FACULTAD DE CIENCIAS HUMANAS Y SOCIALES

OSINT en la captación terrorista y la radicalización

Autor: Iñigo García Bello

Director: Francisco José López Rodríguez

Madrid

2023/2024

ÍNDICE

Introducción

El terrorismo se puede describir desde 2 enfoques: uno de ellos lo describiría desde el marco legal que trata de categorizar unos actos concretos como constitutivos de delito, mientras que el otro enfoque sería el que mantienen los investigadores y especialistas que, sin ser juristas, están ligados a la criminología y ciencias políticas (De la Corte y Jiménez, 2022).

Actualmente, la situación respecto al terrorismo es que convive con nosotros día a día. Cada vez se vuelve más habitual ver en los medios de comunicación noticias que nos informan de atentados llevados a cabo a pesar de las actuaciones de las Fuerzas y Cuerpos de Seguridad para tratar de evitarlos a toda costa (Ramos, 2017).

Habitualmente, estos actos siguen una serie de objetivos políticos y/o religiosos. Dentro del terrorismo llamamos extremismo al empleo de la violencia para la consecución de esos fines, pero el proceso desde el establecimiento de objetivos hasta el uso de la fuerza y la violencia es lo que se conoce como la radicalización (Moyano, 2019). Esto no es un proceso instantáneo, sino que se construye lentamente y puede llegar a adoptar diferentes grados o niveles (Moyano y Trujillo, 2013; Taylor y Horgan, 2006; Trujillo y Moyano, 2018).

En el mundo conviven aproximadamente 8 billones de personas, de las cuales casi 5,5 millones tienen acceso a un teléfono móvil y por tanto a las redes sociales en las que publicar información sobre sus vidas. Esto supone un volumen ingente de datos de cualquier índole (Mañé, 2023).

Puesto que es tal la cantidad de información, es imposible trabajar con toda ella. Por tanto, es importante que se filtre e interpreten los datos para así reducir considerablemente la complejidad de los procesos y optimizar los resultados dentro de una organización. Por esta razón, se empezó a usar la metodología OSINT (*Open Source Intelligence* o Inteligencia de Fuentes Abiertas), la cual se emplea en numerosos ámbitos del trabajo para obtener información de gran valor y trabajarla de manera más sencilla (OSINT: qué es y técnicas más usadas, 2022).

OSINT compone una modalidad de investigación en la que se aprovechan las diversas fuentes de información de dominio público con el fin de obtener información suficiente sobre un objetivo, por lo que se las puede considerar como herramienta de ciberseguridad. Los constantes avances en la tecnologías, propician que cada vez exista una mayor cantidad de

información que la gente publica en sus redes sociales, produciendo un flujo de información masivo y que se encuentra al alcance de cualquier persona (Redacción Keepcoding, 2023).

El punto de unión entre el terrorismo y las herramientas OSINT es el empleo de las mismas por parte de los grupos criminales con fines propagandísticos y de obtención de información sobre perfiles de potenciales miembros. Las constantes y novedosas aplicaciones de mensajería, permiten que personas con intereses similares se conozcan y estén en contacto fácilmente (De la Corte y Jiménez, 2022). Esto hace que en las personas más conservadoras y prudentes a la hora de expresar su opinión, se puedan acelerar procesos de consolidación de opiniones como las extremistas (Sunstein, 2009).

De modo similar, internet se ha convertido en una escuela para los terroristas quienes lo aprovechan tanto como medio de instrucción a través de vídeos explicativos, como herramienta de aprendizaje para fabricar armas o preparar futuros atentados (De la Corte y Jiménez, 2022). Además del reclutamiento y la propaganda, son múltiples los usos que le dan las organizaciones terroristas a las herramientas OSINT: medio para obtener financiación, entrenamiento, comunicación, coordinación, etc. (Sánchez, 2018).

Cuando nos hablan de terrorismo solemos imaginarnos únicamente los escenarios en los que personas armadas atacan a otras, individuos que se inmolan o explosiones. Sin embargo, el terrorismo ni se reduce a estos actos ni empieza con ellos. Esta es solo la cara visible de una conducta que se viene formando tiempo atrás. Para que el terrorismo tenga lugar, tiene que haber gente dispuesta a participar en él y es aquí donde entran en juego los captadores de las diferentes células u organizaciones terroristas, quienes juegan un papel fundamental en la obtención de información sobre perfiles potenciales, adoctrinamiento y propaganda.

Los reclutadores terroristas buscan obtener la información a través de todas aquellas fuentes de información que tenemos desprotegidas como pueda ser una revista, una persona o nuestras redes sociales mismamente. Por este motivo, las agencias de inteligencia y los gobiernos se hacen eco de los avances en tecnología que se producen constantemente para poder aprovechar estas fuentes de información y así prevenir la radicalización.

Los objetivos que se persiguen a través de este trabajo son poner el foco en las OSINT y tratar de explicar qué son y en qué consisten estas fuentes de información, haciendo hincapié

en la importancia en el tratamiento y el cuidado de la información personal. Asimismo se tratará de exponer de qué forma se aprovechan los grupos terroristas de las nuevas tecnologías para la obtención de datos e información con el objetivo de captación de nuevos miembros, propaganda y/u otras actividades ilícitas. También buscaré demostrar cómo los servicios de inteligencia de los diferentes países pueden hacer uso de las OSINT como una herramienta de prevención y en casos en los que no ha sido posible prevenir una amenaza, usarlas como forma de defensa y finalmente aplicar el conocimiento expuesto en el presente trabajo, remarcando cómo ha intervenido en 2 casos reales de terrorismo.

OSINT

¿Qué Son?

Al término OSINT se le puede conocer de diversas formas: inteligencia de código abierto, inteligencia de fuentes abiertas, fuentes abiertas de información, etc. pero todas comparten en común una definición. Suponen todo proceso de obtención de información de manera lícita a partir de fuentes públicas y gratuitas (Parekh, 2021). Dicha información se recolecta, ordena y analiza para así ofrecer una forma de inteligencia de gran valor y que sirva para resaltar las tendencias, oportunidades existentes y problemas potenciales (Arimetics, s. f.).

Las herramientas OSINT consisten en un proceso compuesto de diversas fases con el objetivo de organizar la labor de los investigadores para que se pueda facilitar así su trabajo. Las fases de las que se compone, serían las siguientes (Fonte, 2021):

a) Requisitos. Consiste en la elaboración de las metas que se pretenden lograr. Hay que cuestionar cuál es el problema que queremos resolver, en cuánto tiempo, qué necesitamos, etc.
b) Identificación de las fuentes de información. Se van a seleccionar aquellos recursos que nos puedan proporcionar una información valiosa. Al mismo tiempo se va a describir la metodología que se empleará para obtener los datos, así como definir y clasificar el grado de fiabilidad y disponibilidad de las fuentes de información.
c) Adquisición. En esta fase se produce la obtención de la información que buscamos. Sin embargo, a pesar de que a mayor cantidad de información obtenida, mayor información disponible*;* hay que tener cuidado con la sobrecarga de información porque habrá que analizarla posteriormente para así descartar aquella información que no es útil para el trabajo. Esta etapa, siempre se deberá realizar dentro de un marco legal, para asegurarse de que la información no se pueda invalidar.

d) Procesamiento. Se le da forma a los datos obtenidos en la fase anterior, para usarla posteriormente.
e) Análisis. Consiste en la producción de inteligencia a partir de la información, creando enlaces entre los diferentes datos para poder extraer conclusiones. Para ello, en primer lugar se eliminará toda la información inservible, en base a los criterios establecidos en las primeras fases.
f) Creación de inteligencia. Se elabora la información con un formato que permita su fácil comprensión, mediante el uso de gráficas, tablas u otras formas visuales de presentar la información obtenida.

