La investigación en fuentes abiertas (OSINT) en el ámbito de la seguridad y defensa nacional

Trabajo Fin de Grado en Criminología

Realizado por: Andrea López González

Dirigido por: Inmaculada Ruiz-Fincas

5º Doble Grado Criminología y Trabajo Social.

Curso Académico: 2024 – 2025.

Madrid, 10 de abril de 2025

AGRADECIMIENTOS

Quiero expresar mi más sincero y profundo agradecimiento a los profesionales de las fuerzas y cuerpos de seguridad del Estado por colaborar en la realización de este trabajo. Su disposición y apoyo han sido fundamentales para el desarrollo de esta investigación. Además, quiero rendir homenaje a la labor de estos profesionales, cuya dedicación y compromiso inquebrantables contribuyen diariamente a la seguridad y bienestar de todos los ciudadanos.

ÍNDICE DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE ILUSTRACIONES

GLOSARIO DE TÉRMINOS

Acrónimo	**Nombre Completo**
TFG	Trabajo de Fin de Grado
OSINT	Open Source Intelligence o inteligencia en fuentes abiertas
CFSE	Cuerpos y Fuerzas de Seguridad del Estado
FBIS	Foreign Broadcast Information Service
CIA	Central Intelligence Agency
NSA	Agencia de Seguridad Nacional de Estados Unidos
GCHQ	Cuartel General de Comunicaciones del Gobierno
SIS	Servicio Secreto de Inteligencia
MI6	Military Intelligence Section 6
MI5	Military Intelligence Section 5
HUMINT	Inteligencia Humana
GEOINT	Inteligencia Geoespacial
MASINT	Inteligencia de medición y firmas
SIGINT	Inteligencia de señales
TECHINT	Inteligencia técnica
CYBINT/DNINT	Inteligencia de redes cibernéticas/digitales
FNINT	Inteligencia financiera
IMINT	Inteligencia de imágenes
INCIBE	Instituto Nacional de Ciberseguridad
JDP	Joint Doctrine Publication
RGPD	Reglamento General de Protección de Datos
CE	Constitución Española
CIFAS	Centro de Inteligencia de las fuerzas armadas
CNI	Centro Nacional de Inteligencia
CENIF	Centro Nacional de Inmigración y Fronteras

Acrónimo	**Nombre Completo**
CITCO	Centro de Inteligencia contra el Terrorismo y el Crimen Organizado
CCN – CERT	Centro Criptológico Nacional – CERT
CMO	Oficina Central MASINT
OSINTER	Investigador OSINT

1. INTRODUCCIÓN: CONCEPTUALIZACIÓN DE LA INVESTIGACIÓN EN FUENTES ABIERTAS

Como bien es sabido, internet ha sufrido una gran evolución como consecuencia del avance tecnológico que estamos experimentando. No sólo se ha convertido en una plataforma digital donde encontrar cualquier información que solicitemos al instante, sino que también es la mayor fuente de datos. Es en internet donde cada uno de nosotros vertimos todo tipo de información, generando así una huella digital. Es decir, se registra y almacena información sobre nuestras interacciones, comportamientos y preferencias cuando navegamos por la web.

Esta huella digital puede ser analizada para múltiples fines, tanto para aspectos relacionados con el marketing (personalización de servicios, publicidad dirigida, mejora de experiencias del usuario…) como para prevenir y resolver delitos. A este análisis de información pública que se deposita en internet de forma consciente o inconsciente es a lo que en el ámbito de la seguridad de la información se denomina Open Source Intelligence o inteligencia en fuentes abiertas (OSINT de ahora en adelante).

¿Qué son las fuentes abiertas?

Las fuentes abiertas hacen referencia a todo tipo de fuente cuya información es de carácter público y no está protegida de ninguna forma. Es importante tener en cuenta que, a diferencia de lo que se cree, "una información no tiene que ser secreta para que tenga valor, pues gran parte de ella no está publicada de forma consciente" (Carcaño, 2018). A diferencia de ellas, las fuentes cerradas son aquellas cuyo acceso a los datos está restringido por medidas de seguridad al no permitir el acceso a personas no autorizadas. En este contexto, cualquier acción que restrinja el acceso, ya sea física o digital, se considera medida de seguridad (Bruno y Sumer Elías, s. f.).

Algunos ejemplos de fuentes abiertas son: redes sociales, medios de comunicación, publicaciones, listados públicos, legislaciones… Por el contrario, no lo serían: información clasificada, bases de datos o comunicación privada.

¿En qué consiste la *inteligencia* en fuentes abiertas?

La labor de hacer inteligencia a partir de fuentes abiertas consiste en buscar, recolectar y difundir la información obtenida para nuestro beneficio o el de terceros. Sin

embargo, es fundamental comprender que la información encontrada en las fuentes abiertas debemos convertirla en inteligencia para que nos resulte útil.

Es importante tener en cuenta que, al contrario de lo que comúnmente se entiende como inteligencia, en este contexto nos referimos a ella como un producto derivado de un ciclo, no mera información, pues la finalidad es mejorar el proceso de toma de decisiones.

Aplicaciones y usos del OSINT según Bruno y Sumer Elías (s. f.).

- Anticipación frente a acontecimientos meteorológicos, catástrofes naturales, proyecciones climáticas, etc.
- Analizar escenarios de corrupción de empresas o gobiernos.
- Realizar seguimientos sobre conversaciones en redes sociales, foros, chats y blogs.
- Investigar relaciones entre personas, empresas, asociaciones, partidos, etc.
- Detectar fallos de configuración que impliquen la exposición de información.
- Monitorear e investigar páginas fraudulentas y phishing.
- Conocer la reputación online de un usuario o empresa.
- Realizar estudios sociológicos, psicológico, lingüísticos, culturares, geográficos, etc.
- Evaluar tendencias de mercados.
- Identificar y prevenir posibles amenazas en el ámbito militar o de la seguridad nacional.

2. OBJETIVOS Y PREGUNTAS DE INVESTIGACIÓN

2.1 Objetivo general

Dado que el OSINT tiene una fuerte presencia en ámbitos de defensa y seguridad, este TFG tiene como principal objetivo analizar la utilidad, el uso y el futuro de esta técnica en el ámbito de la defensa y seguridad nacional.

2.2 Objetivos específicos

- Estudiar en qué medida se utiliza la investigación en fuentes abiertas en las Fuerzas y Cuerpos de Seguridad (FCSE de ahora en adelante).

- Conocer cuál sería el perfil idóneo para ser investigador en fuentes abiertas.
- Examinar los tipos y métodos de obtención de información llevados a cabo en las operaciones.
- Examinar los desafíos a los que nos enfrentamos al investigar en fuentes abiertas y las líneas de futuro que se prevén.
- Investigar las opiniones de los profesionales sobre cómo la inteligencia artificial afectará al OSINT.

2.3 Preguntas de investigación

- ¿Desde cuándo se ha incluido la investigación en fuentes abiertas como herramienta en las FCSE?
- ¿Todos los FCSE utilizan la técnica OSINT en sus investigaciones?
- ¿Existe una unidad especializada para ello?
- ¿Cómo es la estructura que se encarga de la Inteligencia Nacional en España?
- ¿Existe un perfil de investigador OSINT (OSINTER de ahora en adelante) definido? ¿Cuáles serían sus características?
- ¿La investigación en fuentes abiertas se utiliza siempre o solo en determinadas operaciones?
- ¿Qué tipo de información recogen y analizan? ¿A través de que metodología?
- ¿Cuáles son los principales desafíos en la implementación del OSINT?
- ¿Cómo va a afectar la Inteligencia Artificial (IA de ahora en adelante) en el futuro del OSINT?
- ¿Cómo se garantiza la ética y la legalidad en el uso de OSINT dentro de los procesos de investigación?

3. METODOLOGÍA

La metodología de este Trabajo de Fin de Grado (TFG) se basa en un enfoque cualitativo, centrado en la realización de entrevistas a profesionales del ámbito de la defensa y seguridad nacional. Este enfoque es esencial para obtener una comprensión profunda y detallada de las experiencias y percepciones de los participantes en relación con el uso de OSINT (Open Source Intelligence).

La primera etapa de la investigación se centrará en la revisión de fuentes documentales y el análisis de la literatura existente sobre la materia. Este proceso incluirá la recopilación y estudio de artículos académicos, informes técnicos y otras publicaciones relevantes. La revisión de la literatura permitirá establecer un marco teórico sólido e identificar las principales tendencias y desafíos asociados con el uso de OSINT.

La segunda etapa de la investigación consistirá en la realización de entrevistas semiestructuradas a profesionales con experiencia en OSINT en el ámbito mencionado anteriormente, tales como agentes de policía, guardia civil, militares y formadores de las Fuerzas y Cuerpos de Seguridad del Estado (FCSE).
Debido a la escasa literatura existente sobre el fenómeno de OSINT en el ámbito de la defensa y seguridad nacional, la investigación cualitativa basada en entrevistas semiestructuradas es especialmente valiosa para conocer las distintas aristas del fenómeno.

Las entrevistas se han diseñado de forma semiestructurada para obtener respuestas abiertas y detalladas, permitiendo explorar diversas aristas del fenómeno estudiado. El guion de las entrevistas se incluye en el anexo de este documento.

Estas entrevistas han sido realizadas durante los meses de marzo y abril, todas de forma online a través de la aplicación de Teams, según la disponibilidad de los entrevistados. Además, se ha garantizado la confidencialidad y anonimato de los profesionales entrevistados. El consentimiento de colaboración y confidencialidad queda adjuntado en el anexo.

La selección de informantes se ha realizado por conveniencia, aprovechando los contactos personales y los proporcionados por los propios informantes.

Durante toda la investigación, se asegurará la correcta citación de todas las fuentes bibliográficas utilizadas, respetando los principios éticos y de rigor académico.

4. MARCO TEÓRICO

4.1 Aproximación a la investigación en fuentes abiertas (OSINT)

4.1.1 Origen del OSINT: antecedentes y evolución.

La práctica de utilizar fuentes abiertas para hacer inteligencia no es algo novedoso, pues ya en la antigüedad los comerciantes, juglares y gobiernos hacían uso de ellas, pero sí lo es su desarrollo y formalización en las últimas décadas (Equipo IUCPOL, 2023).

Los inicios de la disciplina OSINT se remontan a la década de los 40, cuando en Estados Unidos surge el Foreign Broadcast Information Service (FBIS) para dar respuesta a la necesidad de recopilar información y generar inteligencia con fines militares (Equipo IUCPOL, 2023).

El FBIS utilizaba como fuente las transmisiones extranjeras que promocionaban la guerra, los bandos recolectaban y analizaban mensajes lanzados por radio o periódicos para obtener información sobre las intenciones y movimientos del enemigo. De hecho, se cree que gracias al trabajo del FBIS se pudo anticipar la intención de Japón de intervenir en la segunda guerra mundial (Rojo, 2023).

En 1947, una vez finalizada la II Guerra Mundial, el FBIS fue absorbido por la Central Intelligence Agency (CIA) (Equipo IUCPOL, 2023).

Sin embargo, fue a finales de la década de los 80, con el fin de la Guerra Fría, cuando se acentuó la importancia para los gobiernos de adquirir la mayor información pública posible. Y no es hasta 2013 cuando la Agencia de Seguridad Nacional de Estados Unidos (NSA), divulgó un manual de capacitación destinado a sus agentes, en el cual se enseñaba cómo utilizar Google para encontrar información relevante (Rojo, 2023).

Este gran valor que se le iba añadiendo a esta información, sumado a la llegada de la era digital con internet fue el detonante para OSINT.

Se pueden destacar dos acontecimientos que marcaron el despegue del OSINT: la creación de la Community Open Source Program Office en EE. UU en 1992 y el atentado del 11 de septiembre de 2001. Este último acontecimiento marcó un punto de inflexión para OSINT, destacando su importancia en la lucha contra el terrorismo global y la seguridad nacional. Desde entonces, OSINT se ha convertido en una herramienta primaria

y fundamental de inteligencia, utilizada en todo el mundo por todo tipo de agentes, desde fuerzas de seguridad, hasta el ámbito político, civil y empresarial (Rojo, 2023).

Su historia refleja una evolución continua, adaptándose a los avances tecnológicos, los cambios políticos y las crecientes demandas de seguridad global.

4.1.2 Análisis de actualidad.

Nos situamos en la era de la tecnología e información, periodo característico por la producción constante de datos en todas las esferas de nuestra vida: redes sociales, ámbito laboral, relaciones interpersonales, búsquedas académicas…

Partiendo de la idea del filósofo Jean-Paul Sartre "el hombre está condenado a ser libre", o que nuestra vida está marcada por nuestras elecciones, todas las decisiones y acciones que ejecutamos en el entorno digital dejan un rastro. Todas las plataformas digitales generan un flujo continuo de información alimentado por descargas, búsquedas, publicaciones, localizaciones, preferencias musicales, temas de interés, transacciones…

Esta evolución ha dado lugar al desarrollo de la disciplina encargada de analizar toda esa información pública depositada en fuentes abiertas de internet, derivando en la inteligencia en fuentes abiertas. Esta inteligencia no sólo se ha ganado su lugar en la esfera de la ciberseguridad, sino que abarca desde la seguridad nacional hasta la investigación criminal, el análisis empresarial, el periodismo o el marketing, entre otros. El valor reside en la gran aplicabilidad en múltiples contextos.

En este mundo donde la información es poder y, además, cada vez hay más información, gracias al OSINT podemos convertir datos aparentemente convencionales de fuentes de acceso público, en material valioso, y gracias ello, adoptar decisiones estratégicas.

En España, el desarrollo del OSINT ha seguido tendencias internacionales, pero comenzó a ganar relevancia principalmente en las últimas décadas del siglo XX, pues con la expansión de internet, las agencias españolas comenzaron a integrar fuentes abiertas como un complemento a otras formas de inteligencia (HUMINT y SIGINT).

Un país con una gran estructura de inteligencia sería, por ejemplo, Reino Unido, dónde el OSINT desempeña un papel clave en el marco de la inteligencia nacional. Al

igual que en EE. UU, diversas agencias y organismos colaboran para apoyar en la toma de decisiones en materia de seguridad y defensa. Los tres principales servicios de inteligencia de Reino Unido son los siguientes (González, s.f.):

- **Cuartel General de Comunicaciones del Gobierno (GCHQ):** su principales funciones incluyen la inteligencia de señales (SIGINT), que implica la supervisión, interceptación y descifrado de datos, especialmente en la lucha contra el terrorismo y el crimen organizado; y la Information Assurance, una rama especializada de la seguridad de la información, destinada a proteger los sistemas de comunicación informática del gobierno británico ("Government Communications Headquarters", 2025).
- **Servicio Secreto de Inteligencia (SIS):** Servicio de inteligencia exterior también conocido como MI6 (Military Intelillenge Section 6), encargado de recoger y analizar de manera encubierta HUMINT exclusivamente en el extranjero para asistir a la seguridad nacional de Reino Unido ("MI6", 2025).

- **Servicio de seguridad (MI5):** Servicio de inteligencia dedicado a la seguridad interna del país. A diferencia del MI6, es responsable de las actividades de espionaje del interior del país ("MI5", 2024).

4.2 Clasificación de disciplinas de inteligencia

Existe una gran familia de disciplinas de inteligencia, su clasificación responde a la naturaleza de las fuentes empleadas, al método utilizado para recolectarla, analizarla y explotarla, y al propósito de la información obtenida. Cada una de ellas aporta una perspectiva única, lo que permite una comprensión integral de los fenómenos analizados (Ferreira, 2024).

Las diferentes fuentes de información en las que nos apoyamos son reconocidas como disciplinas de inteligencia, de ahí el sufijo añadido "-INT" a cada una de ellas. Estas disciplinas permiten a los analistas cubrir un amplio espectro de necesidades y contextos, integrando información de diversas procedencias para generar conocimiento accionable (Ferreira, 2024).

Tabla 1: Disciplinas de inteligencia

DISCIPLINAS DE INTELIGENCIA	
HUMINT	Inteligencia Humana
GEOINT	Inteligencia Geoespacial
MASINT	Inteligencia de medición y firmas
OSINT	Inteligencia en fuentes abiertas
SIGINT	Inteligencia de señales
TECHINT	Inteligencia técnica
CYBINT / DNINT	Inteligencia de redes cibernéticas/digitales
FNINT	Inteligencia financiera
IMINT	Inteligencia de imágenes

Fuente: Elaboración propia a partir de Ferreira (2024).

A continuación, se procede a realizar una breve explicación de cada una de las disciplinas de inteligencia según Ferreira (2024):

- **Inteligencia Humana – HUMINT:** recopilación de información de fuentes humanas, abiertamente (entrevistas a testigos o sospechosos) o medios encubiertos (espionaje).

- **Inteligencia Geoespacial – GEOINT:** Estudio y representación gráfica de actividades vinculadas a la seguridad terrestre, lograda mediante la combinación de imágenes, inteligencia visual e información geoespacial.

- **Inteligencia de medición y firmas – MASINT:** Relativa a las capacidades de las armas y las actividades industriales. El principal usuario de los datos MASINT es la Oficina Central MASINT (CMO) de la Agencia de Inteligencia de Defensa. Se ha vuelto cada vez más importante por el aumento de la preocupación por la existencia y propagación de armas de destrucción masiva. Un ejemplo de ello sería ayudar a identificar armas químicas o señalar las características específicas de sistemas de armas desconocidos.

- **Inteligencia en fuentes abiertas – OSINT:** información y fuentes ampliamente disponibles tales como información procedente de medios de comunicación, registros profesiones y académicos, datos demográficos, discursos, ponencias…

- **Inteligencia de señales – SIGINT:** transmisiones electrónicas que pueden ser recopiladas por barcos, aviones, sitios terrestres o satélites. Un tipo es COMINT (communications intelligence) que es la interceptación de comunicaciones entre dos partes.

- **Inteligencia técnica – TECHINT:** analiza información científica y técnica extranjera para evaluar sistemas, armas y procesos de producción, considerando su desarrollo, capacidades y contexto estratégico (TECHINT: Technical Intelligence, s.f.).

