sino que opera también desde lo emocional, lo visual y lo narrativo.

Para complementar el análisis cualitativo de la propaganda digital de ISIS, se realizó una sistematización parcial de contenido de tweets basada en ejemplos documentados en estudios clave como The ISIS Twitter Census (Berger & Morgan, 2015), los informes del SITE Intelligence Group (2015–2017), el trabajo de Charlie Winter (2017) sobre narrativa visual y el informe “Isis in America” (2016).

Se tomaron como base más de 40 tweets y publicaciones representativas, que circularon entre 2014 y 2017 en cuentas vinculadas al Estado Islámico o a simpatizantes del califato. El proceso consistió en una clasificación temática de los mensajes según su contenido dominante, un análisis del tono emocional predominante en cada mensaje, y por último la categorización manual y estimación porcentual proporcional.

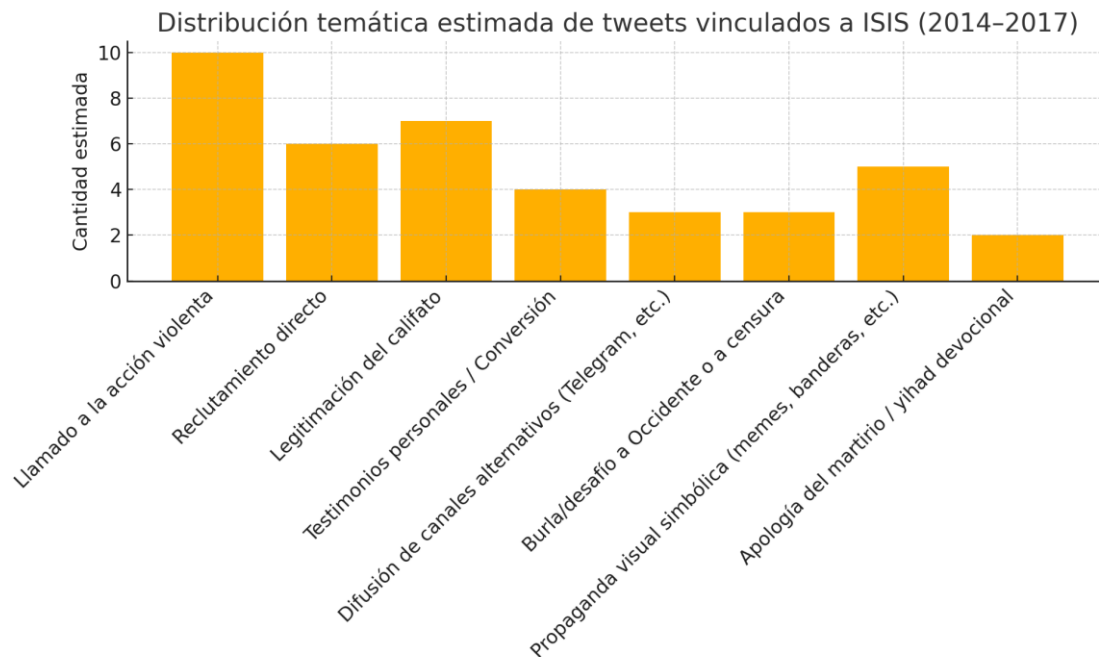
La finalidad no fue obtener una muestra estadísticamente representativa, sino construir una aproximación visual y explicativa del tipo de mensajes que circularon con mayor frecuencia e impacto en redes sociales durante el auge de ISIS.

Estos resultados están representados en:

- Un gráfico de barras que muestra la distribución temática estimada de los tweets
- Un gráfico de torta que ilustra el tono emocional predominante en los mensajes

analizados.

Ambas visualizaciones complementan el análisis argumental de esta tesis y contribuyen a visualizar cómo ISIS estructuró su narrativa digital para captar, radicalizar e inspirar violencia individualizada en jóvenes occidentales, especialmente en Estados Unidos.



**Figura 6<sup>18</sup>.** Distribución temática estimada de tweets vinculados a ISIS (2014–2017).

### ¿Qué representa?

- Llamados a la violencia: Incluye tweets que incitan directamente a cometer atentados o asesinatos.
- Reclutamiento: Tweets que invitan a unirse al califato o emigrar hacia Siria/Irak.
- Legitimación del califato: Contenido que muestra a ISIS como un Estado legítimo y funcional.

---

<sup>18</sup> Figura de elaboración propia.

- Propaganda visual simbólica: Videos o imágenes de ejecuciones, combates
- Testimonios personales: vida cotidiana bajo ISIS
- Difusión de canales alternativos,
- Desafío a Occidente
- Yihad devocional

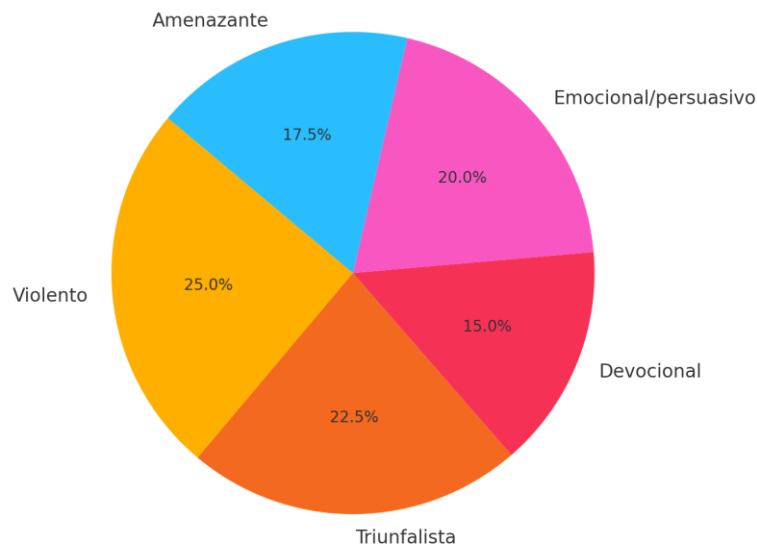
Esta distribución temática subraya el carácter intencional y multifacético de la propaganda de ISIS. No se trataba de mensajes homogéneos, sino de una estrategia segmentada, diseñada para interpelar a distintos perfiles de usuarios y acompañar diferentes fases del proceso de radicalización individual.