No obstante, las fuentes abiertas de obtención de información no se reducen únicamente a la búsqueda a través de navegadores o motores de búsqueda. A su vez existen otras ramas de inteligencia dedicadas a la obtención de información (Galindo, 2018):

- SOCMINT (Social Media Intelligence): Inteligencia a partir de las redes sociales.
- SIGNIT (Signals Intelligence): Inteligencia generada a través de la interceptación de señales.
- GEOINT (Geospatial Intelligence): Inteligencia obtenida de la geolocalización.
- HUMINT (Human Intelligence): Inteligencia que se adquiere mediante la interacción de 2 o más individuos a través de diversos medios de comunicación.
- Otras disciplinas son ELINT (Electronic Intelligence), FININT (Financial Intelligence), IMINT (Imaginary Intelligence) o COMINT (Communication Intelligence).

A continuación en el siguiente apartado se verán con más detalle 2 de las principales disciplinas de la obtención de datos de código abierto: HUMINT y SOCMINT.

HUMINT Y SOCMINT

Actualmente, las redes sociales son una de las principales fuentes proveedoras de información, si no la que más, para cualquier tipo de organización (gubernamental, policial, empresarial, etc.). Por ello en los últimos tiempos ha experimentado un enorme auge la disciplina de SOCMINT (Social Media Intelligence). En un primer momento se denominó como SOCINT, aunque a día de hoy este término se emplea más para la Inteligencia generada a partir de la sociedad y la cultura. Dentro de la metodología SOCMINT se podrían diferenciar dos subtipos (Díaz-Canaleja, 2019; LISA Institute, s. f.):

- Social Media Analysis (SMA). Dirigida a la obtención de cualquier tipo de material a partir de las reces sociales.
- Social Network Analysis (SNA). Se centra en el análisis de los dato obtenidos en la SMA.

De manera general, la inteligencia de las redes sociales se dedica a realizar una escucha activa sobre los usuarios de las diferentes aplicaciones acerca de personas de relevante interés, marcas comerciales o algún producto o servicio. Posteriormente, se buscará tratar esos datos obtenidos para darles un valor y significado relevantes con el que posteriormente tomar decisiones. Esto se consigue mediante el análisis de nuestras preferencias y el uso que damos a nuestras redes sociales, para poder crear un perfil de cada consumidor. Sin embargo, para poder llevar a cabo esta tarea, se necesita gente que esté formada en OSINT y en el análisis de Inteligencia, al igual que en las herramientas requeridas para el desempeño de su trabajo (LISA Institute, s. f.).

Al igual que la metodología OSINT, en las SOCMINT también se cuenta con una serie de fases que componen todo el proceso (LISA Institute, s. f.):

a) Planificación. Se van a fijar las informaciones que se buscan y los objetivos perseguidos que motivan el uso de estas herramientas. También se debe planificar unas fechas límite y una metodología a seguir.
b) Investigación y monitorización. Se hace uso de la actividad de los usuarios en las redes sociales y analizándolo, para localizar un nicho de mercado en el que cubrir unas necesidades de grupo.
c) Análisis. Cuando contamos con todos los datos recopilados, los procesaremos para alcanzar los objetivos marcados.
d) Toma de decisiones e innovación. Cuando se ha dado un significado a la información obtenida, se tomarán decisiones sobre el mejor curso de acción posible. En esta fase también se debe realizar una revisión del proceso al completo e incluso, si fuese necesario, corregir alguno de los pasos.

¿Cómo Y Por Qué Surgen?

Las primeras apariciones que constan de tecnologías OSINT, datan de principios de 1940. Por aquel entonces, El Servicio de Monitoreo de Transmisiones Extranjeras (FBMS) se encargaba de controlar y analizar las transmisiones provenientes de países extranjeros o provenientes del interior del país con dirección a otro del extranjero, buscando cualquier indicio

de actividad sospechosa. El actual término de inteligencia de código abierto (OSINT) se empleó 40 años después por el ejército estadounidense. Trataron de explicar que las fuentes de información no debían ser estáticas, sino que tenían que aprovecharse técnicas diferentes para alcanzar la victoria en el campo de batalla. En el 2004, 3 años después de los ataques del 11-S, Estados Unidos contrató los servicios de una agencia de inteligencia de fuentes abiertas, lo que motivó a los diferentes gobiernos a incorporar la suya propia (Parekh, 2021).

Beneficios

Algunos de los efectos positivos que conllevan el uso de las fuentes abiertas de Inteligencia son los siguientes (Arimetics, s. f.):

- Accesibilidad. La información pública es de libre y gratuito acceso, por lo que cualquier persona puede acceder a ella.
- Velocidad y eficiencia. Gracias a los avances tecnológicos, buscar y obtener información de cualquier tipo se produce de manera casi instantánea. Es por ello, que en situaciones donde la rapidez de los actos es vital, las herramientas OSINT son muy útiles.
- Cobertura global. Se puede obtener información de cualquier parte del mundo a través de los recursos OSINT.
- Amplia gama de aplicaciones. Se puede emplear en múltiples ámbitos.

¿De Dónde Se Puede Obtener Información?

Son muchas las fuentes de origen de la cuáles podemos obtener inteligencia de código abierto. No obstante, se pueden agrupar en 9 categorías (Arimetics, s. f.; Gonzalo, 2022; Parekh, 2021):

1. Internet. En este grupo se incluyen las redes sociales (Instagram, Facebook, Linkedin, etc.), foros, blogs o publicaciones en línea. Dado a la gran cantidad de posibilidades de las que se pueden obtener información, es la categoría más amplia.
2. Motores de búsqueda. Como pueden ser Google, Bing o Yahoo.
3. Medios de comunicación. Revistas, periódicos, televisión o radio provenientes de cualquier zona del mundo.
4. Archivos públicos. Podemos obtener información de informes, presupuestos o registros de las diferentes instituciones públicas.
5. Personas. A pesar de que esta categoría se puede englobar dentro de muchas de las demás categorías, existe la posibilidad de obtener información proveniente de la interacción con otra persona de manera física.

6. Publicaciones profesionales y académicas. Son las revistas y artículos académicos.
7. Datos de sensores. Son aquellos que se pueden obtener de dispositivos de seguridad (cámaras) o de localización (GPS o satélites) que recogen información de manera constante.
8. Literatura gris. Dentro de esta categoría se encuentran los elementos de más complejo acceso, al emplearse vías de transmisión de la información poco habituales. Puede tratarse de informes técnicos y patentes.
9. Datos comerciales. Imágenes y bases de datos comerciales.

¿Qué Fines Lícitos Puede Tener?