- **Inteligencia de redes cibernéticas/digitales – CYBINT/DNINT:** Asociada con el desarrollo de las redes de ordenadores que se encarga de la combinación de datos, algoritmos y técnicas especiales para analizar información de red y paquetes de datos IP a medida que viajan a través de una red en tiempo real (Ortiz, 2020).

- **Inteligencia financiera – FNINT:** El objetivo de FININT es detectar y rastrear actividades y transacciones sospechosas de dinero, proporcionando inteligencia útil a las autoridades, con el objetivo de investigar y enjuiciar los delitos financieros (Cilleruelo, 2024).

- **Inteligencia de imágenes – IMINT:** Recopilar información sobre su entorno. Esta se practicó más en la primera y segunda guerra mundial cuando ambos bandos tomaban fotografías desde aviones.

4.3 Fases del ciclo de inteligencia

Antes de iniciar una investigación OSINT, se deben tener en cuenta una serie de factores que guiarán el proceso y condicionarán a la hora de escoger las herramientas más adecuadas (LISA Institute, 2020):

1. Tipo de datos o información a buscar.
2. Objetivo o target y su nivel de exposición.
3. Medios disponibles: técnicas y herramientas OSINT que se conocen, disponen y dominan.
4. Disponibilidad de otras fuentes (HUMINT, IMINT, SIGINT, etc.).
5. Urgencia/importancia de la búsqueda.
6. Grado de exigencia de reserva de la investigación.

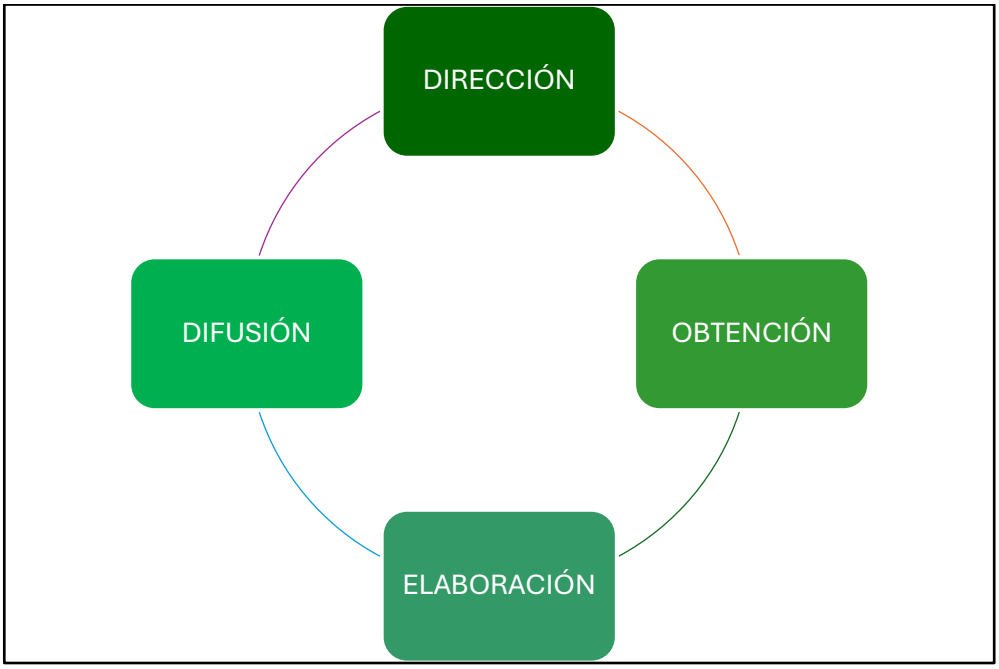
El OSINT no hace referencia a una herramienta en sí misma, ni a recolectar toda la información posible; para hacer OSINT es necesario aplicar una metodología de trabajo determinada, denominada *ciclo de inteligencia* o *ciclo OSINT*. Este se compone por distintas fases que finalizan en el producto final, en este caso, un informe de inteligencia.

Cabe destacar, que, durante el trabajo de investigación, se han apreciado ciertas diferencias en cuanto a las fases que conforman el ciclo OSINT según diferentes organizaciones. En España, contamos con el Ciclo de inteligencia establecido por el CNI (Centro Nacional de Inteligencia) y con el INCIBE (Instituto Nacional de Ciberseguridad). Ambos organismos se dedican al sector de defensa, por lo que, a pesar de presentar alguna diferencia en el procedimiento, los dos son ampliamente válidos y aceptados por las instituciones de inteligencia.

A su vez, existen diferentes enfoques del proceso en diferentes países, como el de la CIA (Center Intelligence Agency) o el Ciclo de inteligencia según el JDP 2-00 (Joint Doctrine Publication) en Reino Unido.

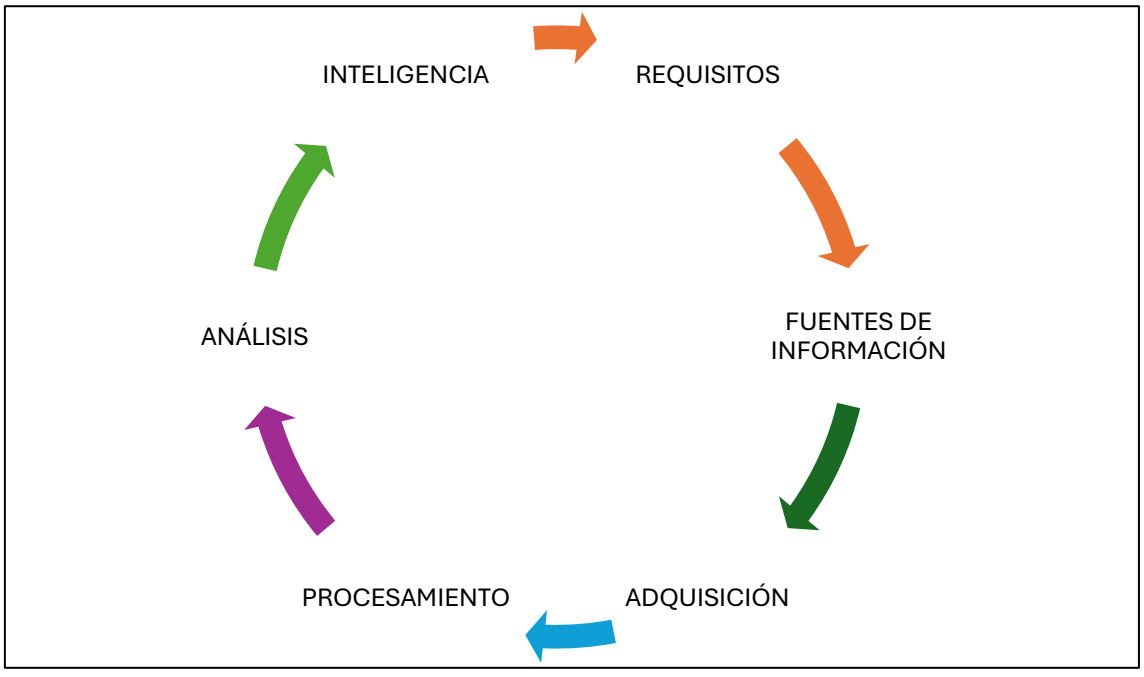
A continuación, se exponen los ciclos de inteligencia de los 4 organismos mencionados anteriormente y una breve explicación del predominante en España según Castillejo (2024):

Ilustración 1: Ciclo de inteligencia según el CNI y del JDP 2-00 Reino Unido



Fuente: Elaboración propia a partir de Castillejo (2024)

Ilustración 2 Ciclo de inteligencia según INCIBE



Fuente: Elaboración propia a partir de Martínez (2014)

1. **Requisitos**

Es la fase inicial del proceso, en la que deben ser definidas concretamente las preguntas que guarán nuestra investigación.

2. **Fuentes de Información**

Consiste en determinar qué fuentes pueden proporcionar datos relevantes según el objetivo de la investigación. Por ejemplo, si el foco de análisis es una persona, se emplearán fuentes que faciliten la recopilación de datos personales (nombres de usuario en redes sociales, direcciones…); y si el objetivo es una empresa, se pueden utilizar herramientas para analizar su infraestructura digital, identificar dominios asociados u obtener registros de correos electrónicos corporativos expuestos en brechas de seguridad.

3. **Adquisición de Información**

En esta fase se procede a recopilar toda la información disponible de las fuentes previamente identificadas. La cantidad de datos puede ser extensa, por lo que es fundamental contar con herramientas adecuadas para extraer la información de manera eficiente. Suele ser la etapa que más se dilata en el tiempo.

4. **Procesamiento de Datos**

En esta fase se estructuran y filtran los datos útiles para la investigación. Se descartan elementos irrelevantes o redundantes y se clasifican los datos de acuerdo con su relevancia y confiabilidad.

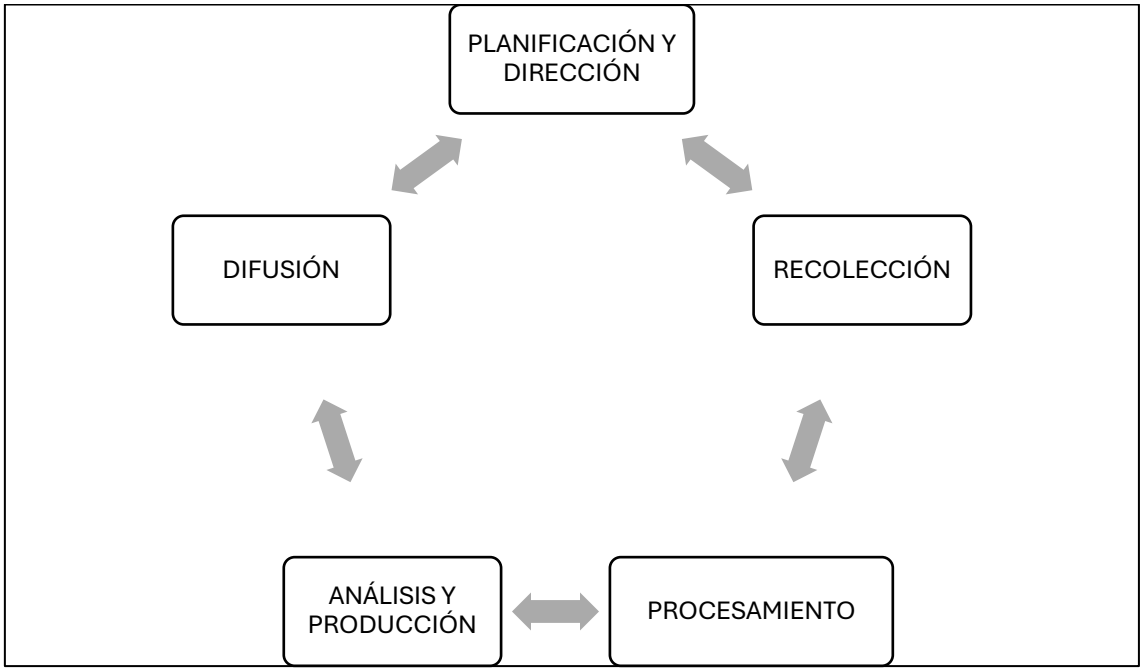
5. **Análisis**

En esta fase se identifican patrones, correlaciones y relaciones entre los datos para darles coherencia y significado. A partir de esta interpretación, pueden surgir nuevas líneas de investigación o hallazgos adicionales.

6. **Inteligencia**

Una vez finalizado el análisis, la información procesada se transforma en inteligencia útil, lista para ser presentada en un informe estructurado.

Ilustración 3 Ciclo de inteligencia según la CIA



Fuente: Elaboración propia a partir de Castillejo (2024)

Por último, es importante señalar que el elemento distintivo entre los diversos enfoques reside en su estructura. Aunque mantienen una base común, estos enfoques se diferencian por la inclusión de etapas intermedias o por la variación en la nomenclatura de las fases existentes. No obstante, es crucial subrayar que la gran mayoría de estos modelos incorporan una fase de evaluación y retroalimentación, lo cual constituye un punto de convergencia significativo. Además, los ciclos no son necesariamente lineales; en muchas ocasiones, los hallazgos pueden llevar a la necesidad de regresar a etapas previas para refinar o ampliar la información recopilada (Castillejo, 2024).

4.4 Perfil profesional en OSINT

La metodología OSINT fue inicialmente desarrollada para los servicios de inteligencia, sin embargo, se ha ido extendiendo a otros campos, dando lugar a una aplicabilidad muy amplia que abarca prácticamente a cualquier profesión. Por ello, es importante realizar una descripción general sobre las características que debe tener un OSINTER independientemente del ámbito en el que trabaje.

Un investigador de OSINT no debe adoptar una perspectiva ejecutora, ya que no realizará un trabajo eficaz si dedica la mayor parte de su tiempo a probar herramientas para determinar cuál puede ser efectiva. Debe pensar y analizar; es decir, a partir de la comprensión de cómo fluye la información en internet, debe seleccionar las herramientas más adecuadas para la investigación (Gutiérrez, s.f.).

Existen numerosas plataformas desde las cuales se pueden obtener datos sin necesidad de realizar búsquedas exhaustivas, ya que muchos de ellos están completamente expuestos. La clave radica en un cambio de mentalidad: en lugar de utilizar herramientas con la esperanza de encontrar información al azar, es más efectivo reflexionar sobre dónde es más probable que un usuario haya almacenado esos datos (Gutiérrez, s.f.).

Una vez definida la visión de trabajo, se procede a enumerar ciertas cualidades propias de un investigador en fuentes abiertas (Gutiérrez, s.f.):

- Dominio de los conceptos fundamentales de la materia.
- Aplicación de un método y un sistema de trabajo estructurado para gestionar la información de manera eficiente.
- Manejo adecuado de herramientas especializadas y métodos más recientes para realizar investigaciones en línea de manera rápida y segura.

Además de las cualidades previamente mencionadas, LISA Institute (2020) identifica y añade varias características adicionales que son fundamentales para la práctica de OSINT:

- Comprender el potencial de las técnicas de investigación OSINT a nivel profesional en las áreas pública y privada.
- Comprensión del entorno digital, con un enfoque en el flujo de la información en internet, lo que facilita un cambio de perspectiva y enfoque analítico.
- Saber cómo llevar a cabo búsquedas avanzadas de información y datos sobre personas, empresas e instituciones de forma anónima.
- Entender cuáles son las regulaciones actuales que permiten investigar con seguridad legal.
- Proteger tu entorno de trabajo para resguardar tu identidad y evitar otros peligros durante la investigación.

- Conocer el concepto de la Deep Web y la Dark Web, así como los riesgos que estas áreas implican.

4.5 Tipos de fuentes abiertas de recolección de datos

Según González (s.f.), las fuentes abiertas se pueden clasificar de manera general en dos tipos, basándose en el procesamiento de la información y en su disponibilidad y acceso. Esta clasificación permite una mejor organización y utilización de las fuentes, facilitando así el trabajo de los profesionales de la inteligencia.

Comenzando por la clasificación según el procesamiento de la información, nos encontramos con fuentes primarias, secundarias y terciarias.

Las fuentes primarias son aquellas que almacenan información original de primera mano, sin haber sido modificada ni procesada en ningún momento.

Por otro lado, las secundarias son el resultado del tratamiento documental de las primarias. Además, su valor incrementa mediante elementos como resúmenes, agrupaciones temáticas, correspondencia con otros idiomas, bibliografías… Algunos ejemplos serían: catálogos, repertorios legislativos y bases de datos.

Las fuentes terciarias se caracterizan por ser similares a las fuentes secundarias, pero se les atribuye una finalidad específica: la integración de la información mediante un análisis crítico de las unidades documentales de una disciplina, destacando de cada una los aspectos más relevantes en cuanto a innovación y avance. Algunas de estas fuentes serían las reseñas (review) y los "state of the art" (resumen actualizado y detallado del conocimiento más reciente sobre un tema o disciplina específica).

Por último, en relación con su disponibilidad y acceso, la información en fuentes abiertas se puede clasificar en literatura blanca (publicada de manera tradicional), white-st ("Literatura de corto plazo": "literatura efímera") y literatura gris (literatura no disponible públicamente).

La literatura blanca hace referencia a la que queda publicada de manera tradicional tras pasar por un proceso de revisión, edición y publicación a cargo de una entidad reconocida, como una editorial o una institución académica.

Por otro lado, la literatura de corto plazo o literatura efímera (White-st), engloba elementos de interés que permanecen publicados por tiempo limitado y se utiliza para identificar determinados acontecimientos en escenarios cambiantes. Algunos ejemplos pueden ser: horarios y cancelaciones, lista de asistentes a un evento, matrículas de coches que circulan, reservas de alojamiento, manifestaciones, conciertos…

Finalmente, en lo que respecta a la literatura gris, es aquella que se genera en determinados sectores sin estar sujeta al control de editores comerciales. Se trata de material de acceso abierto (nacional o extranjero), que suele distribuirse a través de canales especializados y que, en muchos casos, no forma parte de los sistemas convencionales de publicación.

4.6 Métodos de obtención de información

La información disponible en fuentes abiertas es altamente accesible; sin embargo, es crucial saber cómo acceder a ella. Según el LISA Institute (2020), existen diversos métodos para obtener información, los cuales varían en función de nuestros objetivos.

En primer lugar, la **obtención pasiva**, cuya finalidad es obtener información sobre un objetivo sin que este sea consciente de ello. Esta metodología implica una mayor aplicación de medidas de seguridad, pues el investigador debe pasar totalmente desapercibido por la red. Además, es necesario tener en cuenta que la información recogida de forma pasiva es limitada, pues únicamente se observa el tráfico y contenidos que genera el objetivo, sin contrastarla ni verificarla.

Por otro lado, la obtención **semi-pasiva** se realiza a través del tráfico que el propio investigador genera en la red, ya sea a través de consultas, chequeos o solicitudes de acceso a servidores. Con este método se obtiene mayor cantidad de información que con la obtención pasiva, sin embargo, el investigador asume más riesgos de poder ser detectado por el objetivo, por lo que es muy importante actuar con la mayor discreción posible.