**Figura 7<sup>19</sup>**

<sup>19</sup> Figura de elaboración propia

Tono emocional en tweets vinculados a ISIS (2014–2017)



**Figura 8<sup>20</sup>.** Análisis del tono emocional en tweets vinculados a ISIS (2014–2017)

El tono utilizado en estos mensajes se puede clasificar en: Triunfalista (ej.: proclamaciones de lealtad al califato), Amenazante (llamados a la violencia directa), Devocional (uso de expresiones como inshallah, bay'ah, mujahedeen)o/y Emocional (construcción de sentido de propósito y sacrificio). El lenguaje combina referencias religiosas, lenguaje informal y un tono altamente performativo, que busca generar identificación y pertenencia.

## **5.2 Estrategia Comunicacional de ISIS en Twitter: Objetivos, Audiencias y Tácticas**

Tipología del Contenido Difundido:

A partir del examen de los tweets seleccionados, se identificaron diversas categorías de contenido, cada una con una función específica dentro de la estrategia global:

---

<sup>20</sup> Figura de elaboración propia

- **Exhortaciones Directas a la Acción:** Mensajes concisos que instaban a los usuarios a perpetrar ataques, manifestar lealtad (bay'ah) al califato o establecer contacto con facilitadores del reclutamiento.
- **Narrativas Testimoniales:** Relatos en primera persona, a menudo atribuidos a individuos de origen occidental (ejemplificados por usuarios como “abdualyousef” o “abuukkashah”), que presentaban una visión idealizada de la vida bajo el califato y reforzaban la idea de pertenencia.
- **Diseminación de Canales Seguros:** Publicaciones que proporcionaban información de contacto a través de plataformas de mensajería cifrada, como Telegram, facilitando la comunicación privada para etapas avanzadas de reclutamiento o planificación.
- **Contenido Visual Memetizado:** Uso de imágenes y memes para ridiculizar las contramedidas de la plataforma (como la suspensión de cuentas, evidenciado en el ejemplo “coming back from Twitter suspension like...”), buscando generar camaradería y resiliencia entre simpatizantes.
- **Declaraciones de Adhesión Ideológica:** Mensajes que reafirmaban el compromiso con la ideología de ISIS y la justificación de la violencia, como el tweet previo al atentado atribuido a Elton Simpson (#texasattack).

Se constata una preferencia marcada por la combinación de texto breve y el uso de imágenes de perfil con fuerte carga simbólica o impactante. Este formato optimiza la rápida diseminación (viralización) en el entorno digital de Twitter, facilita la memorización de los mensajes clave y promueve el reconocimiento mutuo entre miembros y simpatizantes de la red.

### Objetivos Comunicacionales Inferidos:

Del análisis del contenido y su estructura temática, se desprenden los siguientes objetivos comunicacionales centrales perseguidos por ISIS en Twitter:

- Legitimar la Violencia: Presentar las acciones armadas no como actos criminales, sino como un deber religioso y una respuesta justificada.
- Diseminar la Ideología del Califato: Construir una identidad colectiva sólida y ofrecer una contranarrativa atractiva frente a los valores y sistemas políticos occidentales.
- Incitar al Odio y a la Acción: Fomentar la hostilidad hacia los "enemigos" designados y motivar la participación activa, glorificando el martirio y ridiculizando al adversario.
- Reclutar Militantes y/o Inspirar Atacantes Autónomos: Utilizar mensajes personalizados, accesibles y cargados emocionalmente para atraer nuevos miembros o incitar a individuos ya radicalizados a cometer actos violentos de forma independiente ("lobos solitarios").

### Audiencia Objetivo Primaria:

La segmentación implícita en los mensajes y temas permite inferir los grupos demográficos y psicológicos a los que ISIS dirigía prioritariamente sus esfuerzos de comunicación en esta plataforma:

- Musulmanes Residentes en Occidente: Particularmente aquellos que experimentaban sentimientos de alienación cultural, marginalización social o conflicto identitario.

- Jóvenes en Búsqueda de Propósito: Individuos, independientemente de su trasfondo religioso inicial, que atravesaban etapas de vulnerabilidad, búsqueda de identidad, sentido de pertenencia o rebeldía.
- Simpatizantes Previamente Radicalizados: Individuos ya convencidos ideológicamente y potencialmente dispuestos a pasar a la acción directa.

La estrategia comunicacional estaba calibrada para maximizar la resonancia en estos perfiles específicos, activando simultáneamente narrativas de redención personal, pertenencia a una comunidad global y una lógica de polarización extrema ("nosotros contra ellos")

### ***5.3 Nota metodológica***

Cálculo de porcentajes: Para cada categoría temática y emocional, se usó la siguiente fórmula: *Porcentaje de una categoría = (Cantidad de tweets en esa categoría / 40) × 100*

Ejemplo: 10 tweets con llamados violentos  $\rightarrow (10 / 40) \times 100 = 25\%$

6 tweets de reclutamiento  $\rightarrow (6 / 40) \times 100 = 15\%$  Y así sucesivamente.

La clasificación fue realizada de manera manual y cualitativa, y los porcentajes resultantes reflejan la frecuencia relativa de cada categoría dentro del conjunto total analizado. Es importante destacar que este análisis no pretende ser exhaustivo ni estadísticamente representativo del universo total de tweets radicales, sino que busca visualizar tendencias generales y brindar una herramienta interpretativa para comprender cómo ISIS estructuró su discurso digital en función de distintos objetivos propagandísticos.

Este trabajo no solo confirma el rol fundamental de las TICs para ISIS, sino que obliga a

reformular los marcos teóricos tradicionales de seguridad y terrorismo. El extremismo digital opera como un ecosistema simbólico que debe abordarse desde la interdisciplina.