Empresa

En el entorno empresarial las herramientas OSINT tienen una gran repercusión. Cada vez son más las organizaciones que intentan mostrarse tal y como son al público, de manera que se pueda conocer cuáles son los servicios y productos que ofrecen. Algunas de las tecnologías que posibilitan el acceso a la información relacionada a una empresa son Maltego, Shodan, The Harvester o Tineye:

- Maltego: herramienta gráfica de análisis de enlaces que describe varias relaciones en línea.
- Shodan: un motor de búsqueda para dispositivos conectados a Internet.
- The Harvester: una herramienta que se utiliza para obtener correo electrónico e información relacionada con el dominio fuera de una organización.
- Tineye: una herramienta que se utiliza para identificar si una imagen está disponible gratuitamente en línea. (Parekh, 2021).

Igualmente, los recursos OSINT en el mundo de las empresas, también se pueden emplear para el análisis de riesgo y de mercados. Los trabajadores, a partir de la información pública obtenida pueden ver cuáles son las vulnerabilidades de la organización o aquellos potenciales objetivos de un ataque. Al mismo tiempo, puede servir como una herramienta de evolución, desarrollo y mejora. Es decir, una empresa aprovecha estas tecnologías para investigar sobre la actividad de competidores con el objetivo de mejorar un servicio o un producto, así como mejorar en al logística a la hora de tomar decisiones y planificación (Arimetics, s. f.).

Gobiernos

Los gobiernos de los diferentes países pueden darle diferentes usos a las tecnologías OSINT, en función de los objetivos que se buscan alcanzar. Entre sus principales objetivos están el poder garantizar la seguridad de la ciudadanía y asegurar el correcto funcionamiento de la nación (Parekh, 2021).

Dirigir la desinformación. En una sociedad tan influenciada por lo que se publica y consecuentemente se viraliza en las redes sociales, es fundamental poder asegurarse de que la información que se transmite sea correcta y no de lugar a equívocos o confusiones. Si esto no se pudiese controlar, nos encontraríamos en un escenario de desinformación, en el que las personas podrían fingir ser otras, emitir *fake news* o propagar información ilegítima. Estas informaciones incorrectas posibilitan que las correspondientes autoridades del gobierno traten de solucionar los problemas de la manera más rápida posible (Parekh, 2021).

Seguridad en el transporte. Los medios de transporte son globalmente conocidos como uno de los epicentros de problemas en la gestión de una ciudad o incluso de un país. Si las infraestructuras que posibilitan la movilidad o el transporte se ven en riesgo, se pueden producir diversos incidentes. Las diferentes unidades del gobierno que se encargan del correcto funcionamiento del transporte, también emplean OSINT como forma de prevención y coordinación de respuestas en caso de incidentes. Asimismo, la información pública sirve como método de advertencia para amenazas en medios de transporte (Parekh, 2021).

Hacer frente a las crisis nacionales. A pesar de ser poco frecuente, los incidentes a nivel nacional y, en ciertas ocasiones, a nivel global, pueden presentarse de diversas formas. Es por esto, que es esencial que las agencias de inteligencia de los diferentes países cuenten con todos los datos posibles. De esta manera, se facilita el conocimiento de los elementos críticos y las formas de respuesta llevadas a cabo por otros países (Parekh, 2021).

Seguridad nacional

Las tecnologías OSINT también se utilizan para identificar e impedir amenazas internas o externas, para así generar perfiles de individuos o grupos que puedan suponer un riesgo. Dentro de la seguridad nacional, las herramientas de código abierto se suelen emplear para la lucha contra el terrorismo o para la ciberseguridad (Arimetics, s. f.).

En el caso del primero, las amenazas terroristas se producen de manera nacional e internacional y las llevan a cabo células terroristas independientemente del tamaño que tengan. La lucha antiterrorista que se lleva a cabo, se produce a través de los espacios en línea o plataformas de redes sociales que sirven como elemento de comunicación y propaganda entre diferentes movimientos terroristas. No obstante y a pesar de que las tecnologías OSINT son de libre acceso, eso no quiere decir que sean de fácil acceso. Es decir, los grupos terroristas usan dichas plataformas de comunicación a las que podemos acceder sencillamente, pero con un lenguaje codificado haciendo más ardua la labor de los investigadores (Parekh, 2021).

En el segundo de los casos, el de la ciberseguridad, los ataques pueden ser llevados a cabo por individuos solitarios o por organizaciones delictivas. Sus ataques suelen ser sinónimo de peligros financieros y políticos. El uso de estas herramientas permite responder de manera eficaz ante ataques que comprometen la seguridad de los datos de los ciudadanos (Parekh, 2021).

Investigación criminal

En las investigaciones criminales de las Fuerzas y Cuerpos de Seguridad del Estado, se ha visto que el empleo de las OSINT son de gran ayuda, puesto que sirven para recabar información sobre los posibles sospechosos que existen en una investigación y establecer relaciones entre ellos o descubrir nuevas pesquisas que pudieran pasar desapercibidas o que no eran conocidas. Las tecnologías OSINT, también se las puede asociar a las investigaciones en fraudes. Concretamente para detectar actividades fraudulentas y por consiguiente delictivas (Arimetics, s. f.).

Búsqueda de personas y seguimiento: los influencers

De manera concreta, las tecnologías SOCMINT sirven de herramienta a las marcas que tratan de promocionar un producto y buscan una figura conocida que les ayude en la promoción. Por tanto, también pueden funcionar como herramienta de marketing. Otro de los usos que se le puede dar a las SOCMINT, en relación al marketing, es el seguimiento del impacto que genera en los consumidores un producto y su publicidad a través de las redes sociales (LISA Institute, s. f.; OSINT: qué es y técnicas más usadas, 2022).

Terrorismo Radical

El terrorismo yihadista ha sido capaz de aprovechar los avances tecnológicos para incorporarlos a sus actividades. Esta adaptación no se ha producido de manera inmediata, sino que es el fruto de muchos años. Klaussen et al. (2021) han distinguido y dividido este proceso en 4 etapas:

- La primera de ellas se produce en los años 80 con la divulgación por parte de líderes terroristas de sermones en forma de textos escritos, con la ayuda de medios audiovisuales que facilitaban su propagación.
- La segunda fase tendría lugar a mediados de los años 90 cuando aparecen las denominadas "webs verticales". Es decir, páginas web que están totalmente controladas por personas relacionadas con grupos yihadistas que ordenaban lo que se debía publicar.
- La tercera sería a principios del 2000 cuando el surgimiento de los foros permitió que los consumidores publicasen contenido relacionado con la yihad.
- Finalmente, la cuarta etapa se inicia en el 2007 con la aparición de las redes sociales que suponen las principales y más importantes fuentes de difusión de la información.

El terrorismo más radical busca con su actividad en la red lograr determinados objetivos. Como hemos mencionado anteriormente, uno de ellos es el reclutamiento de nuevos integrantes. Gran parte de la propaganda que se distribuye, pretende atraer a nuevas personas que quieran formar parte de las organizaciones terroristas. Para ello, se dirigen a objetivos que son vulnerables por distintas razones (marginación, humillación, injusticias, etc.). En función de la edad, adaptan su mensaje con dibujos animados o juegos de ordenador en el caso de que los usuarios sean menores de edad. Estas formas de divulgación, hacen que la tarea de investigación por parte de las agencias gubernamentales se complique. Además, cada vez se busca más embaucar a mujeres jóvenes, ya que se considera que puedan servir como gran objeto de reclamo para atraer a más hombres (Gerwehr, 2006; Lejarza, 2015; Weimann, 2014).