Por último, la obtención **activa**, a través de la cual el analista interactúa directamente con el objetivo y sus recursos. Se trata del método que permite mayor recopilación de información en comparación con los demás. Implica la realización de consultas continuas al servidor, lo que lo hace poco discreto para mantenerse indetectable en una investigación OSINT.

4.7 Mecanismos y herramientas para hacer OSINT

El campo del OSINT ofrece una amplia gama de herramientas y servicios para la implementación efectiva de sistemas de inteligencia. Estas soluciones abarcan todo el espectro del ciclo de inteligencia, desde la recolección inicial de datos hasta el análisis avanzado. Las diversas opciones disponibles permiten a los profesionales de OSINT adaptar sus metodologías y flujos de trabajo a las necesidades específicas de cada investigación o proyecto, mejorando la eficiencia y la precisión en la obtención y procesamiento de información de fuentes abiertas (Rojo, 2023).

A continuación, se presentan las dos tipologías de buscadores existentes según Bielska et ál. (2020) junto a tablas de elaboración propia con ejemplos basadas en la autora mencionada anteriormente.

Buscadores habituales

Los buscadores habituales permiten recopilar toda la información que clasifican e investigar usando parámetros específicos y concretos. De esta forma, se pueden realizar búsquedas con un alto nivel de precisión.

Tabla 2: Buscadores Habituales

EJEMPLOS BUSCADORES HABITUALES	
Googlesearch	Infospace
DuckDuckGo	Baidu
Bing	Ask
Yandex	Yahoo! Search

Buscadores especializados

Los buscadores especializados son aquellos que se enfocan en la búsqueda y recopilación de información de un sector concreto, proporcionando información más exacta y en profundidad sobre temáticas a través de fuentes y recursos especializados. (Calvo, 2025)

Tabla 3: Recolección de metadatos

EJEMPLOS HERRAMIENTAS DE RECOLECCIÓN DE METADATOS	
FOCA	Metadata2Go
Metagoofil	Pymeta
Anonymouth	Doc Scrubber

Tabla 4: Buscadores a partir de un dominio

EJEMPLOS BUSCADORES A PARTIR DE UN DOMINIO	
DomainEye	intoDNS
Iwantmyname	Whoxy
Whois	Urlscan

Tabla 5: Buscadores a partir de una imagen

EJEMPLOS BUSCADORES A PARTIR DE UNA IMAGEN	
PimEyes	TinEye
Reverse Image Search	ShotHotSpot
Photosint	Fotoforensics

Tabla 6 Buscadores a partir de un Email

EJEMPLOS BUSCADORES A PARTIR DE UN EMAIL	
Have I Been Pwned	SimpleMail
EPIEOS	Email Rep

Tabla 7 Buscadores mercantiles

EJEMPLOS BUSCADORES MERCANTILES	
Empresia.es	NorthData Smart Research
Librebor	Informa D&B

4.8 Consideraciones legales

Dado que la literatura es escasa en este aspecto, el autor más relevante es Fernández (2023), por lo que la totalidad del apartado queda referenciada al mismo.

En toda investigación OSINT, es crucial conocer no sólo qué información se necesita y cómo obtenerla, sino también los límites legales y éticos de su recopilación y difusión.

La información pública, en principio, no está sujeta a restricciones para su recopilación, siempre que se obtenga de fuentes verdaderamente abiertas y no protegidas por barreras de seguridad. Cuando un individuo expone voluntariamente sus datos en una fuente abierta, se considera que ha otorgado un consentimiento tácito que excluye esa información específica de su derecho a la intimidad y protección de datos personales (artículos 18.1 y 18.4 de la CE). Esto se aplica también a imágenes, vídeos, audios y conversaciones publicadas en redes sociales, que quedan desvinculados del derecho a la propia imagen y al secreto de las comunicaciones.

Sin embargo, el uso indebido de técnicas OSINT puede dar lugar a diversos delitos, dependiendo del contexto y las intenciones del investigador. La línea entre la investigación legítima y la actividad delictiva puede ser tenue, especialmente cuando se trata de información personal o sensible. Aunque la información esté disponible

públicamente, su recopilación, procesamiento y uso pueden estar sujetos a regulaciones estrictas, como el Reglamento General de Protección de Datos (RGPD de ahora en adelante) en la Unión Europea.

Las consecuencias de un uso indebido de OSINT no se limitan al ámbito legal, sino que también tienen implicaciones éticas significativas. Pueden afectar a la reputación profesional, la confianza pública en las instituciones y, en casos extremos, la seguridad nacional o individual. Por ello, es fundamental que los profesionales que utilizan OSINT se adhieran a códigos de conducta estrictos y se mantengan actualizados sobre las normativas legales aplicables.

En última instancia, la responsabilidad recae en el investigador para asegurar que sus prácticas de OSINT se mantengan dentro de los límites legales y éticos establecidos. Es esencial equilibrar la necesidad de obtener información con el respeto a los derechos individuales y colectivos, teniendo especial cuidado con las leyes de protección de datos en el almacenamiento y difusión de la información obtenida.

<u>Recolección</u>

- Según el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (2016), se exige el consentimiento explícito de los usuarios antes de recopilar sus datos personales.

- Según la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (2002), se obliga a los proveedores de servicios en línea a informar a los usuarios sobre la recopilación de sus datos personales.

<u>Almacenamiento</u>

- Según la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones (2007), se establece la obligación de los operadores de telecomunicaciones de retener ciertos datos de comunicaciones electrónicas por un período determinado.

- Según el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (2016), se regula cómo se deben almacenar y proteger los datos personales recopilados.

Difusión

- Según la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (2018), se regula la publicación y difusión de datos personales, especialmente de menores, a través de servicios de redes sociales.

- Según el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (2016), establece que los usuarios tienen derecho a saber cómo se utilizan sus datos y pueden solicitar su eliminación.

Posibles delitos que se pueden cometer durante una investigación OSINT

1. Invasión de la privacidad y ciber espionaje: apoderamiento, utilización o modificación sin autorización de datos reservados, personales o familiares, que estén registrados en soportes o ficheros informáticos para alterarlos o utilizarlos en perjuicio del titular o de un tercero (Código Penal, 197.2).
2. Phishing y suplantación de identidad: realizar ataques personalizados, como correos electrónicos fraudulentos o spear-phishing (Código Penal, 249 y 401).
3. Acceso no autorizado a sistemas: Usar técnicas como "Google dorking" para encontrar vulnerabilidades en aplicaciones web y utilizarlo para explotar dichas brechas (Código Penal, 197 bis 1).

4.9 Consideraciones éticas

En primer lugar, entendiendo la ética como *"Conjunto de normas morales que rigen la conducta de la persona en cualquier ámbito de la vida"* (Real Academia Española, s.f.), en este ámbito debemos considerarla en relación con los derechos legales, las expectativas de privacidad y los beneficios para la sociedad.

Además de los aspectos legales, el OSINT está sujeto a principios éticos que marcan el comportamiento de los investigadores (Comunidad GINSEG, 2020). Es decir, la recopilación de información de fuentes abiertas puede plantear problemas de privacidad y ética, especialmente cuando se trata de datos personales y sensibles (M. Pascual, comunicación personal, 10 de marzo de 2025). Por ello, los OSINTERS deben ajustar su trabajo a principios éticos como la integridad, la transparencia y el respeto a los derechos individuales, pues son los responsables de garantizar que las investigaciones sean éticas y legales, evitando el uso inapropiado de la información recogida. (Comunidad GINSEG, 2020).

Algunos de los estándares éticos que deben respetarse en el uso del OSINT según Cybermentor (2025), son:

- Legalidad: Aunque la información esté disponible públicamente, eso no implica que su utilización sea siempre legal. Por ejemplo, recopilar datos que infringen la privacidad de un individuo u obtener información de fuentes seguras puede ser ilícito.
- Consentimiento: Es fundamental tener presente que, a pesar de que los datos son accesibles al público, emplear información personal sin el permiso del dueño puede acarrear complicaciones éticas y legales.
- Confiabilidad de las fuentes: Un aspecto clave es comprobar la credibilidad de los datos. El uso de OSINT debe enfocarse en reunir información de fuentes confiables y comprobadas, y evitar el aprovechamiento de rumores y datos no confirmados.
- Confidencialidad: Aun cuando la información sea de acceso público, es fundamental considerar la posible afectación a la privacidad de los individuos, su seguridad y la salvaguarda de los datos.

- Responsabilidad: Las entidades que utilizan OSINT deben ser responsables en la forma en que utilizan los datos obtenidos. El uso inapropiado puede resultar en implicaciones legales, daños a la reputación y otras repercusiones adversas.

4.10 Beneficios de la investigación en fuentes abiertas

Investigar en fuentes abiertas tiene múltiples ventajas en comparación con otras metodologías, pues se caracteriza por ser mucho más eficiente, económico y seguro (LISA Institute, 2020).

Por ejemplo, para hacer OSINT en el ciberespacio, sólo es necesario disponer de un dispositivo electrónico (móvil, Tablet u ordenador) y de conexión a internet. Es decir, la accesibilidad a la información es inmediata y de bajo coste independientemente de la ubicación del investigador, y pueden acceder a la investigación los analistas que resulten necesarios sin restricciones de acceso a la información. Sin embargo, el hecho de necesitar pocos medios no significa que cualquier persona puede hacer OSINT de forma competente, pues es necesario contar con formación y conocimientos especializados para poder investigar de forma profesional y segura (LISA Institute, 2020).

Además, al trabajar con información pública, en la mayoría de los casos, no existen riesgos políticos ni limitaciones desde el punto de vista legal, pues el investigador no está expuesto a ser procesado por espionaje. Excepto en investigaciones semi-pasivas o activas, que debe ser considerada la normativa vigente sobre protección de datos, el código penal y la jurisprudencia al respecto. Cada nación posee una perspectiva distinta respecto a la Protección de Datos, así como en la aplicación de determinadas técnicas y herramientas OSINT (LISA Institute, 2020).

Por otro lado, a diferencia de otras disciplinas (como por ejemplo HUMINT), las investigaciones se llevan a cabo en escenarios con medidas de seguridad específicas que mantienen el anonimato, la confidencialidad y el secreto de la investigación en curso, lo que supone una metodología de riesgo muy bajo para los investigadores y para la investigación. Además, es posible acceder a información filtrada y comparar información de diferentes fuentes de análisis de datos, siendo esta actual y precisa (González, s.f.).

4.11 Desafíos y retos de la investigación en fuentes abiertas

Las investigaciones OSINT se han convertido en una herramienta clave en el ámbito de la investigación, la ciberseguridad y la inteligencia. Sin embargo, su uso no está exento de desventajas, en este apartado se analizarán algunas de ellas (Martínez, 2014).

En primer lugar, las investigaciones OSINT se caracterizan por la recopilación de grandes cantidades de información, pues como bien hemos visto, el volumen de información disponible públicamente en Internet es excesivamente amplio. Esto requiere de un proceso de análisis y selección muy exhaustivo, tanto de información como de herramientas y fuentes de interés (Martínez, 2014). Es cierto que existen herramientas automatizadas para el análisis de información, pero no siempre se contará con los medios necesarios para poder hacer uso de ellas, pues pueden ser costosas o exigir requisitos para acceder a ellas. De todos modos, aun contando con estas herramientas, el tremendo volumen de datos seguirá siendo un desafío (LISA Institute, 2020).

En segundo lugar, este tipo de investigaciones presentan una mayor vulnerabilidad a la desinformación y datos falsos (Martínez, 2014). Por el hecho de alimentarse de fuentes de información abiertas, son investigaciones más susceptibles a noticias falsas, propaganda o manipulación de información en comparación con otros métodos que sí que verifican la información directamente. Por ejemplo, los canales o las redes sociales pueden estar manipulados con *bots* o información errónea, incluso existen campañas de desinformación intencionada lanzadas con el objetivo específico de distorsionar las investigaciones (Rid, 2020). Un ejemplo de ello sería que, durante la investigación de una crisis internacional, se encuentre con imágenes de conflictos pasados compartidas como si fueran actuales, lo que lleva a una interpretación incorrecta de los hechos. Por ello, debemos evaluar previamente las fuentes que alimentarán el sistema de información, ya que una selección inadecuada puede generar resultados incorrectos y contribuir a la desinformación (Martínez, 2014). Esta evaluación y validación de las fuentes de información mediante OSINT es un proceso complejo (LISA Institute, 2020).

En este punto, cabe hacer referencia a la *contrainteligencia*, pues juega un papel crucial en la lucha contra la desinformación y datos falsos. Ayuda a identificar y contrarrestar actividades de espionaje y sabotaje que pueden generar o propagar

información falsa, protegiendo la información crítica y gestionando riesgos asociados a la obtención no autorizada de datos. Además, analiza amenazas potenciales, incluyendo campañas de desinformación, y promueve una cultura de seguridad dentro de las organizaciones. En este sentido, es fundamental para fortalecer la capacidad de una organización para manejar información de manera segura y precisa, evitando que las investigaciones sean susceptibles a noticias falsas, propaganda o manipulación de información. (LISA Institute, 2025).

En tercer lugar, como bien expone Heuer, la falta de contexto y la subjetividad son desafíos clave en las investigaciones OSINT. A diferencia de disciplinas como HUMINT, no permite entrevistas ni contacto directo con el sujeto u objetivo a investigar, no se conoce la intención real por la que se ha publicado la información. Además, los analistas trabajan principalmente con información de segunda mano, lo que puede derivar en conclusiones erróneas o sesgadas. Además, las percepciones personales de los analistas, posiblemente sesgadas por creencias, experiencias o expectativas, pueden ser tan engañosas como los informes de segunda mano. La falta de un contexto completo y la tendencia a confiar en lo que se observa directamente pueden resultar en conclusiones incompletas o equivocadas (1999).

En cuarto lugar, la falta de acceso a información privada o restringida limita la profundidad de las evidencias, pues no es posible obtener registros confidenciales, como historiales bancarios, llamadas telefónicas o correos privados. Tampoco se tiene acceso a las comunicaciones internas de empresas u organizaciones cerradas, ni a documentos clasificados del gobierno (Clark, 2021).

Además, a diferencia de otras disciplinas que almacenan datos de forma estable, como archivos policiales, registros oficiales o las mencionadas anteriormente, el OSINT depende de plataformas cuya accesibilidad y permanencia pueden verse alteradas. Las redes sociales, por ejemplo, pueden cambiar sus políticas, ocultar perfiles o restringir búsquedas, y los sitios web pueden desaparecer o cambiar sus URLs, lo que afecta la trazabilidad y la integridad de la investigación (Buchanan, 2020).

5. ANÁLISIS DE RESULTADOS

A continuación, se llevará a cabo un análisis exhaustivo de las seis entrevistas realizadas a profesionales del ámbito de la defensa y seguridad nacional. De este modo, se expondrán los principales resultados obtenidos en cuanto a las variables preguntadas en cada una ellas.

5.1 Estructura de inteligencia en España

Tras haber indagado sobre cómo está organizada la estructura de inteligencia en España, nos encontramos con diversas respuestas según los entrevistados, pero todos ellos mencionaron al CNI como principal organismo encargado de la inteligencia nacional.

> "Los organismos de inteligencia como el CNI, que es el equivalente al MI5 y MI6 de Reino Unido" (entrevista 2)

> "Tenemos el CNI, que es el que lleva toda la parte de inteligencia y apoya también en el CCN CERT" (entrevista 3)

> "Normalmente es el CNI, en el caso en España" (entrevista 5)

Sin embargo, en relación con la estructura de inteligencia, los profesionales muestran una diversidad de opiniones. Mientras que algunos de ellos indican que, "al igual que en Reino Unido también está muy estructurada" (entrevista 1), otros argumentan lo contrario "existe una estructura de inteligencia, pero no está muy bien definida" (entrevista 5). Respecto a esta última opinión, se comenta que, sí que existe una división de competencias en el ámbito de inteligencia, el problema está en el desconocimiento de los órganos subordinados al CNI.

Por otro lado, los organismos que forman parte de la estructura de inteligencia nacional en España, a parte del CNI, varían según el ámbito de los profesionales entrevistados.

El entrevistado 1 expuso que, dentro del CNI, nos encontramos con el Centro Criptológico Nacional, la Oficina Nacional de Seguridad y la Oficina Nacional de inteligencia y contrainteligencia. Además, añadió otros organismos con competencia en inteligencia:

- Secretaría de Estado de la seguridad: Centro de inteligencia contra el terrorismo y el crimen organizado, dentro del Ministerio del Interior.
- Comisaría General de información y la Comisaría General de Policía Judicial de la Policía Nacional.
- Servicio de Información de la Guardia Civil y la Unidad Central Operativa.
- Secretaría General de Instituciones Penitenciarias.
- Policías autonómicas:
    - Mossos d´esquadra: comisaría General de Información
    - Ertzaintza: unidad de información y análisis
    - Policía Foral de Navarra: división de información
- Servicio de Vigilancia Aduanera de la Agencia Tributaria

Además, se añade el CIFAS, centro de inteligencia de las fuerzas armadas. Este se dedica a hacer inteligencia en aquellos teatros de operaciones donde hay fuerzas militares o hay interés en desplegarlas. "En muchos de estos cuarteles de una unidad militar, tienen una parte que se dedica a hacer inteligencia para el análisis de la planificación de operaciones del enemigo" (entrevista 2). Por último, se agrega el CITCO (Centro de Inteligencia contra el Terrorismo y el Crimen Organizado) y el CENIF, (Centro Nacional de Inmigración y Fronteras) (entrevistado 6).

5.2 Aplicación del OSINT

Los profesionales coinciden en que el uso del OSINT en las FCSE resulta de gran utilidad, pues se trata de una disciplina que, "a pesar de no ser muy profunda, puede ser muy útil para investigaciones iniciales, como puede ser información sobre terreno, puertos y clima de una zona." (entrevista 1). Un ejemplo de ello lo encontramos en el ámbito de la logística, pues muchas empresas que hacen construcciones en África estudian cómo están las carreteras, cómo están los puertos y qué capacidades tienen para no tener problemas en el transporte y distribución.