#### ***5.4 Limitaciones del Análisis***

Es fundamental reconocer ciertas limitaciones inherentes al presente análisis de la estrategia comunicacional de ISIS en Twitter, derivado de la metodología empleada y la naturaleza de los datos disponibles:

- **Tamaño y Representatividad de la Muestra:** La principal limitación radica en que el análisis se basa exclusivamente en una muestra reducida de 40 tweets específicos, seleccionados y presentados en los informes previamente mencionados. Este corpus es inherentemente limitado y no puede considerarse estadísticamente representativo del volumen total ni de la diversidad completa de las comunicaciones de ISIS en Twitter entre 2014 y 2017 como se mencionó previamente. Los hallazgos, por tanto, deben interpretarse como indicativos de ciertas tácticas y temas presentes, pero no necesariamente exhaustivos.
- **Dependencia de la Fuente Secundaria:** El análisis se sustenta en ejemplos ya filtrados y presentados por fuentes secundaria. No se realizó una recopilación y análisis primario de un conjunto de datos más amplio directamente desde la plataforma dado la eliminación de los tweets y la suspensión de cuentas . Esto implica una dependencia de los criterios de selección y posible sesgo de los informe originales utilizados, cuyos objetivos específicos podrían diferir de los de esta investigación.
- **Especificidad Temporal:** Los tweets analizados corresponden a un marco temporal

específico. Las tácticas y estrategias de comunicación de grupos como ISIS son altamente dinámicas y adaptativas, evolucionando en respuesta a las contramedidas de las plataformas y los cambios en el entorno geopolítico. Por consiguiente, las conclusiones extraídas podrían no ser directamente aplicables a periodos anteriores o posteriores de la actividad en línea de ISIS.

- **Enfoque Exclusivo en Twitter:** Este análisis se centra únicamente en Twitter (X) . ISIS operó (y otros grupos extremistas operan) a través de un ecosistema digital complejo que incluye múltiples plataformas (Telegram, WhatsApp, foros en la Dark Web, etc.), cada una con características y dinámicas propias. La estrategia en Twitter es solo una faceta de su presencia online global, y las tácticas pueden variar significativamente entre plataformas.
- **Contexto Geográfico y Lingüístico:** es plausible asumir un sesgo hacia contenido en inglés y/o relevante para el contexto estadounidense dado los informes utilizados y el caso seleccionado. Esto podría limitar la generalización de los hallazgos a las operaciones de comunicación de ISIS en otros idiomas (como el árabe, francés, etc.) o dirigidas a otras regiones del mundo.
- **Naturaleza Interpretativa:** La inferencia de los objetivos comunicacionales y la identificación de las audiencias objetivo, si bien se basan en el contenido textual y visual de los tweets, conllevan un componente interpretativo por parte de la investigadora.

## **CAPÍTULO 6: CONCLUSIONES Y RECOMENDACIONES**

### **6.1. Limitaciones de las políticas de seguridad tradicionales**

#### *El papel de las plataformas digitales y la regulación de contenidos*

Las plataformas han pasado de una postura neutral a implementar políticas activas de moderación. Sin embargo, persisten dilemas éticos sobre la libertad de expresión, el uso de IA y la definición de extremismo. La cooperación con los Estados es clave para regular eficazmente estos espacios sin caer en la censura.

Las redes sociales y plataformas digitales se convirtieron en espacios de propaganda, captación y coordinación para grupos terroristas, obligando a las empresas tecnológicas a asumir un rol activo en la moderación y eliminación de contenido extremista. Inicialmente muchas plataformas defendían su neutralidad, pero tras casos como el uso de Twitter y YouTube por parte de ISIS, implementaron medidas como: la eliminación automática de contenido, el bloqueo de cuentas reincidentes, ajustes algorítmicos, entre otras. Weimann (2016) advierte que estas acciones empujaron a los extremistas hacia espacios encriptados como Telegram, lo que plantea nuevos desafíos.

### **6.2. Implicaciones para la seguridad global**

En una entrevista realizada a la directora del Center on National Security, Karen Greenberg, ella expresó: “ISIS, in addition to being a force in the Middle East, is essentially a global gang preying upon alienated youth and providing an identity for self-selecting men and women who are isolated, angry and, at the same time, in search of a mission in life,” (New York Times, 2016).

Los grupos terroristas en este caso, no se enfrentan directamente a los estados de manera simétrica, dado que cuentan con las de perder. Entonces, desarrollan estrategias para poder combatir contra ellos, yendo hacia su eslabón más desprotegido, los ciudadanos. Aquí podemos ver la naturaleza política de estos actos de terror.

Ahora bien, la contradicción que se encuentra es que mientras esta organización terrorista buscaba formas alternativas de ataque, dada la reducción de su poder militar, el mundo se fue moviendo hacia una “Era Digital” que imposibilitaba un control estatal total sobre el contenido expresado en las redes. En otras palabras, el advenimiento de la era digital significó que un mayor volumen de gente estuviera expuesta a una gran cantidad de mensajes cibernéticos, potencialmente peligrosos, al tiempo que los Estados perdían capacidad para regularlos. En este contexto, el Estado Islámico aprovechó este vacío de seguridad, utilizando las tecnologías de información para contactar a los ciudadanos más expuestos y cooptarlos para que se unieran a su causa.

Las políticas de seguridad tradicionales, centradas en la defensa territorial, la militarización y la vigilancia, resultan cada vez más obsoletas frente a las nuevas amenazas que se desarrollan en el entorno digital. El terrorismo contemporáneo, especialmente el representado por el Estado Islámico (ISIS) en este trabajo, ha demostrado una notable capacidad de adaptación y ha utilizado las TICs para radicalizar, reclutar y coordinar acciones sin necesidad de una presencia física organizada.

Como señala Richard Jackson (2018), la concepción actual de seguridad sigue anclada a un paradigma estado-céntrico, mientras que el terrorismo digital “trasciende fronteras y jerarquías, operando en redes descentralizadas que desafían las estructuras

tradicionales de inteligencia y defensa”.