Otro de los objetivos es el de la incitación, con el que se busca animarles a cometer los actos y defender la causa. El problema para los Estados es que es muy difícil delimitar lo que se considera incitación. Esto hace que la justificación de la prevención de ataques terroristas, sea suficiente para limitar la libertad de expresión (Pacto Internacional de Derechos Civiles y Político, 1966, artículo 19; Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, 2008; Lejarza, 2015; Weimann, 2014).

La radicalización sería el tercero de los objetivos que buscan, ya que es todo proceso que busca convertir a los individuos en fieles guerreros para su causa bajo el lema de una ideología terrorista (Lejarza, 2015; Weimann, 2014).

La Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC), añadió 3 objetivos que también perseguían las organizaciones terroristas a través de Internet. Estos son la propaganda, adiestramiento y la planificación. Vamos a verlos un poco más en profundidad:

- Propaganda. A través de publicaciones en diferentes formatos, se ofrece a los usuarios explicaciones ideológicas de los hechos cometidos por otros individuos. Para el 2010, el número de webs dedicadas a la propaganda era superior a los 10 mil. Desde entonces el nivel de complejidad de estos sitios webs ha ido aumentando, haciendo que se vuelvan más seguras para continuar con el envío de información. Esto es un reto para las agencias gubernamentales y los gobiernos, puesto que supone que se debe distinguir entre lo que es propaganda de la comunicación de una mera opinión (Arquilla, y Ronfeldt, 2001, Sánchez, 2010; Sánchez, 2015; UNODC, 2013).
- Adiestramiento. Internet sirve como un campamento que ayuda a los nuevos individuos a formarse y prepararse para cuando sean llamados para perpetuar un ataque. A través de webs, vídeos o manuales; aprenden a fabricar bombas o a manejar fusiles, pistolas u otras armas de fuego. Otros aprendizajes que adquieren están relacionados con las tácticas y la estrategia a la hora de llevar a cabo un ataque (Morán, 2017; UNODC, 2013; Weimann, 2014).
- Planificación. Muchas veces los individuos no se conocen entre ellos, por lo que el uso de Internet facilita que puedan comunicarse la estrategia que deben seguir para ejecutar un atentado (UNODC, 2014).

Captación, Adoctrinamiento Y Radicalización

Como comentaba en apartados anteriores, la labor del adoctrinamiento se ha visto favorecida por los avances en comunicación existentes. Además, la explosión de las redes sociales, permite a las organizaciones obtener una gran cantidad de información sobre posibles objetivos y sobre potenciales miembros (Conesa et al., 2016; Moliner et al., 2018).

La radicalización supone el proceso de incorporación y expresión de un conjunto de creencias haciendo uso de la violencia para alcanzar un objetivo concreto. Por ello, internet se

podría considerar en sí mismo un medio de radicalización (Jordán, 2009, Van Stekelenburg et al., 2010).

El Departamento de Policía de Nueva York utiliza un modelo para dar respuesta a cómo se produce la radicalización de individuos con intereses salafistas. Para ello se distinguen 4 fases, aunque el hecho de haber pasado por ellos no significa que se vaya a cometer un atentado. Estas fases son (Christmann, 2012; Madriaza & Ponsot, 2015; Silber y Bhatt, 2007):

a. Pre-radicalización. El individuo se muestra receptivo a ideologías diferentes a la suya sin que se produzcan cambios en su vida normal.
b. Auto identificación. El individuo comienza a dejar de lado su vida habitual guiado por una persona externa.
c. Indoctrinamiento. El sujeto acoge la nueva ideología y se involucra en ella. Esta fase es fácil de identificar porque suelen dejar sus actividades rutinarias cuando acuden a la mezquita y por la interpretación y sentido que da a su día a día y lo que ocurre en él.
d. Yihadización. El sujeto se percibe como *muyahidín* y toma decisiones como marcharse a Oriente a formarse de manera militar, confecciona ataques y los lleva a cabo.

De las diferentes fuentes abiertas que existen, las fuentes humanas (HUMINT) juegan un papel muy importante. Se dedican a vigilar y monitorizar a determinados individuos que son vulnerables y de fácil captación. Para ello se puede aprovechar la confianza que se genera en la persona o por la influencia previa sobre esa persona al ser alguien de referencia para el individuo (Orav, 2015).

Lograr que el sujeto pierda esa identidad que poseía y adopte una nueva, no es tarea fácil. Para ello, se suelen usar diferentes formas de manipulación como el aislamiento de su círculo habitual. Para las mujeres, es habitual que deliberadamente y sin presión abandonen su vida al verse atacadas por sus allegados por haber adoptado una nueva perspectiva. Los grupos aprovechan estas situaciones de vulnerabilidad para hacer hincapié en el drama que viven. Además, la búsqueda de información en internet hace que los algoritmos indirectamente presionen a la persona al mostrarle solo información al individuo sobre el tema buscado. No obstante, no resulta infrecuente que se recurra a otro método de control efectivo como es el miedo (Trujillo et al., 2018).

Radicalización no es lo mismo que el reclutamiento. El primero de los términos se refiere a la apertura a nuevas ideas y opiniones que de manera potencial podrían llevar al individuo a cometer un ataque terrorista. Por su parte el reclutamiento es la iniciativa de una persona que ya está radicalizada a cometer el acto terrorista (Litmanovitz et al., 2017). Es por ello que hay que entender que no todo individuo que se acerca a grupos terroristas va a cometer un ataque, pero si todo aquel que ha perpetuado un ataque, ha sido radicalizado previamente (International Centre for Counter-Terrorism, 2016; Neumann, 2013; Litmanovitz et al., 2017).

La radicalización se puede entender desde tres puntos de vista o niveles: micro, meso y macro. En el nivel micro encontramos una serie de factores que explican los comportamientos de carácter político. Dichos factores son los elementos racionales, los emocionales, los normativos y los identitarios. Estos elementos fortalecen la radicalización, pero no hacen que sea irreversible. Es decir, no siempre va a llegar a producirse la radicalización, porque se puede estancar en algún momento del proceso (Jordán, 2009, Marín, 2004).

En el nivel meso se encuentran las redes sociales, que suponen factores exógenos a la persona pero que son de alcance inmediato. De Federico (2002) dice que dichas redes pueden ser:

- Redes de amistad y parentesco. En terrorismo, tienen el mismo valor las relaciones entre iguales que las parentales. De hecho, una relación de amistad puede ser hasta más importante para la radicalización. El motivo puede ser que desde el principio buscaba su captación o porque en un grupo puede haber alguien cercano al yihadismo y que arrastre a los demás (Federico de la Rúa, 2004; Silber y Bhatt, 2007).
- Comunidades virtuales en internet. La participación en foros y chats virtuales, suscribirse a canales de difusión, etc. son los pilares para la construcción de una identidad acorde a la cultura yihadista (Hoffman, 2006; Ulph, 2005).
- Redes sociales vinculadas a la predicación radical. Dentro de los foros y canales de difusión pueden surgir amistades y lazos afectivos que refuercen la ideología radical (Jordán, 2009).
- Redes sociales en prisiones. Las prisiones es uno de los núcleos que más se tratan de controlar por su fuerte papel en la captación y difusión de mensajes yihadistas. Encontrar gente de la misma nacionalidad o con valores culturales compartidos hace que se convierta en una herramienta de gran utilidad para la captación (Jordán, 2009).