El OSINT sin duda se utiliza mucho por parte de los cuerpos de seguridad, además "ellos tienen bases de datos y acceso a informaciones que nosotros desde fuera no tenemos" (entrevista 3).

Una de las aplicaciones también fundamentales del OSINT en la Guardia Civil es en la propaganda de los grupos radicales: "Para nosotros es muy importante una cosa que es básicamente OSINT, que es la evolución de la propaganda yihadista, eso sigue por OSINT. Tenemos equipos que hacen el seguimiento de la evolución de la propaganda, qué mensajes se mandan, si hay referencias a Europa, si hay referencias a España…" (entrevista 5).

Por otro lado, el entrevistado 2, hizo hincapié en que el uso de OSINT en el ámbito militar depende de dos factores: el nivel de planificación y el objetivo del análisis. En un nivel bajo de planificación operativa, la atención se centra en la zona de terreno que se debe ocupar (utilizando principalmente SIGINT, IMINT y GEOINT), por lo que las fuentes abiertas son prácticamente irrelevantes en este nivel. Sin embargo, "a medida que se asciende en el nivel de planificación, las fuentes abiertas adquieren mayor importancia. Es decir, en un análisis de muy alto nivel, especialmente en el ámbito político, las fuentes abiertas son fundamentales."

Es interesante destacar que, diferencia de la función que cumple el OSINT en los cuerpos mencionados anteriormente, en la Policía Local de Alcobendas se utiliza prácticamente en exclusiva desde un enfoque meramente preventivo.

> "La obtención de información en fuentes abiertas la usamos con el objetivo de prevenir cuestiones de todo tipo que puedan afectar a la seguridad dentro del municipio." (entrevista 6)

Es decir, no están monitorizando constantemente las fuentes abiertas, sino que lo hacen en base a hechos concretos como fiestas, concierto, concentraciones de coches… De esta forma obtienen información relevante para poder anticipar los dispositivos que realizan y organizar patrullajes, puntos de control, etc…

No obstante, la mayor parte de los entrevistados comentaron que el OSINT debe ser complementado generalmente con otras disciplinas, como HUMINT, SIGINT e IMINT, para maximizar su potencial.

> “Lo único que el OSINT solo no vale, hay que afinar la búsqueda. El OSINT solo es muy raro que sea la solución, pero siempre es una actividad complementaria a otras.” (entrevista 2)

> “No necesitas autorización judicial, lo utilizas para generar inteligencia básica y hacerte una idea global de la amenaza, o investigar a una persona concreta” (entrevista 5)

5.2.1 Otras disciplinas de investigación predominantes en el ámbito de la seguridad nacional

En cuanto a las disciplinas -INT más utilizadas en el ámbito de la seguridad nacional, a pesar de hacer uso de todas ellas complementándolas entre sí, se distinguen ciertas diferencias significativas en relación con el cuerpo al que pertenecen los entrevistados.

En la entrevista 3 se comentó que, en el ámbito policial, el HUMINT tiene más relevancia sin duda, porque es el momento en el que se hace el interrogatorio y, además, se cuenta con activos que te aportan datos (llamados colaboradores).
En la misma línea se señaló en la entrevista 5 que el HUMINT en la Guardia Civil es la disciplina más desarrollada.

> “Nosotros por historia HUMINT lo tenemos muy, muy muy muy trabajado. Para nosotros es fundamental, tenemos unas muy buenas estructuras de HUMINT y trabajo de fuentes”

Por otro lado, el GEOINT también se utiliza, pero tiene más relevancia en el ámbito militar.

> “La parte de GEOINT se utiliza, pero a nivel militar se utiliza mejor. Se utiliza más enfocado, sin duda.” (entrevista 3)

En cuanto a este aspecto, el entrevistado 4 expone que, a parte del ámbito militar, es especialmente útil para los profesionales que realizan los operativos previos a una redada, como el reconocimiento completo del lugar, barreras arquitectónicas, etc.

Un ejemplo de ello lo encontramos en la entrevista 5, donde se comenta que en la Guardia Civil también se utiliza GEOINT en determinadas ocasiones.

> "Alguna vez, pero muy poco. Para una operación en un caserío pues evidentemente, tenemos que utilizar toda la información geográfica por dónde entrar, qué hacer, si ponemos un helicóptero, si no o si patrullas. Bueno, eso se utiliza." (entrevista 5)

Respecto al IMINT, no se hace mucha referencia. Sin embargo, en la entrevista 5 se menciona que, aunque IMINT se asocia con la obtención de imágenes, debería incluir un análisis más profundo. IMINT se utiliza para obtener imágenes en tiempo real o fotografías y analizarlas para entender la evolución de estructuras o actividades. Sin embargo, cuando solo se necesita una imagen en tiempo real para una operación, no siempre se considera IMINT en su totalidad.

La utilización del SIGINT también se utiliza en cierto modo en toda la parte de señales, intervenciones telefónicas o balizamiento… "Para nosotros son medidas de investigación básicas." (entrevista 5)

5.3 Perfil profesional en OSINT

En cuanto a la descripción del perfil idóneo de un investigador en fuentes abiertas, a grandes rasgos todos los entrevistados coincidieron en las siguientes características:

1. Capacidad de análisis: Habilidad para realizar análisis profundos que van más allá del simple conocimiento de las herramientas disponibles.
2. Conocimiento del ámbito: Pleno conocimiento del contexto en el que se enmarca la investigación ya sea en el sector empresarial, público u otro.
3. Técnicas de recopilación de datos: Competencia en el uso de motores de búsqueda, metabuscadores, herramientas de extracción de datos, aplicaciones de monitorización y herramientas de análisis de metadatos.
4. Fuentes de información: Conocimiento exhaustivo de diversas fuentes de información, incluyendo bibliotecas, librerías, revistas y entrevistas.

5. Habilidad en búsqueda y evolución: Capacidad para mantenerse actualizado en el uso de herramientas de obtención y análisis de datos, demostrando destreza en la búsqueda y adaptación a nuevas tecnologías.
6. Meticulosidad: Atención al detalle y precisión en el trabajo realizado.
7. Pasión por los datos: Entusiasmo por el manejo de datos, con un perfil similar al de un periodista, caracterizado por la curiosidad y la perspicacia para ir más allá de la información superficial y extraer datos relevantes de páginas web y perfiles.
8. Solución de problemas: Capacidad para aportar soluciones efectivas en la obtención y análisis de información.
9. Capacidad de procesamiento: Habilidad para manejar documentación estructurada y no estructurada, bases de datos e información dispersa, destacando la importancia del procesamiento previo al análisis y el filtrado de información.

Sin embargo, también se han hecho distinciones según la estructura y el enfoque de trabajo de los equipos OSINT. El entrevistado 5 remarca los dos enfoques de trabajo existentes actualmente en las Fuerzas Armadas y en la Guardia Civil:

> "Hay dos tipos de estructuras, una que tienen las Fuerzas Armadas, en la que los equipos OSINT son equipos a disposición de cualquier analista convirtiéndose en equipos independientes y, por tanto, deben ser personas muy generalistas."

> "La otra es como lo estemos establecido nosotros en la Guardia Civil, por amenazas. No tenemos un equipo OSINT, tenemos muchos equipos OSINT especializados, el equipo trabaja con la amenaza directamente."

5.4 Fuentes analizadas según el procesamiento de la información

En cuanto a la utilización de fuentes primarias, secundarias y terciarias de información, todos los profesionales coinciden en que recurrir a las fuentes primarias son siempre el principal objetivo para hacer un buen análisis, puesto que "cuanto más proceso tenga, más sesgo tiene el medio". (entrevista 2)

En las investigaciones siempre se empiezan por las fuentes primarias, sin embargo, a medida que va avanzando el análisis se va complementando con fuentes secundarias y terciarias. Un ejemplo de ello es que "las fuentes secundarias se utilizan para validar las informaciones que hemos obtenido de manera inicial, para saber que se trata del mismo perfil que se está buscando y para validar también que esta información sea correcta" (entrevista 3).

Como bien comenta el entrevistado 5, un aspecto para tener en cuenta es la posibilidad de que las fuentes secundarias y terciarias envenenen o falseen el análisis. Requiere de un nivel de alerta mayor trabajar con ellas, es posible que cinco países comuniquen la misma noticia, pero ¿dicen lo mismo con medios propios o dicen lo mismo porque están integrando información de un tercero que ya los ha llevado por este camino?

5.5 Métodos de obtención de información realizados

Respecto a los métodos de obtención de información en investigaciones OSINT (activa, pasiva o semi pasiva), se expone que, independientemente del ámbito, predomina siempre la investigación pasiva, aquella en la que el objetivo no sabe que está siendo analizado.

> "El OSINT pasivo es la mejor y es la base de todo esto. Hamás tuvo publicaciones, revistas, periódicos, publicaciones especializadas… un montón de cosas que te dan mucha información de inteligencia básica" (entrevista 5)

Sin embargo, en numerosas ocasiones resulta necesario pasar a un modo semi activo o incluso activo, pues "es una inteligencia de oportunidad y no encuentras lo que buscas, sino que encuentras lo que existe". Este otro modo de investigación en ocasiones es necesario para obtener información del atacante, con el fin de rastrear quien está detrás, obtener información adicional sobre sus tácticas, técnicas y procedimientos y poder analizarlo para deducir si se trata de un grupo determinado (iraní, ruso, chino…) entre otras cosas. (entrevista 1). Además, "las unidades de inteligencia suelen tener sus contactos y suelen tener fuentes incluso que colaboran activamente y que son perfectamente conocedores de que están colaborando, aunque ahí estaríamos ante HUMINT". (entrevista 2)

No obstante, resulta complicado diferenciar entre una obtención de información activa y una intervención policial ordinaria, pues en toda obtención de información activa OSINT se cuenta con un *agente encubierto virtual*, identidad suplantada bajo orden judicial que únicamente pueden hacer uso de ello las FCSE. (entrevista 5)

5.6 Ciclo de inteligencia

El ciclo de inteligencia, tal como lo reconocen la mayoría de los entrevistados, se refiere al modelo definido por el CNI, aplicando en algunas ocasiones una variante muy similar ajustada al ámbito de operaciones. Un ejemplo de ello es en la planificación militar, pues a partir del plan de operaciones y los objetivos, se orienta la inteligencia y se le comunica a la sección correspondiente.

> "El ciclo de inteligencia del ejército es prácticamente el mismo que el del CNI. La diferencia está en dónde se plantea." (entrevista 2)

En términos generales, el ciclo de 6 fases se extrapola al ámbito deseado. Sin embargo, dentro de los FCSE, la división del ciclo puede variar en determinadas ocasiones. Esta información es muy hermética e inaccesible, por lo que no se conoce con certeza.

Además del ciclo de inteligencia, en la entrevista 1 se explica un protocolo que enmarca de manera general las investigaciones en fuentes abiertas:

1. Identificación de la fuente: quién sabe de qué, valoración de fuentes, uso de motores de búsqueda: redes sociales, blog, wikipedia, foros, Deep web…
2. Explotación de fuentes de información: buscar medios para poder explotar esa fuente de información, extraer la información, descargar vídeos... Por ejemplo: medios de comunicación, periódicos, televisión, revistas, radio, bases de datos pública, eventos, conferencias, temáticas.
3. Recolección de datos: se pueden emplear herramientas como Google Hacking, OSINT Framework, Maltego, Sodan, Megadow…

4. Procesamiento de datos: organización, estructuración de los datos recopilados para facilitar el análisis, crear la línea temporal…
5. Análisis de los datos procesados y recopilados: instalar información útil y posteriormente generar inteligencia: generación de informe, producto de inteligencia, recomendaciones basadas en análisis de los datos…
6. Distribución de la información

El ciclo de inteligencia es una herramienta fundamental que se adapta según las estructuras y capacidades disponibles. Generalmente, se divide en cuatro fases, pero estas pueden variar, especialmente en las fases de obtención y elaboración, dependiendo de si los equipos OSINT están integrados o no. Si los equipos no están integrados, se deben hacer peticiones a otras unidades que tienen su propio ciclo de obtención.

Esto se traduce en dos enfoques básicos del ciclo de inteligencia:

1. Sin acceso directo entre el elaborador y el obtenedor: En este caso, el grupo que desarrolla y diseña la investigación (elaborador) no tiene acceso directo al grupo que recolecta los datos (obtenedor). “En algunos sistemas, esta separación se mantiene estrictamente para asegurar una valoración más aséptica y objetiva, porque, aunque se pierde agilidad, se gana en objetividad” (entrevista 5). Los servicios de inteligencia más tradicionales suelen utilizar estructuras estancas y separadas para garantizar esta objetividad.
2. Con acceso directo entre el elaborador y el obtenedor: el elaborador tiene acceso directo al obtenedor, lo que puede hacer el proceso más ágil pero también más subjetivo.

> “Nosotros preferimos la valoración estrecha, que puede sacrificar un poco de objetividad inicial, pero se compensa con las revisiones y diligencias posteriores para asegurar la precisión y objetividad de los resultados.” (entrevista 5)

5.7 Desafíos y retos de la investigación en fuentes abiertas

En primer lugar, la infointoxicación y la desinformación son los principales retos en OSINT, ya que "la cantidad abrumadora de información disponible en Internet hace que filtrar y analizar datos relevantes sea una tarea monumental. Cada vez más personas publican contenido en línea, lo que complica aún más esta labor" (Entrevista 1). Además, la integración de datos de múltiples fuentes y formatos para obtener una visión coherente y completa puede ser complicado. La calidad y veracidad de la información también es un desafío, debido a la proliferación de noticias falsas y opiniones que dificultan obtener información de calidad. "Aunque las opiniones pueden ser interesantes si provienen de influenciadores, generalmente no son útiles para la inteligencia y pueden polarizar" (Entrevista 1). En este sentido, es crucial evitar la polarización, trabajando con una mente abierta, buscando datos objetivos y evitando prejuicios.

Otro reto importante es el tiempo y la cronología, ya que establecer una línea temporal precisa es complicado debido a las fechas de publicación y modificación de los artículos en Internet. Además, la evolución de las personas en el tiempo puede hacer que la información antigua en Internet no refleje las opiniones actuales de las personas.

> "Internet puede tener información muy antigua que no significa que una persona que escribió hace 20 años una cosa siga pensando de la misma manera." (Entrevista 1)

Por otro lado, también existe un sesgo de exposición que lleva a juzgar más a las personas que están más expuestas en las redes. También, la tendencia a la viralización y el uso de IA presenta riesgos, ya que la inteligencia artificial puede dar verosimilitud a informaciones virales que no son necesariamente veraces.

> "Es un sexto sentido que el analista tiene que desarrollar con su experiencia profesional y con conocimiento que va más allá de lo que son las herramientas." (Entrevista 2)

Para hacer un buen análisis, es necesario especializarse en el área correspondiente. El analista sólo con su conocimiento y sus herramientas de lo que es el OSINT, no le valdría para hacer un análisis adecuado." (Entrevista 2)

Además, el aumento de la garantía de privacidad complica el acceso a la información, a veces requiriendo pequeñas vulneraciones o engaños para obtener datos.

> "Ahora esto lo va complicando, por eso tienes que dar un pequeño salto, normalmente de pequeña vulneración o de un pequeño engaño, etcétera para entrar."

Finalmente, las herramientas tecnológicas son cada vez más sofisticadas y caras, y la transparencia y garantías que se les da a los ciudadanos en la adquisición de estas herramientas puede ralentizar el proceso. Además, la colaboración con empresas, especialmente en redes sociales y telefonía, es complicada porque priorizan la seguridad del ciudadano, lo que dificulta la colaboración con los analistas de OSINT.

> "Pasó con BlackBerry, que era la referencia y nosotros hacía años que interveníamos. Cuando empezaron a salir las sentencias en las que se veía claramente que la Guardia Civil intervenía la mensajería, BlackBerry desapareció del mercado." (Entrevista 5)

Cabe mencionar que la globalización se ha señalado como otro reto significativo debido a la diversidad de idiomas.

5.8 Integración de la inteligencia artificial en las investigaciones OSINT

La Inteligencia Artificial es concebida por todos los entrevistados como una herramienta sumamente útil que simplificará tareas objetivas tales como: la generación de contenidos, la adquisición y alimentación de perfiles, las traducciones y la automatización de diversas tareas. Del mismo modo, también coinciden en que no supondrá un obstáculo en sí misma, sino que los riesgos asociados a esta emergente tecnología provendrán de su mal uso.

> “Será mucho más fácil y mucho más sencillo, siempre y cuando sepamos usar las herramientas de inteligencia artificial” (entrevista 4)

> “Todo avance siempre va a suponer un reto, por ello, los profesionales deben adaptarse a ellos, ese será el verdadero reto de los investigadores: “poder estar a la vanguardia de todo lo nuevo.” (Entrevista 4)

Algunos de los posibles desafíos asociados con la IA son:

- Aumento de la desinformación
- Viralización de noticias falsas
- Mejora en la creación de identidades falsas
- Deepfakes: dificultad de detectar falsedades extremadamente realistas que pueden llegar a desestabilizar un país.
- Información aportada por la IA considerada como falsa

5.9 Perspectivas futuras del OSINT

El OSINT se percibe como una herramienta útil y con gran potencial. Las empresas están comenzando a implementar sistemas de OSINT en sus organizaciones para la selección de personal, inteligencia competitiva, análisis de mercado y la identificación de amenazas en desplazamientos al exterior de su personal.

En todos estos ámbitos, el OSINT tiene un futuro prometedor. Se espera que en poco tiempo surjan herramientas muy potentes capaces de realizar análisis complejos, como la evaluación de riesgos cibernéticos. Sin embargo, será necesario verificar la fiabilidad de estas herramientas y no confiar únicamente en ellas, pues “la persona no tiene probablemente capacidad de procesar tanta información como la inteligencia artificial, pero hoy por hoy puede juzgar mejor que ella.” (entrevista 2)

6. DISCUSIÓN DE RESULTADOS

A continuación, se examinarán los resultados de las entrevistas mencionadas anteriormente, relacionándolos con el marco teórico. Este análisis tiene como objetivo

profundizar en el uso de la investigación en fuentes abiertas (OSINT) en el ámbito de la seguridad nacional, así como identificar posibles tendencias y relaciones entre los resultados.