### **6.3. Cooperación internacional en la lucha contra el terrorismo digital**

*Propuestas para abordar la radicalización digital: Estrategias de contra-narrativa y desradicalización digital*

Los ejemplos concretos de tweets y contenidos digitalmente viralizados —como los que alentaban a perpetrar ataques desde cualquier lugar del mundo o promovían la emigración al califato mediante el hashtag #HijrahToISIS— muestran cómo la ideología extremista fue traducida a códigos accesibles, reproducibles y atractivos para sectores juveniles, especialmente en contextos de vulnerabilidad, marginación o crisis identitaria. En este marco, la radicalización digital pasó a convertirse en uno de los principales desafíos de la seguridad internacional contemporánea. Su carácter transnacional, su velocidad de propagación y su potencial de impacto exigen repensar no solo las herramientas de prevención y disuasión, sino también los propios marcos teóricos desde los cuales abordamos el fenómeno terrorista.

Este trabajo ha buscado, desde una perspectiva crítica y multidisciplinaria, aportar al entendimiento de este nuevo ecosistema de violencia política, donde el algoritmo, la imagen, el lenguaje y la emocionalidad juegan un rol tan determinante como las armas. La identificación de las limitaciones de las políticas de seguridad tradicionales, así como la evaluación de las estrategias de contra-narrativa, cooperación internacional y regulación de contenidos, permite afirmar que las respuestas estatales aún son fragmentarias y reactivas frente a un fenómeno que exige anticipación, inteligencia colectiva y una ética democrática firme.

La radicalización violenta ya no depende únicamente del adoctrinamiento físico o del contacto directo con organizaciones terroristas. En el entorno digital, el proceso se vuelve más difuso, descentralizado, operando a través de comunidades simbólicas y discursos que interpelan subjetividades vulnerables. Frente a este nuevo escenario, se vuelve imprescindible articular estrategias multidimensionales que aborden la radicalización desde sus causas estructurales hasta sus mecanismos narrativos.

Entre las principales recomendaciones destacan:

1. Fortalecer estrategias de contra-narrativa adaptadas al entorno digital: Una de las herramientas más relevantes es la contra-narrativa, entendida como el conjunto de mensajes que busca desactivar, neutralizar o reemplazar las narrativas extremistas. No se trata solo de refutar ideologías, sino de ofrecer discursos alternativos creíbles, emocionales y culturalmente resonantes, que logren captar la atención de las mismas audiencias objetivo (apoyarse en análisis de datos y segmentación digital). Para que estas estrategias sean eficaces, deben cumplir con ciertos requisitos: Ser creadas y difundidas preventivamente y no sólo como una reacción ante los discursos extremistas, ser difundidas por actores con legitimidad social, como ex radicalizados, líderes comunitarios o figuras culturales cercanas a los públicos en riesgo. A su vez, deben utilizar los mismos recursos: incorporar formatos dinámicos (videos cortos, reels, podcasts, memes) y lenguajes propios de las redes sociales.
2. Establecer marcos sólidos de cooperación público-privada: La vasta mayoría de la infraestructura digital donde ocurre la radicalización es de propiedad y gestión privada. Las empresas poseen la capacidad técnica, el acceso a los datos (dentro de marcos legales) y el control sobre los algoritmos y políticas de moderación. Los

gobiernos poseen la legitimidad democrática, el mandato de seguridad nacional y las capacidades de inteligencia y aplicación de la ley. Ninguno puede afrontar por sí solo la lucha contra el extremismo online. Por ello, se requiere un esquema/mecanismos de gobernanza compartida, en el que los sectores público y privado articulen esfuerzos de forma sostenida, transparente y respetuosa de los derechos humanos. Esto implica: Establecer protocolos claros de detección y remoción de contenidos extremistas, invertir en centros conjuntos de monitoreo y análisis algorítmico, capaces de anticipar tendencias de radicalización, estimular acuerdos de cooperación con plataformas emergentes y redes descentralizadas (Telegram, Discord, etc.), donde se traslada parte del discurso radical tras la moderación en redes tradicionales. Otro requisito fundamental es diseñar mecanismos para compartir datos de manera segura, respetando la privacidad pero garantizando capacidad de respuesta.

3. Reforzar la prevención social y comunitaria: El fenómeno de la radicalización no puede ser abordado únicamente desde la ciberseguridad. Se requiere una visión integradora, que articule políticas de inclusión y educación como estrategias de prevención a largo plazo. Abordar las "causas raíz" o los factores de vulnerabilidad (exclusión social, discriminación, crisis de identidad, falta de oportunidades, traumas) reduce la probabilidad de que los individuos sean receptivos a la propaganda extremista online. Comunidades resilientes y cohesionadas deben ser la primera línea de defensa. Algunos programas a llevar a cabo podrían ser:

- Inversión en programas de educación que fomenten la alfabetización mediática y digital y el pensamiento crítico desde edades tempranas.
- Apoyo a iniciativas comunitarias que promuevan la inclusión social, el diálogo

intercultural e interreligioso y ofrezcan espacios seguros para jóvenes.

- Capacitación de actores clave en contacto directo con poblaciones vulnerables (docentes, trabajadores sociales, líderes religiosos, policía de proximidad) para identificar señales tempranas de alerta y saber cómo intervenir o derivar adecuadamente (sin estigmatizar).
- Desarrollo de programas de intervención y desvinculación personalizados para individuos que ya muestran signos de radicalización, ofreciendo apoyo psicosocial, mentoring y alternativas vitales.
- Políticas públicas que luchen activamente contra la discriminación y la desigualdad socioeconómica.

4. Desarrollar un marco legal internacional sobre discurso extremista y responsabilidad

algorítmica: Frente a un fenómeno que trasciende fronteras, es urgente la construcción de un marco normativo global que permita enfrentar el extremismo digital sin vulnerar los derechos fundamentales. Actualmente, existe una brecha significativa entre las legislaciones nacionales, regionales e internacionales, lo que impide una acción coordinada eficaz. Este marco debería incluir:

- Una definición consensuada de “discurso extremista violento”, diferenciándolo de la libertad de expresión protegida.
- Fomentar el debate y la negociación en foros multilaterales (ONU, Consejo de Europa, G7/G20, etc.) para buscar consensos sobre definiciones de contenido ilícito (incitación al odio, apología del terrorismo) que respeten la libertad de expresión.
- Promover la adopción de estándares internacionales o "soft law" (principios

rectores, códigos de conducta) sobre la moderación de contenidos y la transparencia algorítmica.