El último de los niveles, el macro, son los factores exógenos generales como pueden ser su entorno económico, social, político y cultural; en el que se encuentra el individuo (de la Corte y Jordán, 2007).

Propaganda

Es evidente que internet ha contribuido a que el mensaje salafista pueda llegar con mayor facilidad a cualquier usuario sin que éste tenga que depender del criterio de decisión por parte de los medios de comunicación a la hora de determinar lo que deben contar y lo que no. Además, con las diversas herramientas en línea existentes, prácticamente cualquier persona puede producir contenido propagandístico (Ulph, 2005).

Las redes sociales son un instrumento de propaganda instantánea y con un alcance inimaginable, que ofrecen la posibilidad de actuar de manera anónima. Los motivos por los que los grupos terroristas optan por ellas son porque suponen un medio económico de publicación de contenido, son de fácil acceso, no hay controles de publicaciones, los mensajes llegan a prácticamente todo el mundo y su inmediatez (Lejarza, 2015).

Al Qaeda e ISIS son algunos de los grupos que más uso hacen de las redes sociales. El primero, conocido por su antiguo líder Osama Bin Laden, lleva aproximadamente 20 años compartiendo contenido en internet. Por su parte el ISIS opta más por las redes sociales. Otros grupos como Hamas, Hezbolá o el Frente al-Nusra tienen mucha actividad en Twitter (Lejarza, 2015).

Shane Shook (2014) constata que el uso que el ISIS le da a las redes sociales es para generar terror a través de 3 formas:

- Creación de hashtags y apropiándose de aquellos que estén siendo de gran relevancia.
- Usando monitores por control remoto que compliquen las labores de búsqueda por parte de las agencias.
- El uso de apps propias para comunicarse entre ellos y suplantar la identidad de usuarios de otras redes sociales haciendo publicaciones en su nombre.

Ventajas E Inconvenientes

Ventajas

Las principales ventajas que supone el uso de las fuentes abiertas son su baja complejidad, su fácil difusión y su fiabilidad, que es más difícil que sea manipulada la información por terceros (Jordán, 2016). Asimismo, se trata de una herramienta muy amplia que permite obtener información de manera inmediata y de diferentes orígenes. Los costes de obtener la información son calificados como bajos y rentables, teniendo en cuanta el volumen de datos que se pueden obtener. Finalmente, todo el material obtenido, no tiene inconvenientes jurídicos, ya que al tratarse de una fuente abierta toda la información es de origen legal (Hwang et al., 2022).

Respecto a las ventajas particulares de las diferentes formas de inteligencia de fuentes abiertas, en las HUMINT encontramos 2 principales ventajas que surgen de su utilización (Jordán, 2016): que proporciona información que es realmente difícil de obtener por otros medios y que pueden aprovecharse para engañar o dar falsa información a enemigos.

A pesar de no ser un número abrumador de ventajas, su valor es incalculable si se tiene en cuenta el punto desde el que partían la s agencias de inteligencia hace 50 años mismamente.

Inconvenientes

Sin embargo, también existen algunos inconvenientes o limitaciones de hacer uso de este tipo de inteligencia. Dichos inconvenientes son (Jordán, 2016):

- Obtener información a través de una fuente humana requiere de tiempo que en ocasiones no se dispone y proximidad física con esa persona, pudiendo hacer que corra peligro la integridad de la fuente o se desencadene un conflicto diplomático.
- Las comunicaciones entre la fuente y los controladores no suelen producirse de manera inmediata.
- La fuente puede modificar la información por motivos internos o externos.
- Existe un enorme volumen de información que se debe analizar y requiere de mucho tiempo.
- En ocasiones la información se debe completar con otra proveniente de diversas fuentes o contrastarla para asegurarse de la fiabilidad.
- A pesar de que no es un medio de obtención de información caro, tampoco resulta económico ya que conlleva un gasto constante.

Uso De OSINT Como Forma De Defensa

Actualmente, entre el 80 y el 90% de la información de inteligencia que está en poder de los gobiernos, procede de fuentes abiertas de obtención de información. Los gobiernos de los diferentes países cada vez hacen más uso de la información obtenible a través del ciberespacio a través de intrusiones en diversos servidores para así acceder al material que se pretende buscar y del que se quiere obtener la información. Esto supone que o bien se obtenga información o que se elimine aquella que esté en posesión de un país enemigo (Rettman, 2011; Sánchez 2018).

Los medios utilizados por las agencias y Fuerzas de Seguridad de los Estados no son públicas por la posible amenaza que supondría si otro país pudiese acceder a ella. En el caso de España, existen diversas organizaciones que colaboran para hacer frente a las amenazas. Algunas de ellas son el CNPIC, el CERT o el CCN-CERT. Estos hacen uso de SOCMINT para, a través de la información proveniente de las publicaciones en redes sociales y la monitorización de la actividad en ellas; producir un contenido de inteligencia que sea de utilidad (Ramos, 2017).

Como último recurso y acercándose al marco de lo ilícito, se podrían llegar a interceptar telecomunicaciones ya que en el artículo 55.2 de la Constitución se limita el secreto de las comunicaciones a las bandas armadas o terroristas (Ramos, 2017).

De cara a la lucha antiterrorista, Frank Gregory (2005) afirma que por parte de las agencias de Inteligencia existen 2 pilares fundamentales en los que se basan sus actuaciones:

- Función preventiva de la actividad terrorista. Se analizan los elementos que potencian las amenazas, con el objetivo de neutralizarlos.
- Función de investigación tras la comisión de la acción. Supone el análisis y acumulación de conocimientos y contenidos que ayuden a la lucha antiterrorista en futuras ocasiones.

Análisis De Casos

Para este apartado vamos a ver cómo las distintas técnicas y usos mencionados de las OSINT han sido empleados en casos de ataques terroristas de gran relevancia mediática en nuestro país. Los casos seleccionados para el análisis son el ataque de Las Ramblas y Cambrils en el 2017 y el ataque del 11-M en Madrid. Estos 2 ataques muestran cómo se produjo la radicalización de algunos integrantes a través de internet, en la mezquita o en las prisiones; el

adiestramiento a través de material audiovisual y de manuales distribuidos a través de internet y la captación mediante el seguimiento de las redes sociales. Para cada uno de los casos, se va a ir describiendo el suceso que tuvo lugar y señalando qué procedimientos OSINT usaron los terroristas.

Caso Barcelona

El 17 de agosto del 2017 se produjeron 2 ataques terroristas en Barcelona. El primero de ellos tuvo lugar sobre las 17 horas en la zona de la Rambla, donde un individuo condujo una furgoneta por una zona peatonal atropellando a decenas de víctimas. La ejecución de este ataque es el resultado de un proceso que se inicia años antes con la actividad de captación y adoctrinamiento realizada por un imán de en Cataluña. Su principal actividad la realizaba en las mezquitas donde observaba a los sujetos más grandes y que se mostraban más descontentos con la vida en Occidente y con ciertos intereses por la actividad terrorista. El imán detectaba en ellos la ausencia de identidad y lo que les ofrecía era la posibilidad de desarrollar una identidad nueva de la mano de la yihad. Para radicalizar a los jóvenes empleaba vídeos de niños entrenando de manera militar, torturas y ejecuciones de civiles cristianos; tal y como comenta una persona conversa gracias a la acción de el imán (Campos y Fernández, 2022).