6.1 Estructura de inteligencia en España

Como se ha expuesto anteriormente en el marco teórico, el CNI es el principal organismo encargado de la seguridad nacional e internacional, sin embargo, nos encontramos con diversas variantes del ciclo de inteligencia según el país o el organismo que lo define. Actualmente en España el CNI lo divide en 4 fases: dirección, obtención, elaboración y difusión y el INCIBE en 6 fases: requisitos, fuentes de información, adquisición de información, procesamiento de datos, análisis e inteligencia. A continuación, se hizo una comparación de estos ciclos de inteligencia frente a otros de interés, como el de la Agencia Central de Inteligencia (CIA) de Estados Unidos y el Joint Doctrine Publication (JDP 2-00) del Reino Unido. Aunque existen diferencias en la nomenclatura y en algunas etapas intermedias, todos estos ciclos comparten una base común, lo cual es crucial para la precisión y la eficacia de la inteligencia.

En las entrevistas realizadas a profesionales del ámbito de la defensa y seguridad nacional, se buscó conocer no solo cuál era el ciclo que realmente definía sus operaciones, sino también qué organismos conformaban la estructura de inteligencia a nivel nacional.

Los entrevistados aportaron una perspectiva práctica sobre la estructura y ciclo de inteligencia en España. Todos confirmaron la premisa de que el CNI es el principal organismo encargado de la inteligencia nacional; sin embargo, en lo referente a la estructura global, algunos profesionales consideran que está bien definida y organizada, similar a la del Reino Unido, mientras que otros opinan que falta claridad y definición en la división de competencias y en el conocimiento de los órganos subordinados. Esta diversidad en cierto modo es un reflejo de la complejidad y los desafíos que enfrenta la estructura de inteligencia en España.

Además, las entrevistas dan a conocer otros organismos que forman parte de la estructura de inteligencia nacional, como el Centro Criptológico Nacional, la Oficina

Nacional de Seguridad, y la Oficina Nacional de Inteligencia y Contrainteligencia (que dan apoyo al CNI), el Centro de Inteligencia contra el Terrorismo y el Crimen Organizado, y diversas unidades de la Policía Nacional y la Guardia Civil (actualmente llamadas de información).

6.2 Aplicación del OSINT

A lo largo del marco teórico, se explica la evolución y relevancia del OSINT en la era digital, pues ha ganado importancia en múltiples contextos, desde la seguridad nacional hasta el análisis empresarial, el periodismo y el marketing. En España, el desarrollo del OSINT ha seguido tendencias internacionales y comenzó a ganar relevancia en las últimas décadas del siglo XX. De hecho, las agencias españolas han integrado fuentes abiertas como complemento a otras formas de inteligencia, como HUMINT (Inteligencia Humana) y SIGINT (Inteligencia de Señales).

Las entrevistas realizadas a profesionales del ámbito de la defensa y seguridad nacional reconocen el gran papel que juega el OSINT en las FCSE. Se destaca que se trata de una herramienta complementaria a otras disciplinas de inteligencia, como HUMINT, SIGINT e IMINT y que resulta especialmente útil, por ejemplo, para analizar propagandas terroristas y para la planificación operativa militar, proporcionando la evolución de mensajes y referencias en la propaganda, así como información inicial sobre terreno, puertos y clima... Sin embargo, como bien he comentado anteriormente, es importante destacar que el OSINT debe ser complementado con otras disciplinas para maximizar su potencial. Puede proporcionar una visión global de la amenaza y generar inteligencia básica, pero es raro que sea la solución completa por sí solo, por lo que es necesario afinar la búsqueda y combinar el OSINT con HUMINT, SIGINT e IMINT para obtener una inteligencia más precisa y detallada.

6.2.1 Otras disciplinas de investigación predominantes en el ámbito de la seguridad nacional

Enlazando con la premisa de que *el OSINT debe ser complementado con otras disciplinas para maximizar su potencial,* en el marco teórico se exponen las disciplinas de

inteligencia consideradas más relevantes en la actualidad (HUMINT, GEOINT, MASINT, SIGINT, TECHINT, CYBINT/DNINT, FNINT e IMINT), con el fin de contrastar cuáles de ellas son las más utilizadas por las FCSE y para qué tipo de operaciones.

Cada disciplina aporta una perspectiva única y permite obtener una base sólida para entender cómo se integran y complementan entre sí para generar inteligencia accionable.

En primer lugar, se destacó el HUMINT en el ámbito policial y de la Guardia Civil como la más valiosa y utilizada. Los entrevistados señalan que es fundamental para la recopilación de información a través de interrogatorios y agentes colaboradores. Por otro lado, se menciona el uso del GEOINT especialmente en operaciones militares y policiales, para el reconocimiento completo del lugar y la planificación de operaciones, entre otras cosas. El SIGINT también es utilizado, por ejemplo, en intervenciones telefónicas y balizamiento, consideradas acciones de investigación básicas. Aunque el IMINT no se menciona con frecuencia, se reconoce su importancia para obtener imágenes en tiempo real y analizar la evolución de estructuras o actividades.

Por lo que se deduce que, disciplinas no mencionadas como el FNINT, MASINT y DNINT, son menos utilizadas o se recurre a ellas en operaciones más concretas y menos frecuentes.

Esta información complementa y amplía la visión presentada en el marco teórico, proporcionando detalles adicionales sobre la aplicación práctica de estas disciplinas en el ámbito de la seguridad nacional.

6.4 Perfil profesional en OSINT

En el marco teórico se describen las cualidades y habilidades más importantes que debe poseer un investigador OSINT. En ellas, se enfatiza la importancia de la capacidad de análisis, el conocimiento del ámbito de investigación, el manejo adecuado de herramientas especializadas, el enfoque analítico y estructurado y la comprensión de cómo fluye la información en internet, entre otras. La descripción de estas cualidades en el marco teórico sirve como fundamento para entender qué se espera de un investigador OSINT y cómo puede maximizar su eficacia en la recopilación y análisis de información.

Los profesionales del ámbito de la defensa y seguridad nacional coinciden en las características esenciales de un investigador OSINT, sin embargo, añaden otras de gran importancia como la habilidad para mantenerse actualizado, el entusiasmo por el manejo de datos, curiosidad, perspicacia, capacidad para aportar soluciones efectivas en la obtención y análisis de información, habilidad para manejar documentación estructurada y no estructurada y, sobre todo, pleno conocimiento del contexto en el que se enmarca la investigación ya sea en el sector empresarial, público u otro.

Además, se mencionan dos perfiles según el enfoque de trabajo: equipos OSINT independientes predominante en las Fuerzas Armadas (perfil investigador muy generalista que analiza todo tipo de amenazas) y equipos especializados predominante en la Guardia Civil (perfil investigador más especializado en amenazas concretas que son de su competencia).

6.5 Desafíos y retos de la investigación en fuentes abiertas

Como se ha comentado a lo largo de esta investigación, actualmente existen múltiples dificultades y retos a las que un investigador debe hacer frente, incluso teniendo formación y herramientas suficientes. Más bien se trata de retos que no dependen del investigador en sí, sino del entorno y ámbito que le rodea.

En este punto, se ha intentado recopilar la mayor cantidad de retos y dificultades a las que se enfrentan los profesionales de las FCSE. El objetivo es conocer con precisión la situación actual y los desafíos específicos que afectan a estos profesionales en el desempeño de sus funciones. Esta recopilación busca proporcionar una visión detallada y exhaustiva de los obstáculos que deben superar, así como de las necesidades y áreas de mejora que podrían optimizar su labor en el ámbito de la seguridad y defensa nacional.

Las grandes cantidades de información, una mayor vulnerabilidad a la desinformación y datos falsos la falta de contexto y la subjetividad, la falta de acceso a información privada o restringida y la alteración de la accesibilidad y permanencia de los datos, son los principales retos detectados a partir de la revisión bibliográfica. A parte de ellos, todos los profesionales destacan la *infointoxicación* y la *desinformación* como los principales retos en las investigaciones OSINT.

Además de estos desafíos, los entrevistados destacan otros retos emergentes que se presentan con el avance continuo de la era digital y no han sido detectados en el marco teórico.

Existe un sesgo de exposición que lleva a juzgar más a las personas que están más expuestas en las redes; la tendencia a la viralización y el uso de inteligencia artificial presentan riesgos, ya que la IA puede dar verosimilitud a informaciones virales que no son necesariamente veraces; el aumento de la garantía de privacidad complica el acceso a la información, a veces requiriendo pequeñas vulneraciones o engaños para obtener datos; las herramientas tecnológicas son cada vez más sofisticadas y caras, y la transparencia y garantías que se les da a los ciudadanos en la adquisición de estas herramientas puede ralentizar el proceso; la colaboración con empresas, especialmente en redes sociales y telefonía, es complicada porque priorizan la seguridad del ciudadano.

Por último, considero importante destacar que, como bien ha comentado el entrevistado 5, la globalización ha generado que la diversidad de idiomas presente desafíos significativos. En un mundo cada vez más interconectado, la comunicación efectiva entre personas de diferentes culturas y lenguas se ha vuelto esencial. Esto implica no sólo la necesidad de aprender nuevos idiomas, sino también de comprender las sutilezas culturales y contextuales que acompañan a cada lengua. La barrera del idioma no radica únicamente en la traducción, sino en la interpretación precisa de los significados y connotaciones. Aunque las herramientas de traducción automática, como Google Translate, pueden facilitar la traducción de palabras y frases, no siempre capturan las connotaciones culturales y contextuales específicas de cada idioma. Los traductores profesionales, que suelen actuar como intérpretes, desempeñan un papel crucial en este proceso. Un intérprete puede identificar que una palabra tiene connotaciones totalmente distintas en diferentes contextos y necesita comprender el contexto completo para interpretar correctamente el significado. Esta capacidad es esencial para desentrañar ideologías y asegurar una comunicación precisa y efectiva, superando las barreras lingüísticas que pueden dificultar la comprensión intercultural.

7. CONCLUSIONES

A lo largo de este trabajo, se ha tratado de abordar cuál es papel de la inteligencia en fuentes abiertas en nuestro país.

El objetivo principal ha consistido en analizar la utilidad, el uso y el futuro de esta técnica en el ámbito de la defensa y seguridad nacional. Para alcanzar este objetivo, se han llevado a cabo seis entrevistas con profesionales del ámbito de la defensa y seguridad nacional (incluyendo militares, guardias civiles e instructores de diversos cuerpos policiales), con el propósito de investigar diversas cuestiones que, en general, no están al alcance de todos. Se ha realizado un análisis exhaustivo de los argumentos presentados, del cual se han extraído diversas conclusiones que permiten comprender en profundidad el uso de las fuentes abiertas. Este análisis también ofrece una perspectiva sobre su posible evolución futura y el impacto que podría tener la IA en las investigaciones.

En primer lugar, gracias a los resultados obtenidos se puede afirmar que las fuentes abiertas, a pesar de ser una herramienta complementaria a otras disciplinas de inteligencia, juegan un papel fundamental en las FCSE. Esta combinación de disciplinas permite a las FCSE desarrollar estrategias más efectivas y tomar decisiones informadas, mejorando así la seguridad y la eficacia operativa. Su utilidad y versatilidad es especialmente notable en áreas como ciberterrorismo, ciberseguridad, inteligencia militar, seguridad en el transporte, seguridad en la logística, análisis de amenazas… (entre muchas otras).

En segundo lugar, los resultados obtenidos nos llevan a la conclusión de que, efectivamente, no hay establecidos unos criterios concretos para trabajar como investigador en fuentes abiertas. Esto se debe a la naturaleza dinámica y diversa del campo de la inteligencia de fuentes abiertas (OSINT). A diferencia de otras disciplinas, donde existen estándares y certificaciones claramente definidos, el ámbito de OSINT se caracteriza por la flexibilidad y la adaptabilidad a diferentes contextos y necesidades.

Sin embargo, se comprueba que sí que existen ciertas características que cualquier OSINTER debe poseer para cumplir con el perfil idóneo. Los resultados confirman que debe tener una combinación de habilidades analíticas, técnicas y contextuales. Es fundamental que el investigador tenga una capacidad de análisis destacada, un conocimiento profundo del ámbito de investigación, y un manejo adecuado de

herramientas especializadas. Además, debe adoptar un enfoque analítico y estructurado y comprender cómo fluye la información en internet.

En tercer lugar, en cuanto a los tipos de información que se consultan para las investigaciones, se puede establecer que se consultan los tres tipos de fuentes de información: primarias, secundarias y terciarias; cada una con su propio valor y utilidad en el proceso de análisis.

Los resultados nos llevan a la conclusión de que las fuentes primarias son las más valoradas y utilizadas en las investigaciones, ya que proporcionan información directa y sin intermediarios. Por otro lado, las fuentes secundarias se utilizan para complementar y validar la información obtenida de las fuentes primarias, y las fuentes terciarias se tratan de evitar al contener posibles sesgos o errores en el análisis.

En cuarto lugar, los datos obtenidos indican que indudablemente son muchos los desafíos presentes en una investigación en fuentes abiertas. De hecho, la mayoría de estos desafíos, no dependen únicamente de su formación o herramientas, sino del entorno y ámbito que les rodea. Es por ello que a medida que siga avanzando la era tecnológica, seguirán aumentando los desafíos de forma proporcional. Un ejemplo de ello es el efecto que ha tenido la globalización en la inteligencia de un país. Por un lado, ha facilitado la transferencia de conocimientos y tecnología a través de fronteras, permitiendo una mayor cooperación internacional y el intercambio de información entre agencias de inteligencia. Sin embargo, también ha planteado retos significativos relacionados con el idioma y la interpretación, ya que dificulta la comunicación efectiva entre personas de diferentes culturas y lenguas.

En este contexto, también se han analizado el posible futuro que le espera al OSINT. Tras recoger los resultados obtenidos en las entrevistas, se espera que el futuro del OSINT sea prometedor. Se conoce que las empresas están comenzando a integrar sistemas de OSINT en sus operaciones diarias, reconociendo su capacidad para proporcionar información valiosa y mejorar la toma de decisiones estratégicas. Además, se espera que surjan herramientas cada vez más potentes y sofisticadas capaces de realizar análisis complejos, como la evaluación de riesgos cibernéticos. Estas herramientas avanzadas podrán procesar grandes volúmenes de datos y detectar patrones que podrían pasar desapercibidos para los analistas humanos. Sin embargo, es crucial mantener un enfoque equilibrado y no depender exclusivamente de la tecnología.

El OSINT promete un futuro brillante, con un potencial considerable para revolucionar la forma en que las organizaciones recopilan y utilizan la información. El éxito dependerá de la integración equilibrada entre tecnología avanzada y juicio humano, permitiendo a las empresas y profesionales de la seguridad maximizar el uso de esta poderosa herramienta.

En quinto y último lugar, se los resultados permiten concluir que la Inteligencia Artificial (IA) será sin duda una herramienta sumamente útil para el OSINT, simplificando tareas como la generación de contenidos, la adquisición y alimentación de perfiles, las traducciones y la automatización de diversas tareas. Sin embargo, no podremos dejar de lado que conllevará también múltiples riesgos, generalmente asociados al mal uso. Todo avance tecnológico supone un reto, y los profesionales deberán adaptarse a estos cambios para mantenerse a la vanguardia.

Por último, considero importante destacar que, aunque la inteligencia artificial puede manejar y analizar datos a una escala impresionante, la capacidad de juicio humano sigue siendo insustituible para interpretar y evaluar la información de manera contextual y crítica. Por lo tanto, el futuro del OSINT dependerá de una integración equilibrada entre la tecnología avanzada y la inteligencia humana.

8. LIMITACIONES DEL ESTUDIO

Durante la realización de este trabajo, se han encontrado varios límites que han influido en el desarrollo y la profundidad de la investigación.

Uno de los principales desafíos ha sido el acceso restringido a información sensible y clasificada. Aunque el OSINT se basa en fuentes abiertas, la naturaleza de la información manejada por las FCSE implica que ciertos datos no puedan ser divulgados. Esta restricción ha limitado en cierto modo la profundidad de algunos análisis y la obtención de ejemplos prácticos.

Otro límite significativo ha sido la disponibilidad de los miembros de las FCSE para participar en entrevistas. Debido a sus responsabilidades y horarios impredecibles, coordinar entrevistas ha requerido una gran flexibilidad.

Mantener la confidencialidad y adherirse a las normas éticas ha sido otro aspecto crucial. Esto ha implicado obtener consentimientos informados y asegurar que la información proporcionada por los entrevistados se maneje de manera responsable. La necesidad de proteger la identidad y la seguridad de los participantes ha limitado la posibilidad de incluir ciertos detalles en el trabajo.

En resumen, los límites encontrados en la realización de este trabajo han sido diversos y han requerido una gestión cuidadosa para asegurar que la investigación se llevara a cabo de manera ética y rigurosa. A pesar de estos desafíos, se ha logrado recopilar información valiosa que contribuye al entendimiento del OSINT y su aplicación en el contexto de las FCSE.

9. LÍNEAS FUTURAS

Durante la realización de este trabajo, se han identificado nuevas líneas de investigación que no estaban contempladas inicialmente en las entrevistas planificadas. La información obtenida y las perspectivas de los miembros de las Fuerzas y Cuerpos de Seguridad del Estado han revelado temas y enfoques adicionales de gran interés para el campo del OSINT.

Estas nuevas líneas de investigación ofrecen oportunidades para ampliar el conocimiento existente y abordar cuestiones relevantes para la práctica profesional y la formulación de políticas. En este apartado, se presentan las propuestas emergentes que pueden contribuir a un entendimiento más completo de esta temática.

La primera posible línea futura de investigación podría centrarse en las diferencias entre el sector público y el sector privado, especialmente en relación con los protocolos. En el ámbito empresarial, las empresas tienen mayor libertad para establecer sus propios procedimientos, siempre y cuando cumplan con las leyes vigentes. Cada empresa puede desarrollar políticas internas y cuestionarios de cumplimiento para asegurar que sus socios comerciales cumplen con los mismos estándares.
En contraste, en el sector público, y en particular las FCSE, se opera bajo protocolos rígidos y estandarizados. La asignación de recursos y la ejecución de esfuerzos se planifican meticulosamente para garantizar la eficacia y seguridad en las operaciones.