- Explorar modelos de "deber de cuidado" (duty of care) o marcos de co-regulación que exijan a las plataformas evaluar y mitigar los riesgos sistémicos asociados a sus servicios, incluyendo la amplificación de contenido extremista.
  - Mejorar los mecanismos de cooperación judicial internacional para investigar y enjuiciar delitos relacionados con el terrorismo y el extremismo violento online.
- La creación de un observatorio intergubernamental sobre extremismo online, que provea datos comparativos y recomendaciones técnicas.

En conjunto, estas propuestas conforman una respuesta integral, preventiva y adaptada al ecosistema digital contemporáneo. Su implementación requiere voluntad política, coordinación institucional y una firme defensa de los valores democráticos frente a los discursos que buscan deslegitimarlos desde las sombras del entorno virtual.

El aporte central de esta tesis reside en evidenciar que la lucha contra el extremismo violento ya no se libra exclusivamente en los campos de batalla, sino también —y cada vez más— en los entornos digitales donde se construyen subjetividades, identidades y visiones del mundo. La batalla por el significado, la pertenencia, es hoy un componente esencial de la seguridad global, y requiere del compromiso activo de gobiernos, plataformas digitales, actores sociales y académicos por igual.

#### **6.4. Reflexión final**

A través del análisis de más de 40 publicaciones de cuentas asociadas/inspiradas en ISIS, se identificaron patrones temáticos, lingüísticos, estratégicos y emocionales que ayudan a validar esta hipótesis. La radicalización no fue un proceso aleatorio ni espontáneo, sino

intencionalmente diseñado, estructurado para alcanzar públicos específicos y conducirlos a una transformación cognitiva, afectiva y conductual.

La evidencia reunida en este capítulo ayuda a la hipótesis central de la tesis: el uso estratégico de las TICs por parte del Estado Islámico ha modificado la estructura de la amenaza terrorista y plantea nuevos desafíos a la seguridad internacional. La radicalización ya no requiere de contacto físico, entrenamiento militar ni jerarquía organizacional. Basta una narrativa bien diseñada, una red social disponible, y un receptor emocionalmente susceptible.

Este trabajo ha contribuido a visibilizar cómo el extremismo digital opera como un ecosistema narrativo, emocional y simbólico que desborda los marcos tradicionales del análisis securitario. El Estado Islámico no solo innovó en el campo militar o territorial, sino también en el uso de la palabra, la imagen, y el algoritmo como armas de guerra.

La lucha contra el extremismo violento requiere una transformación profunda de las herramientas analíticas y políticas. La vigilancia, la cooperación internacional deben ir acompañadas de estrategias narrativas contrahegemónicas, alfabetización digital, y una ética democrática capaz de resistir tanto el terror como el autoritarismo. En última instancia, la seguridad del siglo XXI se jugará también en los márgenes del discurso, en las redes que conectan símbolos, emociones e identidades.

## Bibliografía:

- Abuuthmaan1988. (2014, June 29). Currently brainwashing little children to enjoy themselves and live in a society without fear [Tweet]. Retrieved from: <https://twitter.com/Abuuthmaan1988/status/483359222013624321>
- Awan, I. (2017). “Cyber-Extremism: Isis and the Power of Social Media”. Society, Vol. 54, No. 2. Disponible en <https://link.springer.com/content/pdf/10.1007%2Fs12115-017-0114-0.pdf>
- Barrett, R. (2017). Beyond the Caliphate: Foreign Fighters and the Threat of Returnees. The Soufan Center. <https://thesoufancenter.org/wp-content/uploads/2017/11/Beyond-the-Caliphate-Foreign-Fighters-and-the-Threat-of-Returnees-TSC-Report-October-2017-v3.pdf>
- Bazaga Fernández, I. y Tamayo Sáez, M. (2021). Radicalización violenta. Eunomía. Revista en Cultura de la Legalidad, 20, pp. 322-333. <https://doi.org/10.20318/eunomia.2021.6079>
- Berger, J. M. & Jonathon M. (2015). “The ISIS Twitter census: Defining and describing the population of ISIS supporters on Twitter”. Brookings Project on U.S. Relations with Islamic World. Washington, DC: The brookings Institution. No. 20, March 2015. Disponible en: <https://www.brookings.edu/articles/the-isis-twitter-census-defining-and-describing-the-population-of-isis-supporters-on-twitter/>
- Cano Paños, M. (2008). Ob; cit, Thevessen, (pp. 82 y ss). “Internet y terrorismo islamista. Aspectos criminológicos y legales”. EGUZKILORE, Número 22. San Sebastián Diciembre, p 67 - 88. Disponible en <https://www.ehu.eus/documents/1736829/2176658/03+Cano.indd.pdf>

- Castells, M. (2009). Comunicación y poder. Madrid, Alianza Editorial, 679 pp. [ISBN: 978-84-206-8499-4]
- Center on National Security. (2016). “Case by case: ISIS prosecutions in the United States”. New York, NY: Fordham Law. Disponible en: [https://www.centeronnationalsecurity.org/s/CNS\\_case\\_by\\_case\\_ISIS\\_july2016.pdf](https://www.centeronnationalsecurity.org/s/CNS_case_by_case_ISIS_july2016.pdf)
- Chomsky, N. (2002). 9-11: Was There an Alternative? Seven Stories Press.
- Cohen-Almagor, R. (2017). “Jihad Online: How Do Terrorists Use the Internet?”, en Francisco Campos Freire, Xosé Rúas Araújo, Valentín Alejandro Martínez Fernández, and Xosé López García, Media and Metamedia Management, Dordrecht: Springer, pp. 55-66. Disponible en Cohen-Almagor, Raphael and Cohen-Almagor, Raphael, Jihad Online: How Do Terrorists Use the Internet? (December 1, 2016). in Francisco Campos Freire, Xosé Rúas Araújo, Valentín Alejandro Martínez Fernández, and Xosé López García (eds.), Media and Metamedia Management (Dordrecht: Springer, 2017), pp. 55-66, Available at SSRN: <https://ssrn.com/abstract=2878429>
- Dodwell, B. Milton D, & Rassler D. (2016). The Caliphate’s global workforce: An inside look at the Islamic State’s foreign fighter paper trail. West Point, NY: Combating Terrorism Center at West Point. Disponible en: <https://ctc.westpoint.edu/the-caliphates-global-workforce-an-inside-look-at-the-islamic-states-foreign-fighter-paper-trail/>
- Dubet (2020). La Época de las Pasiones Tristes, cap. 4 (Iras e indignaciones)
- Fernández, A. (2015). Here to stay and growing combating ISIS propaganda networks. Washington, DC: brookings Institution. Disponible en:

[https://www.brookings.edu/wp-content/uploads/2016/06/IS-Propaganda\\_Web\\_English.pdf](https://www.brookings.edu/wp-content/uploads/2016/06/IS-Propaganda_Web_English.pdf)

- Ganor, B. (2002). Defining Terrorism: Is One Man's Terrorist another Man's Freedom Fighter? *Police Practice and Research*, 3(4), 287–304.  
<https://doi.org/10.1080/1561426022000032060>
- Ganor, B. (2016). *Global Alert: The Rationality of Modern Islamist Terrorism and the Challenge to the Liberal Democratic World*. Columbia University Press.
- Ganor, B. (2021). Understanding the Motivations of "Lone Wolf" Terrorists: The "Bathtub" Model. *Perspectives on Terrorism*, 2021, Vol 15, Issue 2. Terrorism Research Initiative. Disponible en <https://www.jstor.org/stable/27007291>
- García-Magariño, S., Valentín Cotobal, V. y Jiménez, M. (2022). Un intento de explicación teórica de la radicalización violenta islamista en España. *Revista Colombiana de Sociología*, 45(2), pp 141-164  
<https://dialnet.unirioja.es/descarga/articulo/9759390.pdf>
- González Torres, I. (2018). “Las TICs y el terrorismo: al-Qaeda”. *RSW La web de la Seguridad Global*. Recuperado de <https://www.redsafeworld.net/post/las-tecnolog%C3%ADas-de-lacomunicaci%C3%B3n-y-el-terrorismo-al-qaeda>
- Greenberg, K. (2016). “Counter-Radicalization via the Internet”. *The Annals of the American Academy of Political and Social Science (ANNALS, AAPSS)*. Vol. 668, Issue: 1, 165-179. Disponible en: <https://doi.org/10.1177/0002716216672635>
- Gruenewald, J., Chermak, S., & Freilich, J. D. (2013). Distinguishing “loner” attacks from other domestic extremist violence. *Criminology & Public Policy*, 12(1), 68.

- Habermas, J (2022) “Reflections and Hypothesis on a Further Structural Transformation of the Political Public Sphere” *Theory, Culture & Society*, 39:4, pp. 145-171
- Hellmich, C. (2008). *Marc Sageman: Leaderless Jihad: Terror Networks in the Twenty-First Century* : (Philadelphia: University of Pennsylvania Press, 2008). *Democracy and Security*, 4(3), 318–320.  
<https://doi.org/10.1080/17419160802463779>
- Hoffman, Y. (2017). Who is afraid of ISIS? ISIS anxiety and its correlates. *Stress and Health*, 2017, 1–9. PMID:28589703 Disponible en <https://doi.org/10.1002/smi.2764>
- Ingram, H. J. (2018). An Analysis of Inspire and Dabiq: Lessons from AQAP and Islamic State’s Propaganda War. *Studies in Conflict & Terrorism*, 41(5), 357-377. Disponible en [10.1080/1057610X.2016.1212551](https://doi.org/10.1080/1057610X.2016.1212551)
- Jackson, R. (2007). “The core commitments of critical terrorism studies”, *European Political Science* 6 (2007). Disponible en: doi: [10.1057/palgrave.eps.2210141](https://doi.org/10.1057/palgrave.eps.2210141)
- Jackson, R. (2008). The Study of Terrorism after 11 September 2001: Problems, Challenges and Future Developments. *Political Studies Review*. 7(2), 171-184.  
<https://doi.org/10.1111/j.1478-9299.2009.00177.x>
- Klausen, J. (2014). Tweeting the Jihad: Social Media Networks of Western Foreign Fighters in Syria and Iraq. *Studies in Conflict & Terrorism*, 38(1), 1–22.  
<https://doi.org/10.1080/1057610X.2014.974948>
- Lind, W. (1989) The changing face of war: Into the fourth generation, *Quantico USA, Marine Corps Gazette*, pg. 22 a 26 .

- Lobato, R. (2019) “En busca de los extremos: tres modelos para comprender la radicalización”, *Revista de Estudios en Seguridad Internacional*, Vol. 5, No. 2, (2019), pp. 107-125. Disponible en : <http://dx.doi.org/10.18847/1.10.7>
- McElreath, D. H., Doss, D. A., McElreath, L., Lindsley, A., Lusk, G., Skinner, J., & Wellman, A. (2018). The communicating and marketing of radicalism: A case study of ISIS and cyber recruitment. *International Journal of Cyber Warfare and Terrorism (IJCWT)*, 8(3), 26-45. [10.4018/978-1-7998-2466-4.ch039](https://doi.org/10.4018/978-1-7998-2466-4.ch039)
- McLuhan, M.; Powers, B.R. (1995) *La aldea global*. Barcelona: Gedisa Editorial.
- Midhio, I., Ismadi, A., & Waluyo, A. (2017). The Impact of Radicalism toward National Defense. *Jurnal Pertahanan*, 3(1), 1–14  
<https://doi.org/10.33172/jp.v3i1.100>
- Opperman, J & Alhashimi, H. (2014). How ISIS works. Recuperado de: <http://www.nytimes.com/interactive/2014/09/16/world/middleeast/how-isis-works.html>
- Oppermann, T. (2019). The Digital Jihad: How ISIS Used Social Media to Recruit and Radicalize Fighters. *Journal of Terrorism Studies*, 8(2), 115-134
- Sawyer, D. (2017). “A look at how ISIS is recruiting young Americans through the internet”. de ABC News. Recuperado de: <https://abcnews.go.com/Nightline/video/isis%20recruiting-young-americans-internet-50926807>
- SITE Intelligence Group (2016). *Islamic State’s New Propaganda Techniques: A Shift in Messaging and Targeting*. Disponible en <https://ent.siteintelgroup.com/>
- Springli, M. S. y Curvale, P. (2021). La Cooperación Internacional en la lucha contra el terrorismo yihadista en el seno de la Unión Europea tras los atentados

terroristas a partir del año 2015. *Revista Integración y Cooperación Internacional*, 33 (jul-dic), 16-34. Disponible en <https://doi.org/10.35305/revistamici.v0i33.79>