Previamente a acercarse a los jóvenes, el imán ya había realizado un seguimiento de las redes sociales de estos sujetos y filtraba entre aquellos que mostraban signos propios de una radicalización. A través de la manipulación y de una visión dicotómica del mundo en la que entendían como los buenos y los malos, lograban que estos chicos abrazasen la causa terrorista. Lo sorprendente es que el imán solamente se encargó de seleccionar a las 3 personas que se encargarían de seleccionar al resto de integrantes de la célula y que se convertirían en partícipes de los atentados. Durante 3 años estuvieron formando y compartiendo ideas extremistas a través de grupos. Tal y como se dice en el documental dirigido por Campos y Fernández (2022), el éxito de un grupo terrorista se basa en la cohesión interna y la confianza.

Una vez se les había convencido de unirse a la causa, comenzaba la etapa de adiestramiento. En ella se les proporcionaba manuales e información sobre la fabricación de granadas, chalecos explosivos y sobre logística para llevar a cabo los atentados. Al mismo tiempo, se demostró que habían consumido en los días previos una gran cantidad de material propagandístico para recordar la importancia de lo que iban a hacer. También se encontraron archivos de vídeo y audio en los que repiten el material de propaganda que habían consumido

y realizaban *nasheeds* (cantos musulmanes a capela con usos de propaganda terrorista) y gestos que reafirmaban la decisión que habían tomado y que significaban el paso previo a la comisión de un atentado como comenta en el documental el experto en terrorismo Manuel Torres Soriano (Campos y Fernández, 2022).

Caso Madrid

El 11 de marzo de 2004 tuvo lugar en Madrid el ataque terrorista más devastador en España y uno de los más graves de Europa. A primeras horas de la mañana, varios trenes distribuidos en diferentes puntos de la red ferroviaria de la ciudad sufrieron explosiones que se saldaron con 192 víctimas mortales y cerca de 2 mil personas heridas. De las 28 personas que se consideró como intervinientes en el atentado, 21 fueron condenados (RTVE, s. f.).

Uno de los líderes de la organización, Jamal Ahmidan, había sido radicalizado en la prisión anteriormente cuando cumplía condena por delitos previos (Jordán, 2009). Cuando el suceso se investigó, sirvió de aliciente para poner énfasis en la vigilancia y prevención de la captación y adoctrinamiento terrorista en el entorno penitenciario.

Simultáneamente, en las mezquitas también se llevó a cabo trabajos de propaganda. El considerado como líder de Al-Qaeda en nuestro país, Abu Dahdah, con ayuda de otros integrantes del grupo, repartieron material impreso en las mezquitas, buscando las reacciones de las personas para saber quiénes podían ser potenciales miembros de la célula (Jordán et al., 2006).

A pesar de que se desconoce si el reclutamiento de los individuos que perpetuaron el ataque se produjo a través de internet, si se tiene constancia de que durante varios meses estuvieron consultando contenido de propaganda terrorista a través de diversos dispositivos (Jordán y Torres, 2007).

Por otro lado, en las investigaciones policiales también se encontró que el principal uso que se le dio a internet fue para la reafirmación del pensamiento extremista y de la ideología en la que se basaba y para el adiestramiento en combate. Las pruebas obtenidas por los cuerpos policiales mostraron que los integrantes de la célula consumieron manuales operativos que les brindaban los conocimientos necesarios para la ejecución del ataque, imágenes de heridos en

Iraq por los ataques dirigidos de Bush y Aznar. Estas imágenes eran difundidas sobre todo por el grupo Al-Battar (Jordán y Torres, 2007; Vidino, 2006).

Discusión

Actualmente se cuenta con una extensa bibliografía relacionada con los usos terroristas de las metodologías OSINT, de la cuál nos podemos apropiar para analizar cuáles son los puntos débiles u objetivos susceptibles de ser atacados, tanto físicos como informáticos, y así protegerlos. Sin embargo, las fuentes de datos de las que obtener información acerca de cómo actúan los órganos de defensa de las naciones haciendo uso de OSINT, son limitados y están controlados en su mayoría por los Gobiernos o Agencias Gubernamentales.

Tal y como empezaba este trabajo, se planteaba un panorama actual en el que el terrorismo ya no se basa únicamente en el sostén de un arma y la muerte indiscriminada de civiles al mismo tiempo que se realiza una reivindicación política/religiosa. Ahora va ligado a un largo proceso en el que el uso de los avances más punteros en tecnología facilitan la ejecución de los ataques, permitiendo esconderse tras una máscara llamada internet.

Inevitablemente, cada vez son más los usuarios que se encuentran conectados a la red a través de un dispositivo electrónico e igualmente, cada vez es más corta la edad de acceso al primero. Por lo que es evidente que la tecnología va a seguir evolucionando y que el progreso no se va a detener ahora. De este modo, si con los avances más actuales se puede lograr acceder a cualquier fuente de información a través de un dispositivo conectado a la red y que genera y recibe millones y millones de datos; se vuelve estrictamente necesario ir un paso más allá con la confección de nuevas herramientas que permitan suprimir casi de manera inmediata toda aquella información que no sea relevante.

Por desgracia, la vara para medir la eficacia de los Cuerpos y Fuerzas de Seguridad del Estado, en cuanto a prevención de ataques terroristas se refiere, no siempre es objetiva. La realidad es que posiblemente el número de casos que conocemos porque han sido documentados a través de medios de comunicación, representa un porcentaje significativo pero no absoluto respecto al total de operaciones en las que se interviene y se logra impedir que alcancen sus objetivos. Lógicamente, estamos hablando de operaciones que en su mayoría son llevadas a cabo por los servicios de inteligencia de diferentes países y de las cuáles su conocimiento no está al alcance o no es de fácil acceso para la población general.

En todas ellas, las OSINT están presentes en cualquiera de las formas que se explicaron a lo largo de este trabajo. Su uso es fundamental para tratar de discriminar al información que

es falsa de la que puede resultar ser una potencial amenaza. El problema es el mencionado anteriormente: la masificación de datos. Es decir, el volumen de información disponible es tal, que es una tarea muy complicada filtrarla y tratarla con éxito, más aún cuando se actúa bajo la presión de una amenaza de atentado, los cuáles suelen ser inminentes. Es por ello que en un futuro es probable que se logren desarrollar nuevos sistemas o *softwares* informáticos que permitan un verificado o un mayor filtrado de la información antes de ser analizada por los agentes.

Si a esto se le suma que las personas jóvenes resultan más influenciables, que en un gran número de casos carecen de una personalidad completamente definida y que son propensos a realizar conductas de riesgo y a la exploración de nuevos contextos; se vuelven un objetivo claro para la captación y radicalización terrorista. Por tanto, sería aconsejable poder profundizar y destinar más recursos a la investigación acerca de los diferentes medios de captación en línea que se producen con el fin de evitarlos, ya que se sabe poco acerca del tema y lo que se sabe es de manera superficial. La mayoría de captaciones son chicos y chicas jóvenes que resultan manipulables fácilmente por sus historias personales. Una futura línea de investigación podría ser sobre el estudio y posterior análisis de variables demográficas e historias personales cargadas de eventos vitales negativos o de "injusticia" y su correlación con la captación terrorista. Con esto se buscaría localizar una serie de factores de riesgo y si existe una relación entre dichas variables con el hecho de ser más o menos influenciable como para adherirse a una célula terrorista. Con esto se buscaría obtener una muestra fiable y suficientemente representativa como para extrapolar estos datos a la población general.