Investigar estas diferencias podría ofrecer valiosas perspectivas sobre cómo optimizar los protocolos en ambos contextos. Esta línea de investigación podría explorar cómo las mejores prácticas del sector privado pueden ser adaptadas al sector público y viceversa, mejorando la eficiencia y efectividad en ambos ámbitos.

La segunda línea futura de investigación podría centrarse en el papel crucial de la contrainteligencia en la seguridad y eficacia de las operaciones de inteligencia, especialmente en contextos de alta amenaza como el terrorismo y el ciberterrorismo. Esta no solo se enfoca en la detección y neutralización de amenazas externas, sino también en la implementación de medidas preventivas que fortalezcan la seguridad operativa y minimicen los riesgos de exposición.

Investigar cómo la contrainteligencia puede mejorar la seguridad operativa y la eficacia de las operaciones de inteligencia en estos contextos de alta amenaza podría proporcionar valiosas perspectivas.

En tercer lugar, las diferencias en el desarrollo del OSINT entre distintos países son significativas y están influenciadas por diversos factores, como los recursos tecnológicos disponibles, las políticas gubernamentales y las necesidades específicas de seguridad. En países como Argentina, el desarrollo del OSINT ha sido impulsado por la necesidad de compensar la falta de recursos tecnológicos avanzados. Las fuerzas de seguridad argentinas han perfeccionado técnicas manuales y métodos innovadores para la recopilación y análisis de información de fuentes abiertas, debido a la limitada disponibilidad de software y hardware especializados.

Por otro lado, en países como España, las fuerzas de seguridad cuentan con mayores recursos financieros y tecnológicos, lo que les permite adquirir herramientas avanzadas que automatizan muchas de las tareas de OSINT. Esta diferencia en recursos tecnológicos facilita la implementación de OSINT en España, pero también puede resultar en una menor necesidad de desarrollar habilidades manuales y técnicas innovadoras.
Estas diferencias reflejan cómo cada país adapta el uso de OSINT a sus circunstancias particulares, lo que puede ofrecer valiosas perspectivas sobre cómo optimizar el uso de OSINT en diferentes contextos.

Para finalizar, la importancia de la prevención mediante el uso de OSINT (Open Source Intelligence) en las operaciones policiales es una línea futura de investigación fundamental. La inteligencia obtenida de fuentes abiertas permite a las fuerzas de seguridad anticiparse a posibles amenazas y planificar sus acciones de manera más efectiva. Esta información permite establecer barreras preventivas, mitigar riesgos mayores y ajustar su despliegue para garantizar la seguridad y el orden público. La prevención es fundamental, y el uso de OSINT permite a las fuerzas de seguridad adelantarse a los posibles escenarios, optimizando sus recursos y estrategias para evitar situaciones de riesgo.

Considero que, dado que la prevención mediante el uso de OSINT es fundamental para la seguridad pública, su estudio puede contribuir significativamente a la eficacia de las operaciones policiales.

10. REFERENCIAS

Bielska, A., Kurz, N. R., Baumgartner, Y., & Benetis, V. (2020). *Open source intelligence: Tools and resources handbook.*

Bruno, G. y Sumer Elías, M. (s.f.). *Introducción a OSINT.* Periodistas Ambientales. https://periodistasambientales.org/introduccion-a-osint/

Buchanan, B. (2020). *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics*. Harvard University Press.

Calvo, C. P. (2025). *Buscadores especializados.* Euroinnova International. Online Education. https://bit.ly/4idDtej

Carcaño Domouso, F. (2018). *Qué son las fuentes abiertas.* OpenWebinars. https://openwebinars.net/blog/que-son-fuentes-abiertas/

Castillejo Cano, D. (2024). *Ciclo de inteligencia nacional: errores y propuestas operativas*. Ministerio de Defensa. https://bit.ly/42odDy2

Cilleruelo, C. (2024). *¿Qué es FININT?* KeepCoding Bootcamps. https://keepcoding.io/blog/que-es-finint/

Clark, R. M. (2021). *Análisis de inteligencia: un enfoque centrado en el objetivo* (4ª ed.). Bosch Editor.

Código Penal. (2020). Artículo 197.2. España. Ministerio de Justicia.

Código Penal. (2020). *Artículo 197 bis 1*. España: Ministerio de Justicia

Código Penal. (2020). Artículo 249. España. Ministerio de Justicia.

Código Penal. (2020). Artículo 401. España. Ministerio de Justicia.

Comunidad GINSEG. (2020). *Legislación y ética en la ciberinteligencia y OSINT*. Cibervigilancia Ciberinteligencia OSINT. https://www.ginseg.com/ciberinteligencia/legislacion-osint/

Cuartel General de Comunicaciones del Gobierno (GCHQ). (2025, 28 febrero). En *Wikipedia*. Recuperado de https://es.wikipedia.org/wiki/GCHQ

Cybermentor. (2025, abril 4). *OSINT: Qué es, aplicación. Cybermentor.* https://cybermentor.net/osint-que-es-aplicacion/

Equipo IUCPOL. (2023). *Introducción e Historia del OSINT*. IUCPOL. https://bit.ly/42B88xn

Fernández, D. J. (2023). *Límites legales en la obtención de información de fuentes abiertas.* Sec2Crime. https://bit.ly/426AJdV

Ferreira, J. (2024). *OSINT Aplicado a Redes Sociales: Obtener información de personas y empresas a través de las fuentes abiertas.* Ediones PY Sello Editorial.

González, J. A. (s.f.). *Open Source Intelillence.* [Archivo PDF]. Comunicación personal.

Gutiérrez, J. (s.f). *Curso gratis OSINT: Técnicas + Herramientas* [Curso en línea]. CIBERPATRULLA. Recuperado de https://ciberpatrulla.com/curso-osint-gratuito/

Heuer, R. J. (1999). *Psychology of Intelligence Analysis*. Center for the Study of Intelligence.

Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones. *Boletín Oficial del Estado*, núm. 251, de 10 de mayo de 2014, pp. 43201-43208. Recuperado de https://www.boe.es/buscar/act.php?id=BOE-A-2007-18243

Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico. *Boletín Oficial del Estado*, núm. 166, de 12 de julio de 2002, pp. 25388-25403. Recuperado de https://www.boe.es/buscar/act.php?id=BOE-A-2002-13758

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. *Boletín Oficial del Estado*, núm. 294, de 6 de diciembre de 2018, pp. 119-1 a 119-88. Recuperado de https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673

LISA Institute. (2020). *OSINT (Inteligencia de Fuentes Abiertas): tipos, métodos y salidas profesionales*. https://bit.ly/4269BeY

LISA Institute. (2025). *Contrainteligencia y protección de empresas*. LISA Institute. https://bit.ly/3RamNcw

Martínez, A. (2014). *OSINT - La información es poder*. INCIBE-CERT | INCIBE. https://www.incibe.es/incibe-cert/blog/osint-la-informacion-es-poder

MI5. (2024, 1 de octubre). En *Wikipedia*. Recuperado de https://es.wikipedia.org/wiki/MI5

MI6. (2025, 28 de febrero). En *Wikipedia*. Recuperado de https://es.wikipedia.org/wiki/MI6

Oñate Peinado, D. (2023). *Análisis de fuentes abiertas con OSINT*. Grupo Oesía. https://grupooesia.com/insight/analisis-de-fuentes-abiertas-con-osint/#elementor-toc__heading-anchor-0

Ortiz, A. E. (2020). *¿Qué es la inteligencia de red (NI, Network Intelligence)?* Blog HostDime Latinoamérica, servidores dedicados. Recuperado de https://www.hostdime.la/blog/que-es-la-inteligencia-de-red-ni-network-intelligence/

Real Academia Española. (s.f.). Ética. En *Diccionario de la lengua española*. Recuperado el 1 de abril de 2025 de https://dle.rae.es/ética

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al

tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). *Diario Oficial de la Unión Europea*, núm. 119, de 4 de mayo de 2016, pp. 1-88. Recuperado de https://www.boe.es/buscar/doc.php?id=DOUE-L-2016-80807

Rid, T. (2020). *Active measures: The secret history of disinformation and political warfare*. Farrar, Straus and Giroux.

Rojo Torres, J. D. (2023). OsiNET - Desarrollo de una herramienta de integración OSINT. *Alcalibe: Revista Centro Asociado a la UNED Ciudad de la Cerámica*, (23), 179-215. https://bit.ly/4lpqgBJ

Sánchez Rubio, M. (2018). *Investigación y extracción de datos en fuentes abiertas (TFG).* Universidad de Alcalá. Escuela Politécnica Superior

TECHINT: Technical Intelligence. (s.f.). *Inteligencia, Espionaje y Servicios Secretos*. https://intelpage.info/techint-technical-intelligence.html

Vivanco, J. (presentadora). (2021, 21 de diciembre). *Investigación en fuentes abiertas -OSINT-. Entrevista a Pablo Lázaro* [episodio 11 de podcast]. Podhack. Observatorio de Cibercrimen y Evidencia Digital en Investigaciones Criminales. Facultad de Derecho. Universidad Austral. Spotify. Recuperado de https://bit.ly/3XR385g

11. ANEXO

11.1 Consentimiento informado

Información sobre la Confidencialidad del Trabajo de Fin de Grado (TFG)

Estimado colaborador,

Me permito informarle que la información recopilada en el marco de mi Trabajo de Fin de Grado (TFG) será tratada con la máxima confidencialidad y utilizada exclusivamente con fines académicos y de investigación. La identidad de las personas que participen en este estudio no será registrada ni divulgada en ninguna fase del trabajo, quedando únicamente bajo mi custodia.

El TFG está supervisado por la profesora María Inmaculada Ruiz Fincias, quien puede ser contactada en caso de requerir más información sobre las garantías de confidencialidad y el uso de los datos a través del correo electrónico miruiz@comillas.edu

Asimismo, el tutor académico no tendrá acceso a ninguna información que permita identificar a los colaboradores, asegurando así el anonimato de su participación.

Las entrevistas se llevarán a cabo de manera telemática y se grabarán en un documento de audio para su posterior análisis. Dichas grabaciones serán utilizadas únicamente para la transcripción y estudio de los datos y no serán difundidas fuera del ámbito académico.

Si tiene alguna duda o requiere más detalles sobre el manejo de la información en este estudio, no dude en ponerse en contacto conmigo.

Por favor, firme a continuación si acepta los términos de confidencialidad y uso de la información mencionados en este documento.

Nombre del colaborador: _____ Fecha: _____

FIRMA

Atentamente,

Andrea López González
Universidad Pontificia de Comillas

11.2 Guion de la entrevista

1. Trayectoria profesional y relación con las fuentes abiertas.

2. ¿Qué organismos gubernamentales forman parte de la estructura de inteligencia en España? ¿existe una estructura determinada encargada de hacer OSINT para la seguridad del país?

3. Dado que existen múltiples disciplinas de inteligencia (HUMINT, GEOINT, socmint, sigint…) ¿cuáles son las más utilizadas en su campo de trabajo?

   3.1 ¿Existe un perfil OSINTER definido? ¿Cuál sería?

4. Existen varios tipos de clasificación de fuentes abiertas según el procesamiento de la información (fuentes primarias, secundarias y terciarias) ¿Con qué tipo/s de información se trabaja más en su ámbito?

   4.1 Entre los métodos de obtención de información nos encontramos con la obtención pasiva, semi-pasiva y activa. ¿Cuál es la predominante en su trabajo?

5. A grandes rasgos, ¿cuáles son las áreas investigaciones en fuentes abiertas en su ámbito de trabajo?

6. ¿Existe un protocolo general que enmarque las investigaciones en fuentes abiertas? ¿Y alguno específico en su ámbito?

7. Retos actuales y futuros para las investigaciones OSINT.

   7.1 Dificultades haciendo OSINT aun teniendo herramientas y formación para ello.

11.3 Transcripción de las entrevistas

11.3.1 Transcripción entrevista 1

Buenos días. Como te comenté en el documento de colaboración y confidencialidad, la información sólo la voy a custodiar yo y simplemente extraeré la información que me sea útil. En principio, me gustaría que fuera enfocada a la parte más militar si puede ser, y luego hacer un poco de hincapié en alguna diferencia entre el ámbito militar más público y el ámbito privado. Hacer algún comentario sobre diferencias, también lo veo bastante interesante.

Pues nada cuéntame tu trayectoria profesional y tu relación con las fuentes abiertas.

Bueno, pues yo soy coronel del ejército del aire en la reserva y he sido profesor del curso superior de inteligencia de las Fuerzas Armadas y del curso básico de inteligencia de las Fuerzas Armadas de los dos y concretamente he sido profesor de OSINT en ambos cursos durante varios años.

Investigando he visto que, en Reino Unido, por ejemplo, sí tiene una estructura muy clara por parte del Gobierno, pues del tema del OSINT. Que está el cuartel central de comunicaciones de Gobierno, el MI5 y el MI6. Aquí en España, ¿la estructura de inteligencia cómo está organizada?

Pues también está muy estructurada porque en el Ministerio de la Presidencia, hay una comisión delegada del Gobierno para asuntos de inteligencia, de ahí cuelga el Ministerio de Defensa con el Centro Nacional de Inteligencia y dentro del Centro Nacional de Inteligencia está el Centro Criptológico Nacional, la Oficina Nacional de Seguridad, la Oficina Nacional de inteligencia y contrainteligencia, y luego dentro de las Fuerzas Armadas, pues tenemos el centro de inteligencia de las Fuerzas Armadas (CIFAS) y luego tenemos órganos de inteligencia en los Estados mayores de del Ejército de tierra, de la Armada, del Ejército, del Aire.

Y bueno, pues también hay cierta relación lógicamente hay una Comunidad de inteligencia con el Ministerio del Interior, que tiene la Secretaría de Estado de la seguridad, está el centro de inteligencia contra el terrorismo y el crimen organizado y dentro del cuerpo nacional de policía tenemos la Comisaría General de información y la Comisaría General de Policía Judicial. Y en cuanto a la Guardia Civil, el Servicio de

Información de la Guardia Civil y la Unidad Central Operativa, la UCO. Luego en la Secretaría General de Instituciones Penitenciarias, también hay una coordinación de seguridad penitenciaria que tiene ciertas competencias de inteligencia. Y las policías autonómicas, los mossos de escuadra tienen la comisaría General de Información, la Ertzaintza tiene la unidad de información y análisis, la policía Foral de Navarra la división de información y la Agencia Tributaria el Servicio de Vigilancia Aduanera, que también tiene ciertos cometidos de inteligencia. En todos los sitios, en todos los organismos de inteligencia se hace OSINT, en todos. Y bueno, realmente el OSINT lo puede hacer cualquier organismo público o privado para la consecución de sus fines y como parte de su sistema de gestión de riesgos siempre que lo haga dentro de la legalidad vigente.

Vale, y sabemos que existen muchos tipos de inteligencia HUMINT, GEOINT, SIGINT, IMINT, en el ámbito de militar, ¿cuáles son las que más se usan? ¿se mezclan todas y dependiendo de las operaciones? ¿Cómo se organiza eso?

Realmente se usan todas, pero hay ciertas ventajas y limitaciones de cada fuente de inteligencia. Por ejemplo, lo bueno que tiene el OSINT es la disponibilidad, el hecho de que la puedes distribuir sin comprometer las fuentes, porque al final son fuentes abiertas.

A pesar de no ser muy profunda, puede ser muy útil para investigaciones iniciales, como puede ser información sobre terreno, puertos y clima de una zona en el ámbito de la logística.

Empresas también lo usan, por ejemplo, empresas que hacen construcciones en África, pues miran cómo están las carreteras, cómo están los puertos, qué capacidades tienen para no tener problemas en la logística.

Y un área en la que yo me enfoco por el tema del trabajo mío en ciberseguridad, está en la ciberinteligencia, es una actividad que implica la obtención y el análisis de la información como objetivo de identificar, rastrear y predecir capacidades e intenciones y actividades de actores, hostiles en el ciberespacio. Dicho de otro modo, en la obtención de información sobre el ciberespacio y los actores que operan en él. No hay que confundir obtener inteligencia del ciberespacio, que usar el ciberespacio para obtener inteligencia, que sería a lo mejor una parte del OSINT.

En el área de ciberinteligencia también se puede recurrir a inteligencia de fuentes abiertas orientada a redes sociales, información técnica de inteligencia técnica, información de inteligencia de señales en un sentido más amplio.

¿Consideras que hay un perfil OSINTER dentro del ámbito militar? Bueno, o en general, ¿existe un perfil, características o cualidades, o realmente cualquier persona podría ocupar ese papel?

Vamos a ver, tenemos que entender primero lo que es el ciclo de inteligencia, ciclo de inteligencia.
Tiene una planificación, una obtención, un procesamiento, un análisis, una difusión y luego una retroalimentación, porque de una inteligencia obtenida se pueden derivar otras necesidades de inteligencia posterior. Esto es un ciclo.

Realmente el OSINT entra claramente en el área de obtención porque necesitas conocer unas técnicas especiales y luego debes tener una capacidad de procesamiento, porque hay veces que tienes que procesar documentación estructurada, no estructurada, base de datos, información muy dispersa y el procesamiento previo al análisis y el filtrado previo de información puede ser muy muy importante.

Por un lado, tienes una persona que se quiera dedicar al OSINT en la en el área de procesamiento, debe tener un conocimiento técnico, un conocimiento profundo de las herramientas y técnicas de recopilación de datos, incluyendo el uso de motores de búsqueda, metabuscadores, herramientas de extracción de datos, aplicaciones de monitorización herramienta de análisis de metadatos, etcétera.