- Stern, J & Berger, J. M. (2015). “ISIS: The state of terror”. New York, NY: ecco.
- Byman, D. (2016). Understanding the Islamic State—A Review Essay [Review of *The Rise of the Islamic State: ISIS and the New Sunni Revolution*; *The ISIS Apocalypse: The History, Strategy, and Doomsday Vision of the Islamic State*; *ISIS: The State of Terror*; *Black Flags: The Rise of ISIS*; *ISIS: Inside the Army of Terror*, by P. Cockburn, W. McCants, J. Stern, J. M. Berger, J. Warrick, M. Weiss, & H. Hassan]. *International Security*, 40(4), 127–165.  
<http://www.jstor.org/stable/43828316>
- The Soufan Group. (2015). Foreign fighters: An updated assessment of the flow of foreign fighters into Syria and Iraq. New York, NY: The Soufan Group. Disponible en: [http://soufangroup.com/wp-content/uploads/2015/12/TSG\\_ForeignFightersUpdate3.pdf](http://soufangroup.com/wp-content/uploads/2015/12/TSG_ForeignFightersUpdate3.pdf).
- Thompson, Robin L. (2011). Radicalization and the use of social media. *Journal of Strategic Security*, 4(4), 170. <http://dx.doi.org/10.5038/1944-0472.4.4.8>  
Disponible en <http://scholarcommons.usf.edu/jss/vol4/iss4/9>
- Vidino, L., & Hughes, S. (2015). \*ISIS in America: From Retweets to Raqqa\*. Program on Extremism, George Washington University. Recuperado de <https://extremism.gwu.edu/sites/g/files/zaxdzs5746/files/downloads/ISIS%20in%20America%20-%20Full%20Report.pdf>
- Watkin, A & Whittaker, J. (2017). “Evolution of terrorists’ use of the Internet”. *Counterterror Business*. Recuperado de: <https://counterterrorbusiness.com/features/evolution-terrorists%E2%80%99->

[use%20internet](#)

- Weimann, G. (2014) "Virtual Packs of Lone Wolves: How the internet made 'lone wolf' terrorism a misnomer": Wilson Center. Recuperado de: <https://medium.com/its-a-medium-world/virtual-packs-of-lone-wolves-17b12f8c455a>
- Weimann, G. (2016). Terrorism in Cyberspace: The Next Generation. Columbia University Press.
- Winter, C. (2015). The Virtual 'Caliphate': Understanding Islamic State's Propaganda Strategy. Quilliam Foundation. Recuperado de <https://core.ac.uk/download/pdf/30671634.pdf>
- Winter, C. (2017). Media Jihad: The Islamic State's Doctrine for Information Warfare. International Centre for the Study of Radicalisation (ICSR). Recuperado de <https://icsr.info/2017/02/13/icsr-report-media-jihad-islamic-states-doctrine-information-warfare/>
- Yourish, K.& Williams J. (2016). "ISIS in América", de New York Times. Recuperado de: [https://www.nytimes.com/interactive/2016/02/04/us/isis-in-america.html?\\_r=1](https://www.nytimes.com/interactive/2016/02/04/us/isis-in-america.html?_r=1)

## 11. Anexos

Figura A:

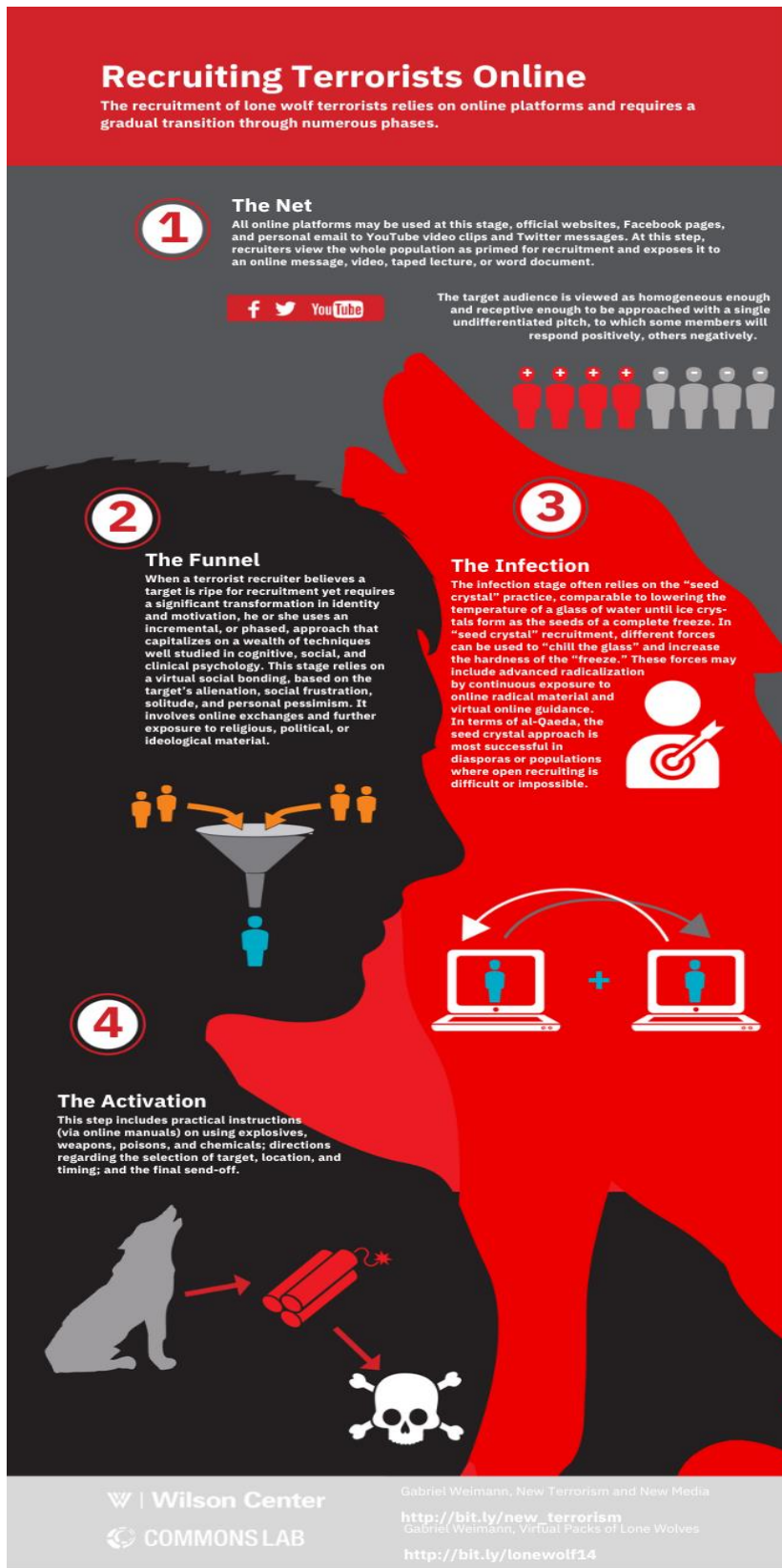


**Figura B**



**Figura A y B: fuente Twitter (2014-2015)**

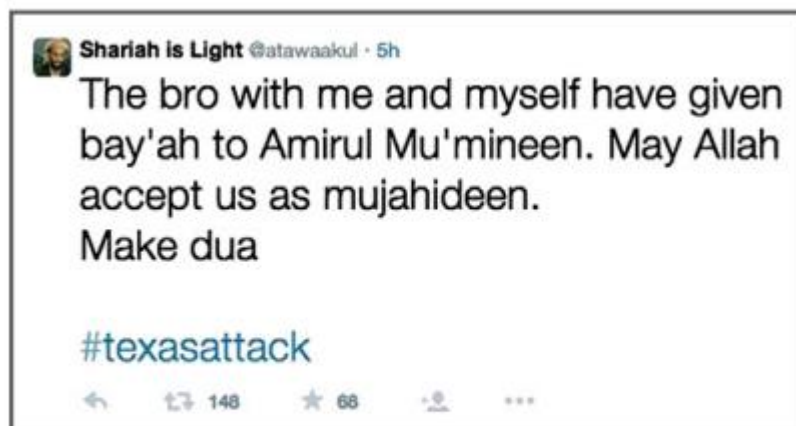
Figura C: fuente The Wilson Center



**Figura D,E,F,G:** Vidino, L., & Hughes, S. (2015). *ISIS in America: From Retweets to Raqqa*. Program on Extremism, George Washington University.

*Todos los tweets analizados en esta sección fueron extraídos del informe “ISIS in America: From Retweets to Raqqa”, elaborado por Lorenzo Vidino y Seamus Hughes y publicado en diciembre de 2015 por el Program on Extremism de la George Washington University.*

**Figura D:**



**FIG. 26** Elton Simpson pledges allegiance to ISIS before his attack.

**Figura E:**



**Figura F:**



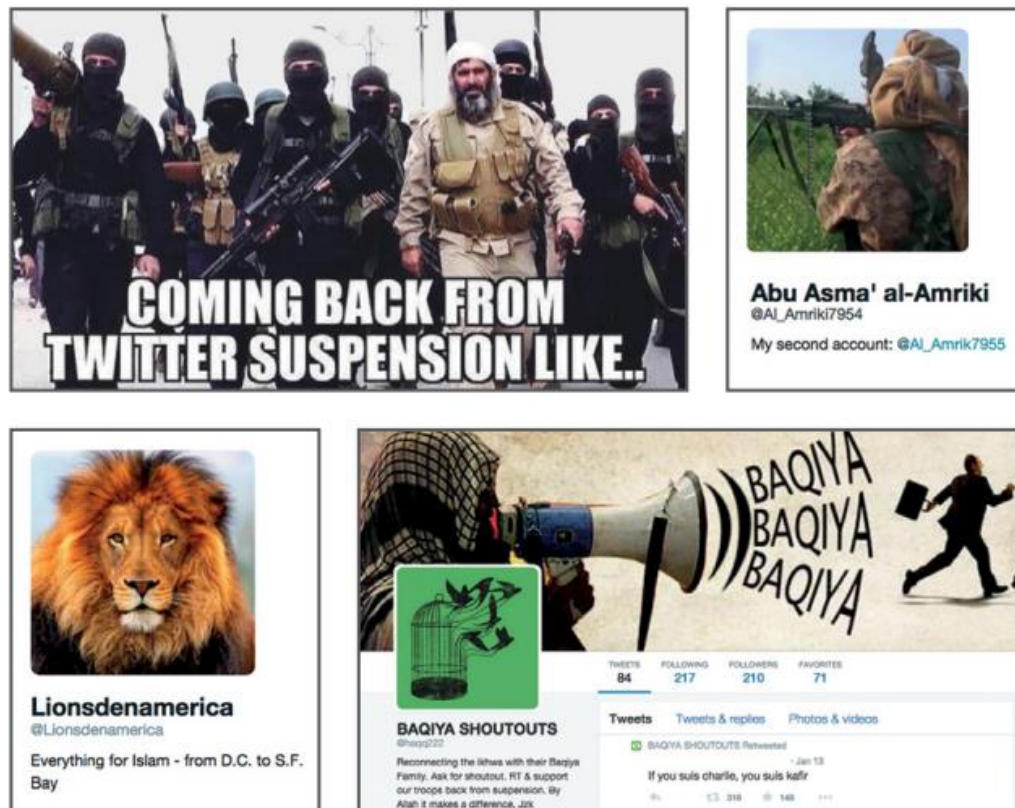
**Figura G:**



**FIG. 25** Mohammed Hamzah Khan on Twitter.

---

**Figura H:**



**FIG. 29** Clockwise: A user announces a new account; examples of node, shout-out, and amplifier accounts.