Finalmente, se podría estudiar la posibilidad de controlar a través de servidores VPN la posibilidad de controlar el envío de cierto material propagandístico con contenido radical. El funcionamiento sería similar al de los servidores que controlan y regulan que unos canales de televisión o aplicaciones de reproducción de contenido puedan ser consumidos o utilizados en un país u otro.

Bibliografía

Alarcón Sánchez, R. (2022). Modernidad tecnológica y propaganda terrorista: propuesta de un análisis discursivo para enfrentar los mensajes del terrorismo en la era digital. *Revista Del Instituto Español De Estudios Estratégicos*, (18), 329–364. https://revista.ieee.es/article/view/4018

Allievi, S. (2003). Islam in the public space: social networks, media and neo-communities. In Allievi, S. y Nielsen, J. *Muslim Networks and Transnational Communities in and across Europe, 1*. (pp. 1-27). https://doi.org/10.1163/9789047401780_004

Arimetics. (s. f.). Qué es OSINT – Open Source Intelligence. Consultado el 14 de agosto de 2023. https://www.arimetrics.com/glosario-digital/osint-open-source-intelligence

Arquilla, J. y Ronfeldt, D. (2001). *Networks and Netwars: The Future of Terror, Crime and Militancy*. National Defense Research Institute. https://doi.org/10.7249/MR1382

Blanco, J. M. (2011, 7 de septiembre). Seguridad e inteligencia 10 años después del 11-S. https://www.ieee.es/temas/inteligencia/2011/DIEEEM09-2011.html

Bonilla, D. N. (2004, 29 de junio). *Estudios sobre Inteligencia: Fundamentos para la Seguridad Internacional*. (Cuadernos de estrategia 127). Instituto Español de Estudios Estratégicos. https://www.ieee.es/Galerias/fichero/cuadernos/CE-127.pdf

Campos, R. y Fernández-Valdés, T. (Productores ejecutivos). (2022). 800 metros [Serie de Televisión]. Bambú Producciones.

Christmann, K. (2012, 16 de noviembre). *Preventing Religious Radicalization and Violent Extremism.* Youth Justice Board for England and Wales. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment data/file/ 396030/ preventing-violent-ex-tremism-systematic-review.pdf

Conesa, P., Huyghe, F. B. y Chouraqui, M. (2016). *La propaganda francófona de Daech: La Mythologie du Combattant Heureux. FMSH. Observatorio de las Radicalizaciones*. París.

De Federico, A. (2002). Tendiendo puentes: de Lilnet a Redes. Introducción teórica a las relaciones entre micro y macro. Contribuciones actuales del análisis estructural. *Redes. Revista hispana para el análisis de redes sociales*, *3*, 3-18.

De la Corte, L. y Jiménez, O. C. (2022). *Terrorismo: causas, efectos y tendencias* (1.ª ed.). Síntesis.

De la Corte, L. y Jordán, J. (2006). *La yihad terrorista* (1.ª ed.). Síntesis.

Díaz-Caneja, J. M. (2019, 14 de marzo). SOCMINT y el análisis de redes complejas. https://www.linkedin.com/pulse/socmint-y-el-an%C3%A1lisis-de-redes-complejas-d%C3%ADaz-caneja-greciano/?originalSubdomain=es

El uso de internet con fines terroristas. (2013, 6 de agosto). UNODC. https://www.unodc.org/unodc/site-search.html?q=El+uso+de+internet+con+fines+terroristas

Federico de la Rúa, A. (2004). Los espacios sociales de la transnacionalidad. Una tipología de la integración relacional de los migrantes. *Revista hispana para el análisis de redes sociales, 7*(4).

Fonte, A. (2021, 8 de marzo). *OSINT, ¿Qué es? ¿Para qué sirve?*. Derecho de la red. https://derechodelared.com/osint/

Galindo, D. (2018). *Investigación y extracción de datos en fuentes abiertas*. [trabajo de fin de grado de ingeniería informática. Universidad de Alcalá]. Biblioteca Digital Universidad de Alcalá. https://ebuah.uah.es/dspace/handle/10017/34020

García, E. F., Pascual, R., Jordán, J., Bonilla, D. N., De la Corte, L., y Espinosa, M. A. (2004, 29 de junio). La inteligencia, factor clave frente al terrorismo internacional. (Cuadernos de estrategia 141). Instituto Español de Estudios Estratégicos. https://www.ieee.es/Galerias/fichero/cuadernos/CE_141_Inteligencia.pdf

Gerwehr, S. y Daly, S., (2006) *"Al-Qaida: terrorist selection and recruitment"*. National Research Defense Institute.

Gonzalo, M. (2022, 3 de agosto). *Qué es OSINT o inteligencia de fuentes abiertas*. Newtral. https://www.newtral.es/que-es-osint-inteligencia-fuentes-abiertas/20220803/

Gregory, F. (2005, 26 de julio). *Contraterrorismo Respaldado Por La Inteligencia: Breve Análisis De La Respuesta Del Sistema Nacional De Reino Unido Al 11-S Y Las Implicaciones De Los Atentados De Londres Del 7 De Julio De 2005*. Real Instituto Elcano. https://www.realinstitutoelcano.org/analisis/contraterrorismo-respaldado-por-la-inteligencia-breve-analisis-de-la-respuesta-del-sistema-nacional-de-inteligencia-del-reino-unido-al-11-s-y-las-implicaciones-de-los-atentados-de-londres-del-7-de/

Hoffman, B. (2006). *The Use of the Internet By Islamic Extremists, Testimony presented to the House Permanent Select Committee on Intelligence*. National Research Defense Institute.

Hwang, Y., Lee, I., Kim, H. y Lee, H. (2022, noviembre). Current Status and Security Trend of OSINT. *Wireless Communications and Mobile Computing, 22*. https://doi.org/10.1155/2022/1290129

International Centre for Counter-Terrorism. (2016). The Foreign Fighters Phenomenon in the European Union. LaHaya. Obtenido de https://www.icct.nl/sites/default/files/2023-01/Special-Edition-1-2.pdf

Jordán, J. (2002) El terrorismo en la sociedad de la información: el caso de Al Qaida. *El profesional de la información, 11*(4). 297-305.

Jordán, J. (2007). Las redes yihadistas en España. Evolución desde el 11-M. *Athena Intelligence Journal, 2*(3), 79-102.

Jordán, J. (2009). Procesos de radicalización yihadista en España. Análisis sociopolítico en tres niveles. *Revista internacional de Psicología Social*, *24*(2), 197-216.

Jordán, J. (2016, 18 de enero). *Una revisión del ciclo de inteligencia*. Análisis Gesi. 2. http://hdl.handle.net/10481/40628

Jordán, J. y Torres, M. R. (2007). Internet y actividades terroristas: el caso del 11-M. *El Profesional De La Informacion*. https://doi.org/10.3145/epi.2007.mar.04

Klaussen, J., Tschaen, E., Reichlin-Melnick, A. y Zelin, A. (2012). The YouTube Jihadists: A Social Network Analysis of AlMuhajiroun's Propaganda Campaign. *Perspectives on terrorism, 6*(1). 36-53.