Luego debe tener un conocimiento de fuentes de información, el estar familiarizado con diferentes tipos de fuente de información OSINT, ya sean el ciberespacio, o sea, documentación, bibliotecas, librerías, revistas, entrevistas, etcétera. Debe tener capacidad analítica porque tiene que filtrar y resumir grandes volúmenes de datos accesibles, filtrando lo que es relevante de lo que no. También tiene que ser capaz de detectar y eliminar información no relevante.

Fake news, darle contexto, así como ser capaz de trabajar con información como he dicho estructurada y no estructurada en varios formatos, puede estar en PDF, Excel, etcétera. Debe tener habilidades de investigación, tiene que ser capaz de realizar investigaciones

exhaustivas que incluye búsquedas de información en internet, redes sociales, base de datos públicas, etcétera.

Y luego debe tener conocimientos de seguridad y ciberseguridad. ¿Por qué? Porque si trabajamos el ciberespacio siempre dejamos huella. Podemos hacer las cosas sin que se vea claramente cuáles son nuestras intenciones.

Tiene que saber de seguridad de la información, ciberseguridad para entender las amenazas y vulnerabilidad de que pueden surgir durante la obtención de información y no revela el interés o el motivo de la investigación. Luego debe tener capacidad de comunicación porque tiene que ser capaz de comunicar su hallazgo de manera eficaz, concisa y clara, tanto en informe escrito como en presentaciones orales. Por supuesto, la ética y la legalidad es crucial para un especialista que opere dentro de los límites legales y éticos.

Completamente de acuerdo, es un poco también lo que yo he recogido en el trabajo, y también un apunte que añadí fue creo que un analista de inteligencia en el ámbito empresarial, por ejemplo, debe tener conocimientos sobre el funcionamiento de las empresas, si es en el ámbito militar, pues sobre el ámbito militar, etc. Es decir, además de esas características, también especialización en cuanto al ámbito en el que opera.

En cuanto al procesamiento de la información, como hay fuentes primarias secundarias terciarias, en el ámbito militar, ¿cuáles se usan, a cuáles se accede o a todas?

Principalmente a primarias y secundarias.

¿Y en cuanto a la recopilación de información?

En el caso del OSINT, esto es prácticamente pasiva. ¿Por qué? Porque es una inteligencia de oportunidad. No encuentras lo que buscas, sino que encuentras lo que existe. No siempre existe todo, no siempre puedes orientar tu búsqueda a la contestación de una pregunta concreta, sino a la obtención de información, indicios. Tienes que dar cierto nivel de validez, o sea, predomina la pasiva, pero en ocasiones, por ejemplo, en el caso

de la ciberinteligencia, cuando recibes un ciberataque, pues pasas a una obtención activa interactuando con el atacante. Intentando sacarle información al atacante. En una estafa, le puedes preguntar al atacante a qué cuenta, quiere que le mandes el dinero. De esa manera, te da una cuenta que, si está en Europa, a lo mejor cabe la posibilidad de rastrear quién está detrás de ella.

También puedes interactuar con el atacante para obtener una fuente adicional de información sobre sus tácticas, técnicas y procedimientos y buscar la manera de atribuirle. Porque todos los atacantes tienen unos conocimientos atómicos. No todos los atacantes saben explotar todas las vías de ataque y siempre hay unas prácticas técnicas y procedimiento muy típica que están usando determinados grupos, o sea, analizando esas tácticas y técnicas y procedimientos, puedes decir, pues esto es un ataque que viene de un grupo iraní, de un grupo chino de un grupo ruso, etcétera.

Si, vamos, un poco depende también del ataque y de y el contexto. ¿Vale, y así, a grandes rasgos, en el ámbito militar, en qué tipo de operaciones se usa OSINT?

Lo enfocamos a mi ámbito de trabajo, a mucho, prácticamente todo es OSINT. Investigación de actores de ciberataques, situación geopolítica internacional que tiene un impacto claro en las operaciones de guerra híbrida y en algunos ciberataques, en las tácticas, técnicas y procedimiento de los atacantes, en las vulnerabilidades que hay, como las están explotando, si existe una explotación activa o no de una vulnerabilidad, el tema de vigilancia digital, que es lo que aparece en la dark web que amenazas hay, qué fugas de información, credenciales filtrados, qué activos conoce el atacante.

Vale y en cuanto a los protocolos, bueno, más bien, ¿el ciclo de inteligencia en el ámbito militar es igual que el del del CNI o hay alguno en concreto que se use?

El ciclo de inteligencia es el mismo siempre, o sea, el ciclo el que te he dicho yo antes. Pero si hay un protocolo que se aplica que es reconocimiento, identificación de fuentes, o sea, fuera del ciclo. El ciclo es una cosa y este protocolo enmarcan las investigaciones en fuentes abiertas, lo primero es identificar la fuente, quién sabe de qué, valorar esas fuentes, incluye motores de búsqueda redes sociales, blog, wiki, foros, hasta la Deep web en caso necesario. Luego está la explotación de fuentes de información: hay que buscar

medios para poder explotar esa fuente, extraer la información, bajarte vídeos, por ejemplo, medios de comunicación, periódicos, televisión, revistas, radio, bases de datos pública, eventos, conferencias, temáticas. Luego, la recolección de datos: recopilación sistemática de datos de fuente identificada y puede emplear herramientas como Google Hacking o sin Framework Maltego Sodan Enemablesus Openbach, Megadow y muchas más herramientas.

La cantidad de herramientas para obtener inteligencia en el caso de Ciberinteligencia son infinitas porque son muchísimos. Luego está el procesamiento de datos que implica la organización, la estructuración de los datos recopilados para facilitar el análisis. Una de las cosas más complicadas en el caso de las fuentes abiertas es la línea temporal, cuando se ha publicado, la fecha que aparece en Internet si es la fecha real o la fecha en la que se escribió el artículo en la que ocurrieron los hechos en la que se modificó el artículo… El crear una línea temporal es muy complicado.

Luego está el análisis de los datos procesados y recopilados para instalar información útil y luego generar inteligencia, que es la generación de informe, producto de inteligencia, recomendaciones basadas en análisis de los datos. Finalmente, la distribución de la información

Vale, y en cuanto a dificultades, haciendo OSINT aun teniendo formación y herramientas en el mundo actual, ¿cuáles serían las principales dificultades a las que nos encontraríamos?

la cantidad abrumadora de información disponible en Internet hace que filtrar y analizar datos relevantes sea una tarea monumental. Cada vez más personas publican contenido en línea, lo que complica aún más esta labor. Luego en la integración de los datos, combinar datos de múltiples fuentes y formatos para obtener una visión coherente y completa puede ser complicado. Por ejemplo, datos que puedes extraer del de algunos documentos, por ejemplo, del Boletín Oficial del Estado. Son datos que tienes que extraer, está en PDF, tienes que pasarlo a un formato que lo puedas analizar, por ejemplo, con una inteligencia artificial y que te haga resúmenes. Todo eso implica cierta complejidad. Luego la calidad y la veracidad de la información cada vez hay más fake news, hay mucha opinión, poca información. Aunque las opiniones pueden ser interesantes si provienen de influenciadores, generalmente no son útiles para la inteligencia y pueden polarizar. Un

buen analista tiene que evitar polarizarse, tiene que trabajar con una mente abierta, buscando los datos objetivos y no dejarse llevar por sus prejuicios. Debes obtener información respetando la legislación, lo cual puede limitar el acceso a cierto tipo de información. Tener las herramientas y las habilidades adecuadas. Hay veces que hay herramientas que están disponibles, pero tienen un coste y que te pueden facilitar la vida, pero tienes que formarte también porque no deja de ser herramienta. No hay nada que te dé una solución final, sino que hay herramienta de recopilación y obtención y manipulación de datos.

Hay una disciplina muy interesante dentro de OSINT que se llama periodismo de precisión, periodismo de datos, que usa fuentes abiertas para obtener un periodismo de calidad basada en datos. Se usan muchísimas herramientas de manipulación, de depuración de datos como Google define y demás que te permite limpiar bases de datos buscar errores. Pues es un trabajo laborioso pero que da buenos resultados.

Y luego, como he dicho, el problema del tiempo, la cronología cuando ocurrieron los hechos y demás puede ser complicado. Además, la evolución de las personas en el tiempo, internet puede tener información muy antigua que no significa que una persona que escribió hace 20 años una cosa siga pensando de la misma manera.

Y retos a futuro relacionados con el OSINT, por ejemplo, la inteligencia artificial o con la automatización de herramientas. ¿Todo esto cómo lo ves?

La inteligencia artificial, hoy por hoy tienes tiene ciertas cosas todavía que mejorar. Desde mi punto de vista, podría ser una herramienta muy útil como he dicho antes, que te puede ayudar a procesar información. Yo la uso de forma objetiva. Por ejemplo, el otro día estaba analizando un archivo muy grande de log de un sistema y le dije a la inteligencia artificial "sácame todas las IPs de origen de estas conexiones" y me las saco. Y luego le dije, "quítame todas las que estén duplicadas" y lo hizo, lo hizo bien, no se inventó nada porque era una pregunta objetiva sobre un conjunto de datos objetivos.
La inteligencia tiene otro reto, que es el tema de la privacidad. El tema de la seguridad que nunca sabes a dónde van a ir a parar los datos, las preguntas y eso tiene también su hándicap en inteligencia. No hay mayor inteligencia para el adversario que sabe lo que buscas.

¿Cómo ves el futuro del OSINT?

Lo veo útil porque, de hecho, como te digo, en ciertas áreas es la primera elección a la hora de hacer investigaciones, de amenazas, de hechos. Las empresas están empezando a establecer sistemas de OSINT en sus organizaciones para tema de selección de personal, para temas relacionados con inteligencia competitiva, análisis de mercado, amenazas en desplazamientos al exterior de personal de empresa. En todo ese tipo de cosas el OSINT tiene mucho futuro.

Vale, pues nada. Por mi parte ya estaría. Si tienes alguna pregunta o alguna duda. De momento, no todo, claro, muchas gracias.

Muchísima, hasta luego.

Gracias, adiós.

11.3.2 Transcripción entrevista 2

Buenos días, como te comenté en el documento de colaboración y confidencialidad, la información sólo la voy a custodiar yo y simplemente extraeré la información que me sea útil. En principio, me gustaría que fuera enfocada a la parte más militar si puede ser, y luego hacer un poco de hincapié en alguna diferencia entre el ámbito militar más público y el ámbito privado. Hacer algún comentario sobre diferencias, también lo veo bastante interesante.

Pues nada cuéntame tu trayectoria profesional y tu relación con las fuentes abiertas.

Bueno vamos a ver. Yo como sabes, soy oficial del ejército de tierra en reserva desde el año 2013. Como oficial de la de las fuerzas armadas del ejército de tierra, he tenido destinos operativos en la primera parte de mi vida profesional.

Luego hice todo el curso de estado mayor que está centrado en la planificación operativa y de alto nivel, planificación militar y planificación estratégica. Y luego he tenido pues distintos destinos relacionados con planificación, entre ellos, estuve en el centro de operaciones del ejército de tierra en el cuartel general del ejército de tierra con

planificación de personal y logística, en la Sección de Operaciones del Estado Mayor de la Defensa con planificación operativa, he estado en DIGENPOL haciendo planificación de relaciones internacionales y de defensa, en Francia en una vacante de intercambio con la delegación de asuntos estratégicos, o sea que se puede decir que he estado haciendo planificación de distintos niveles.

En cuanto a la relación con las fuentes abiertas, bueno, las fuentes abiertas son una de las de las fuentes más evidentes a las que se consulta siempre que se hace en cualquier tipo de planificación y las he empleado desde hace muchos, muchos años, incluso antes de que hubiera estas herramientas para la búsqueda estructurada, etcétera, porque siempre la consulta de fuentes abiertas es fundamental para hacer un apreciación de la situación.

De todas maneras, en los últimos años, ya en el ámbito civil, cuando me salí de las fuerzas armadas y entré en la empresa privada, ahí también he tenido relación porque he desempeñado puestos de director de seguridad en FCC y aquí en el grupo de OESIA y en ambos hemos montado un área dedicada a la elaboración de informes basados en la inteligencia de fuentes abiertas, que son de utilidad para muchas cosas.

Luego, en segundo lugar, yo investigando he visto que claramente tanto en Estados Unidos como en Reino Unido hay una serie de organismos gubernamentales, por decirlo de alguna forma, que sí que se encargan exclusivamente o dan mucho apoyo y son los que gestionan un poco todo el tema de las fuentes abiertas, como el MI5, MI6 o el cuartel general de comunicaciones del gobierno, de todas estas de Reino Unido. En España. ¿Eso cómo está estructurado? ¿Qué entidades gubernamentales almacenan esta información o colaboran? ¿cómo se trata la información aquí en España?

Los organismos de inteligencia como el CNI, que es el equivalente al MI5 y MI6, son los que utilizan también inteligencia de señales (SIGINT), humana (HUMINT) etcétera, y también recurren a inteligencia de fuentes abiertas (OSINT).

¿O sea que aquí realmente sería el CNI?

Si, el CNI. Son los organismos de inteligencia los que fundamentalmente utilizan eso. Pero en España existe también el CIFAS, el centro de inteligencia de las fuerzas armadas. Porque recordarás que en España el CNI, lo que antes era el CSIR en su origen,

inicialmente era el servicio de inteligencia militar, que luego pasó a ser servicio de inteligencia civil. Y cuando eso ocurrió, pues se creó el centro de inteligencia para las fuerzas armadas, que vino a cubrir el hueco que quedaba, que dejaba la suscripción del CSIR, digamos, a la inteligencia gubernamental fundamentalmente. Entonces, el CIFAS se dedica a hacer inteligencia en aquellos teatros de operaciones donde hay fuerzas militares o hay interés en desplegarlas o interés en seguir el teatro de operaciones. Es decir, es un servicio exclusivamente militar y trabaja mucho con fuentes abiertas también, aunque no exclusivamente.

Luego están todas las unidades, las grandes unidades del ejército de tierra, o de cualquier ejército me debería decir. Yo hablo por el ejército de tierra, porque mis orígenes están en el ejército de tierra.

Los cuarteles generales están divididos en áreas de trabajo basados en la función a la que atienden (función de personal, función de inteligencia, función de operaciones, de logística, de transmisiones, etcétera). Hay ocho o nueve secciones de Estado Mayor que se llama, en función del tipo de cuartel general. Puede haber otras áreas. Hay cuarteles generales que a lo mejor no están tan centrados en operaciones y que tienen otras áreas, como las áreas cívico militar, etcétera. En muchos de estos cuarteles de una unidad militar, tienen una parte que se dedica a hacer inteligencia para el análisis de la planificación de operaciones del enemigo, lo que se llama el enemigo en la jerga.

Cuando tú planteas una operación militar para conquistar un objetivo, necesitas analizar el enemigo, necesitas analizar el terreno, analizar las fuerzas militares que hay, y esas unidades militares se ocupan de la inteligencia. Lo que pasa que ahí, más que la inteligencia de fuentes abiertas, que no es tan relevante, prima la inteligencia de señales, señales de radar, inteligencia aérea…

Si, eso es lo que te iba a preguntar. En el ámbito militar, ¿Cuál es la disciplina más utilizada?

Depende de dos cosas: del nivel de planificación en el que te ubiques y del objeto de la planificación. En un nivel bajo de planificación operativa, la atención se centra en la zona de terreno que se debe ocupar (utilizando principalmente SIGINT, IMINT y GEOINT). Las fuentes abiertas son prácticamente irrelevantes en este nivel, a medida que se asciende

en el nivel de planificación, las fuentes abiertas adquieren mayor importancia. En un análisis de muy alto nivel, especialmente en el ámbito político, las fuentes abiertas son fundamentales.

La segunda variable, es el objeto de tu análisis. Si tú quieres hacer un análisis orientado a comportamientos sociales, pues lógicamente la inteligencia de fuentes abiertas tiene más relevancia. Cuando haces un análisis de muy muy alto nivel y ya te ubicas en el nivel político, por ejemplo, lógicamente las fuentes abiertas son relevantes todo lo que tenga que ver con noticias de política, con actividad parlamentaria, o sea que depende del básicamente del nivel del análisis y del objeto del estudio.

A más nivel, más relevancia de las fuentes abiertas. Cuanto más abarque a lo mejor la operación.

Y en el caso de en una operación, utilizar fuentes abiertas, ¿qué técnicas para obtener la información se suelen utilizar? Primarias, secundarias. Terciarias.

Para hacer un buen análisis convenir a la fuente. Cuanto más proceso tenga, más sesgo tiene el medio. Entonces, lo que se suele hacer es hablar de la fiabilidad de la fuente y de la veracidad de la fuente. Normalmente lo ideal es ir a la información lo más primaria posible.

Y en cuanto al tipo de información que se recolecta, ¿se trataría de literatura blanca, literatura gris…?

Bueno, ya te digo, para las operaciones militares, es más bien la información de otro tipo. La información de fuentes abiertas se suele utilizar para el análisis de tipo más político, para el análisis de la situación general, etcétera. Normalmente no son reveladoras de información que sea relevante para las operaciones militares. Sin embargo, hay un fenómeno que con la presencia cada vez mayor de dispositivos móviles en operaciones, cada vez hay que tener más presente en la seguridad de las operaciones, el control de esos dispositivos. Porque a través de análisis de fotos, a través de comunicaciones realizadas por los familiares de los soldados en operaciones, a través de un montón de filtraciones que puede haber con esa dispersión, pues puede tener una vulnerabilidad y también puedes analizar eso.

Más que las operaciones militares, son operaciones de inteligencia, pues el tratar de identificar cuál es el de enemigo, cuáles son las intenciones del enemigo, la moral, a través de todas esas comunicaciones en la red. Eso está cobrando una relevancia cada vez mayor.

Enlazando con la siguiente pregunta, en cuanto a la interacción con el objetivo a investigar, ¿se suele hacer de forma pasiva (el enemigo no sabe que le estás investigando), semi pasiva (que a lo mejor le informas, pero el objetivo no interviene en la investigación), o activa (que es a lo mejor HUMINT trabajando con la persona directamente)?

Pues no sabría ahora mismo que decirte, depende de la investigación. Las unidades de inteligencia que despliegan en zona de operaciones para hacer un seguimiento suelen tener sus contactos y suelen tener fuentes incluso que colaboran activamente y que son perfectamente conocedores de que están colaborando.