Lejarza, E. (2015). *Terrorismo islamista en las redes – La yihad electrónica*. Instituto Español de Estudios Estratégicos. https://www.ieee.es/contenido/noticias/2015/09/DIEEEO100-2015.html

LISA Institue. (s. f.). OSINT (Inteligencia de Fuentes Abiertas): tipos, métodos y salidas profesionales. https://www.lisainstitute.com/blogs/blog/osint-inteligencia-fuentes-abiertas

LISA Institute. (s. f.). SOCMINT o inteligencia de redes sociales: definición, usos y beneficios. https://www.lisainstitute.com/blogs/blog/socmint-inteligencia-redes-sociales

Litmanovitz, Y., Weisburd, D., Hasisi, B., y Wolfowicz, M. (2017, 27 de septiembre). *What are the social, economic, psychological and environmental risk factors that lead to radicalization and recruitment to terrorism?*. Campbell Collaboration. Obtenido de https://campbell-collaboration.org/library/social-economic-psychological-environmental-risk-factors-radicalization-terrorism.html

Madriaza, P., y Ponsot, A. S. (2015). *Preventing Radicalization: A systematic Review*. Centro Internacional Para la Prevención de la Criminalidad. https://doi.org/10.13140/rg.2.1.4862.1682

Mañé, S. (2023, 7 de julio). *Nuevas estadísticas del uso de redes sociales que quieres y debes conocer*. IEBS. https://www.iebschool.com/blog/datos-de-redes-

sociales/#:~:text=El%20n%C3%BAmero%20de%20usuarios%20de,durante%20el%20resto%20del%20a%C3%B1o.

Marín, A. L. (2004). *Sociología: una invitación al estudio de la realidad social.* (2.ª ed.). EUNSA.

Moliner, P., Bovina, I., Tikhonova, A. (2018) *Images propagatrices et textes propagandistes dans la communication islamiste* [Congreso]. Congrès International de Psychologie Sociale en Langue Française.

Morán, S. (2017) La Ciberseguridad y el uso de las tecnologías de la información y la comunicación (TIC) por el terrorismo. *Revista Española de Derecho Internacional*. *69*(2). 195-221.

Moyano, M. (2019). *Radicalización terrorista. Gestión del riesgo y modelos de intervención*. (1.ª ed.). Síntesis.

Moyano, M. y Trujillo, H. (2013). *Radicalización islamista y terrorismo. Claves psicosociales*. (1.ª ed.). Universidad de Granada.

Navarro, D. y Navarro, M. A. E. (2007). *Terrorismo global. Gestión de información y servicios de inteligencia*. (1.ª ed.). Plaza y Valdés.

Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (2008). *Los Derechos Humanos, el Terrorismo y la Lucha contra el Terrorismo,* (32). https://doi.org/10.18356/9789210016049

Orav, A. (2015, 23 de marzo). *Religious fundamentalism and radicalisation.* European Parliamentary Research Service.

OSINT: qué es y técnicas más usadas. (2022, 5 de octubre). Institut de Formació Contínua-IL3. https://www.il3.ub.edu/blog/osint-que-es-y-tecnicas-mas-usadas/

Pacto Internacional de Derechos Civiles y Políticos, Artículo 19º, párrafo 3. 16 de diciembre de 1966.

Parekh, A. (2021, 12 de julio). *Uso de OSINT por parte de los Gobiernos*. BRIGADA OSINT. https://www.brigadaosint.com/uso-de-osint-por-parte-de-los-gobiernos/

Ramos, D. (2017, 16 de junio). *A fondo: Herramientas tecnológicas para combatir el yihadismo*. Silicon. https://www.silicon.es/a-fondo-herramientas-tecnologicas-combatir-yihadismo-2342272

Redacción KeepCoding (2023, 17 de febrero). Herramientas OSINT | KeepCoding Bootcamps. *KeepCoding Bootcamps*. https://keepcoding.io/blog/herramientas-osint-para-ciberseguridad/

Rettman, A. (2011). EU Intelligence Services Opening up to Collaboration. *EUObserver.com, 18.*

RTVE. (s. f.). *Condenados por los atentados del 11-M*. Consultado el 13 de enero del 2024. https://www.rtve.es/noticias/aniversario-11-m/condenados/

Sanchez, G. (2010). La nueva estrategia comunicativa de los grupos terroristas. *Revista Enfoques: Ciencia Política y Administración Pública, 8*(12). 201-215.

Sanchez, G. (2015). El Ciberterrorismo: de la web 2.0 al internet profundo. *Revista Abaco, 3*(85). 100-108.

Sánchez, G. (2018). Internet: una herramienta para las guerras en el siglo xxi. *Política y estrategia, 114.* 224-242. https://doi.org/10.26797/rpye.v0i114.177

Santos, C., y Delgado, J. (2021). Actores terroristas y crimen organizado: medidas de inteligencia para su enfrentamiento. *Seguridad, Ciencia y Defensa, 3*(3), 195–203. https://doi.org/10.59794/rscd.2017.v3i3.pp195-203

Shook, S. (2014). Your Favorite Social Networks Are Now Weapons Of Terror.

Silber, M. y Bhatt, A. (2007). *Radicalization in the West: The Homegrown Threat*. NYPD Intelligence Division.

Sunstein, R. (2009). *Going to extremes: How like minds unite and divide*. Oxford University Press.

Taylor, M. y Horgan, J. (2006). A conceptual framework for addressing psychological process in the development of the terrorist. *Terrorism and Political Violence, 18*(4). 585-601. https://doi.org.10.1080/09546550600897413

Trujillo, H. M. y Moyano, M. (2018). Towards the study and prevention of the recruitment of jihadists in Europe: A comprehensive psychological proposal. In Marrero, I. y Trujillo, H. M. (Eds.). *Jihadism, foreign fighters and radicalization in the European Union: Legal, functional and psychosocial responses* (pp. 211–230).

Trujillo, H., Ferrán, A., Cuevas, J.M. y Moyano, M. (2018). Evidencias empíricas de manipulación y abuso psicológico en el proceso de adoctrinamiento y radicalización yihadista inducida. *Revista de estudios Sociales, 66*. 42-54. https://doi.org/10.7440/res66.2018.05

Ulph, S. (2005, 31 de marzo). A guide to jihad on the web. *Terrorism focus, 2*(7).

Van Stekelenburg J., Oegema D. y Klandermans P. (2010). No radicalization without identification. How ethnic dutch and dutch muslim web forums radicalize over time. En *Identity and Participation in Culturally Diverse Societies: A Multidisciplinary Perspective.* 256–274. https://doi.org/10.1002/9781444328158.ch13

Vidino, L. (2006). Al Qaeda in Europe. The new battleground of international jihad. (1st edition). Prometeus.

Weimann, G. (2014). *New terrorism and new media*. (Research Series 2). Wilson Center. http://www.wilsoncenter.org/sites/default/files/STIP_140501_new_terrorism_F.pdf.

Weimann, G. (s.f.). Terrorismo e Internet. *Revista Étic@net*, *3*.