Lo que se hace es HUMINT, sobre todo, y esas unidades suelen tener sus colaboradores y su red de contactos. Suelen intentar conseguirlo, porque eso es lo más lo más adecuado.

Vale. Y así un poco a grandes rasgos, ¿en qué áreas se decide hacer, OSINT en el ámbito militar?

El CIFAS hace OSINT y aparte de tener sus misiones fuera, pues tienen una unidad de OSINT muy potente con analistas.

O sea que en realidad para cualquier ámbito de seguridad del Estado se hace OSINT.

A nivel fuerzas armadas se acude a eso siempre. Lo único que el OSINT solo no vale, hay que afinar la búsqueda. El OSINT solo es muy raro que sea la solución, pero siempre es una actividad complementaria a otras.

Luego, por otro lado, quería ver si consideras que hay un perfil concreto de OSINTER, de investigador en inteligencia, o si cualquier persona puede hacerlo.

¿Te refieres a gente como tú, que quiere trabajar en las empresas?

Sí, si crees que existe como un perfil establecido para trabajar en ello y que sea como que cumpla unos requisitos, unas características específicas, o qué rasgos debería tener.

Bueno, te puedo decir rasgos que necesita. Primero la capacidad de análisis basada en algo más que el conocimiento de las herramientas. Para mí, el conocimiento de las herramientas y el manejo de las herramientas es necesario, pero en un momento dado puedes tener un analista que no maneje las herramientas y que tenga que esté apoyado por otro, que es el "herramentista". Para hacer un buen análisis hace falta tener una visión geopolítica. Depende del ámbito, si tú vas a hacer análisis de personas, pues te basta a lo mejor con conocimientos de psicología; si quieres hacer análisis de empresas, necesitas saber cómo está organizado el mundo empresarial y saber un poco todos los temas de la propiedad de las empresas, la gerencia, la organización, la ley de sociedades cotizadas, temas de cumplimiento, temas legales… El mundo es muy amplio, habría que centrarse en un tipo de investigación concreta.

Vale, si, en el ámbito militar.

En el ámbito del ejército te hace falta una idea de la geopolítica, que es la ciencia que estudia las relaciones internacionales explicadas a través de factores como la geografía, la economía, la raza, la etnia, la religión, los conflictos interestatales, el reparto del espacio vital las teorías geopolíticas.

Haría falta un poco ese conocimiento geopolítico que en realidad la geopolítica es un compendio de distintas ramas de la ciencia. No es solo economía, no es solo geografía, no es solo religión, es un poco la geopolítica, explica las relaciones internacionales en esos términos: explica por qué Estados Unidos que tiene una posición geográfica determinada, explica por qué Rusia es el país más grande del mundo y le llaman la tierra corazón, pues tiene otro enfoque geopolítico totalmente distinto y por qué hace lo que hace y se preocupa sobre todo de las conquistas territoriales de los países que tiene al lado. Es un puente que une Asia y Europa el Extremo Oriente y Occidente, con una extensión de tierra formidable, que es muy difícil de controlar. Y explica por qué un estado cuando está enclavado pasa a ser irrelevante, como le puede pasar a Bután. Los estados que no tienen salida al mar tienen enormes problemas. Explica la tensión entre Bolivia, Perú y Chile porque a Bolivia la han dejado sin acceso al mar.

La geopolítica explica las relaciones internacionales y la conflictividad en esos términos.

Debes tener ese enfoque.

Sin embargo, si tú estás en una empresa y necesitas validar si un comisionista cumple requerimientos de cumplimiento, pues a lo mejor tienes otros métodos o tienes que analizar otras cosas.

Lo que sí que es clave entender, que yo eso en mi trabajo anterior se lo decía al responsable del área de análisis, yo le decía. vamos a ver porque tú puedes hacer inteligencia dentro de tu propia empresa. Puedes hacer inteligencia empresarial, y para ello necesitas conocer el negocio. El que hace inteligencia empresarial bien es el que conoce bien el negocio.

Luego, el ámbito para hacer inteligencia empresarial es fundamentalmente el ámbito de las personas que están viendo los matices del negocio, lo conocen en profundidad y conocen a toda la competencia.

Entonces, tú llegar como analista y tratar de hacer inteligencia empresarial en una empresa que tenga a lo mejor varios modelos de negocio distintos sin conocerlos bien, pues es muy difícil. Entonces, puedes centrar la inteligencia en tener herramientas para analizar tu propia empresa que a lo mejor necesita ese análisis y necesita esa codificación.

A lo que voy es a que la inteligencia en fuentes abiertas como tal, es un medio que puede servir para muchos fines. Y no es el único análisis que se hace. A veces el pecado y el riesgo del analista puede consistir en pensar que es el único que hace análisis. Y no es así, porque análisis los hacemos todos. El análisis de parámetros de un sistema de ingeniería es otro sistema de información y tú puedes analizar lo que está pasando en cuanto a rendimientos, parámetros de fallo, etcétera.

O sea, quizá en lo que sí que te insistiría mucho Andrea, es en que el analista en fuentes abiertas no es la única persona en la empresa, ni mucho menos, que hace análisis. Todo el mundo, cualquiera que tenga que planificar tiene que hacer un análisis.

Entonces, ¿qué es lo distintivo del análisis de fuentes abiertas? Pues que incorpora una serie de hábitos, una serie de prácticas, una serie de informaciones, que normalmente si no es con esas herramientas, pues no las vas a consultar y te da una ventaja comparativa eso es un poco.

Y en términos de protocolos, está el ciclo de inteligencia en general pero luego sí que es verdad que he visto que por ejemplo el ciclo del CNI y el del INCIBE tiene ciertas diferencias. Realmente todos los ciclos de inteligencia, aunque cambian los nombres, el fin es el mismo, sólo que a lo mejor meten más o menos fases. ¿En el ámbito militar, se sigue alguna estructura o ciclo en concreto?

En el ámbito militar hay que hacer un plan de obtención. Es un ciclo parecido al del CNI, la planificación consiste en establecer unos objetivos y poner los medios para conseguirlos. Yo el del INCIBE no lo conozco porque estará más centrado en el mundo ciber, pero el ciclo de inteligencia del ejército es prácticamente el mismo que el del CNI. La diferencia está en dónde se plantea.

Lo lógico es que un plan de inteligencia requiere que la autoridad que te que te lo encarga pues te apruebe los objetivos de lo que vas a investigar, porque si no, el mundo es tan grande que tienes que saber en qué te centras. En la en la planificación militar, cuando te he hablado antes de que hubiera secciones de los cuarteles generales que se dedicaban al análisis de la información, a partir del plan de operaciones y los objetivos que tengas, se orienta la inteligencia que tiene que hacer y se le dice a la sección correspondiente que hace falta investigar estos puntos. Al final, conceptualmente es una cosa muy sencilla. No te vas a poner a investigar el mundo mundial, tienes que centrar el tiro y saber sobre qué tienes que investigar. Ese esquema general te vale para todo.

Por otro lado, si vamos al ámbito de la empresa privada, ahí la empresa es mucho más libre de los protocolos que quiera establecer. Pero hay una parte mínima, que es la parte de cumplimiento. Es decir, tienes que hacer las investigaciones dentro de lo que te permita la ley. El tema claro es el estudio de background de personal, que tienes que hacerlo de una determinada manera determinada manera, hay cosas que se pueden y cosas que no se pueden hacer.

Luego otros protocolos que tienes que aplicar, pues si tienes que hacer investigaciones para cumplimiento, cada empresa tendrá sus propios protocolos para hacer el cumplimiento, que pueden empezar incluso de un cuestionario que el área de cumplimiento les hace a otras empresas para garantizar para saber que cumplen o no cumplen con los mismos estándares, digamos, de cumplimiento que la empresa que te está contratando.

Es decir, nosotros vamos a contratar a alguien le decimos, oye, mira, yo quiero saber que tú tienes los mismos estándares de cumplimiento que yo, que no produces el país donde hay explotación infantil …

En el mundo militar, que es un mundo igual que el mundo del gobierno, es el mundo de lo público, de lo que se trata es orientar los recursos y determinar cómo se hace el esfuerzo y cómo lo dotas, en el mundo empresarial tienes a lo mejor aparte de eso (que también lo tendrás) pues tienes los protocolos derivados de tus propias políticas internas y de la necesidad de darte de cumplimiento.

Y enlazando con este aspecto, ¿alguna diferencia notable que haya entre el mundo militar y el sector privado?

No. Así que a mí se me ocurra no.

En cuanto a lo que acabamos de comentar de los reglamentos que se tienen que adaptar a ellos, ¿si estás en el sector público son más flexible y la prioridad es otra?

No, no he dicho que en el sector público no haya cumplimiento. El sector público tiene que estar sometido también al principio de legalidad, en eso no hay diferencia, el principio de legalidad opera para todo el mundo.

Lo que digo es que las empresas privadas pues tienen que definir para qué quieren utilizar estas herramientas y tienen que establecer sus políticas.

Pero el principio de legalidad se les aplica todas. Si que es verdad que existe la tentación de no respetar el principio de legalidad y, de hecho, esto da lugar en empresas a escándalos de empresas que han montado gabinetes que se dedicaban a hacer estudios de dudosa legalidad. De hecho, ha acabado gente sentada en el banquillo por hacer cosas que no estaban autorizadas.

Y a la hora de investigar en fuentes abiertas, ¿con qué dificultades aun teniendo herramientas y conocimientos nos podemos encontrar ahora en la actualidad? ¿cuáles son las principales dificultades al hacer OSINT?

Bueno, la primera es que el OSINT por sí solo no es suficiente y muchas veces tienes que completar tu análisis haciendo HUMINT y contratando un agente detective que te dé información más de detalle. Hacer inteligencia sólo de fuentes abiertas en la red es relativamente sencillo, una vez que lo tienes organizado las herramientas valen para muchas cosas. Pero cuando llega el momento de requerir una inversión adicional, ahí hay que pegar un salto cualitativo muy grande en términos de investigación y de costes.

Esa es una cosa que hay que tener clara. ¿El peligro cuál es? que, por no dar ese salto, por no hacer ese gasto, te fíes sólo de lo que estás sacando a redes y que eso pues te lleva a conclusiones falsas. Hay que ser un poco crítico con eso, hay que cuestionar.

Por ejemplo, hay gente que está muy expuesta en las redes y otra que no. Es verdad que dicen que la ausencia de información también da cierta información, pero eso influye. A lo mejor una persona que está más expuesta y que tiene menos riesgo en realidad, pero tu aprecias que tiene más riesgo o más información, es ese sesgo de tender a juzgar más a las personas que están más expuestas a las redes. Por ejemplo, esa es una dificultad.

Si el tema es muy importante y lo que te estás jugando es mucho, lo que habría que hacer es completar eso con información de detective o contratando una agencia que te de información más completa. Eso no siempre es fácil de hacer. Montar una unidad de ese tipo y empezar a prestar servicio es complicado.

La otra es encontrar gente en las empresas. En España esto está cogiendo mucha velocidad, pero sigue habiendo una cierta falta de experiencia, no hay perfiles suficientes.

Y lo tercero es ser capaz de hacer un buen análisis, porque una cosa es la información que tú recopilas y otra cosa es ser capaz en un buen análisis. Ahí una inteligencia artificial bien programada te puede ayudar, porque puede ser capaz de sintetizar cosas que tengas en múltiples fuentes. Eso no le va a dar más más esta actitud al análisis. Además, en inteligencia pasa un fenómeno también, que es que muchas veces la inteligencia se alimenta a sí misma y pasa también en la inteligencia militar. Tú tienes una noticia, la misma noticia que procede de una misma fuente primaria, se te reproduce en varios ámbitos y estadísticamente coge relevancia y se vitaliza, pero eso no le da más veracidad.

Yo creo que hoy por hoy procesar una gran cantidad de información con inteligencia artificial que está basada en estadística cuando hay tendencia a la viralización es un riesgo,

porque te puede dar más verosimilitud para informaciones que simplemente se han viralizado porque son bizarras, extremas, curiosas o lo que tú quieras.

En la inteligencia militar también pasaba eso desde cuándo. Los americanos generaban una información, en todos los servicios de inteligencia de otras naciones se hacían eco de eso porque venía de los americanos, "era muy fiable" y luego cuando llegas a hacer el análisis realmente la fuente primigenia no la conoces, te la ha proporcionado el servicio de inteligencia norteamericano, no sabes realmente lo que hay detrás. Entonces sin tener acceso a la fuente primaria, pues hay que hay que tener mucha experiencia como analista y no fiarse de la inteligencia artificial para para llegar a determinadas conclusiones. Es un sexto sentido que el analista tiene que desarrollar con su experiencia profesional y con conocimiento que va más allá de lo que son las herramientas.

Y yo diría que especializarse. Si tienes que hacer un análisis de economía, conviene que tengas formación en economía y además lo complementes con formación de analista de inteligencia.

La dificultad sería que el analista sólo con su conocimiento y sus herramientas de lo que es el OSINT, no le valdría para hacer un análisis adecuado.

Y, por último, retos a futuro, ¿como ves el futuro del OSINT?

Bueno esto lo del desarrollo de herramientas y de la inteligencia artificial va a tal velocidad, que no me atrevo yo …

Creo que habrá en muy poco tiempo herramientas muy muy potentes que sean capaces de hacer estos análisis y hacer análisis de temas complejos como los riesgos ciber.

Creo que esto va a ir a muchísima velocidad. Entonces, no me cabe duda de que esto evolucionará tan rápido que no me atrevo a predecirlo.

Habrá que ver a dónde vamos.

Pero te repito, al final estas herramientas habrá que pasarles la prueba del algodón y verificarla, no fiarse solo de ellas.

Nosotros aquí, la política de inteligencia estamos escribiendo una política de empleo de inteligencia artificial y una de las condiciones que estamos poniendo es la supervisión de

la persona. La persona no tiene probablemente capacidad de procesar tanta información como la inteligencia artificial, pero hoy por hoy puede juzgar mejor que ella. Las inteligencias artificiales fabulan y eso irá mejorando. La capacidad de proceso va a ir aumentando exponencialmente. El futuro es de cambio de mucho dinamismo, muy acelerado en muy poco tiempo. De hecho, las herramientas nacen y mueren, su plazo de vida yo creo que es corto hoy por hoy.

¿Y consideras que la IA en cierto modo va a obstaculizar las investigaciones o todo lo contrario?

No yo creo que obstaculizar no. De hecho, la inteligencia artificial generativa se ha puesto ahora muy de moda, pero llevamos muchos años con ella y muchas cosas de las que hacemos están basadas en IA (reconocimiento de matrículas, de imágenes de caras, diagnósticos médicos...) entonces riesgos los hay y los habrá, pero normalmente es derivado del mal uso.

Por ejemplo, en china hay miles de cámaras y desde que entras del país hasta que sales saben dónde has estado. Eso aquí en Europa no pasa, porque hay más respeto por la privacidad, pero el riesgo es ese. El riesgo de la falta de privacidad y del abuso por parte de las autoridades.

Y esto va a ser cada vez más eficiente, las herramientas, los motores de búsqueda, los algoritmos… el riesgo es que se emplee mal, pero yo creo que lo que hay es riesgo, la IA no viene a dificultar. Riesgo de que aumente la desinformación, de viralización de noticias falsas, todo eso está claro.

Pues nada, yo no tendría nada más que añadir, si tienes alguna pregunta.

Nada, espero que te haya sido de utilidad.

Si, muchas gracias.

Adiós

11.3.3 Transcripción entrevista 3

Buenos días. ¿Qué tal me escuchas?

Hola, Buenos días, ¿qué tal? Sí perfectamente Andrea, un placer.

Igualmente. Para mí es un placer contar con vuestra, con vuestra ayuda. Si quieres empezamos. Cuéntame un poco, pues trayectoria y qué relación tienes con las fuentes abiertas.

Vale yo, mi trayectoria profesional, yo vengo de carrera de sistemas de la información que es una licenciatura en Brasil, donde se mezcla la administración y la parte de ingeniería informática en que te preparas para gestionar equipos o crear tu propio negocio dentro de la informática en general.

En la carrera ahí por el año de 2007, conocí forense, en 2008 pude hacer una formación en forense, que fue la primera certificación y de ahí hice un máster. Desde entonces vengo trabajando con fuerza y cuerpo de seguridad. Actualmente tengo una empresa de ciberinteligencia, que hago formaciones, consultoría a fuerzas y cuerpos. Soy formador de Interpol para 32 países, lengua española, portuguesa e inglés también. Hago formaciones en LATAM exclusivo a algunos departamentos de policía en Brasil, departamento de Inteligencia, Colombia, México, pues Bolivia, Argentina y en España también he formado tanto Policía Nacional como Guardia Civil, Mossos de Esquadra, Ertzaintza, policías locales, CNI, el CCN CERT y organizo un evento exclusivo que es el OSINTOMÁTICO, que es un evento exclusivo para formar analistas en ingeniería social y fuentes abiertas OSINT.

Luego, la segunda pregunta es un poco también general. ¿En España, cómo está estructurada la red de inteligencia?

Tenemos el CNI, que es el que lleva toda la parte de inteligencia y apoya también en el CCN CERT. Este último lleva más la parte técnica (herramientas o los desarrollos de las herramientas) a nivel de inteligencia. El CNI, sería lo que sería el MI6 inglés o la mezcla entre el FBI americano con algo también de la CIA. La CIA tiene jurisdicción fuera de Estados Unidos, de la misma manera aquí hacemos todo desde la misma casa, o sea, el CNI también tiene jurisdicción fuera de España para poder actuar. Tenemos agentes fuera de España y agentes dentro de España.

Y dado que existen múltiples disciplinas como el GEOINT, HUMINT, SIGINT, ¿hay algunas específicas en, por ejemplo, que en Policía Nacional se usen más o menos? Intuyo que en el ámbito militar GEOINT tiene más relevancia, por ejemplo. ¿Cómo se distribuyen las disciplinas?

Exacto, en el ámbito policía, el HUMINT tiene más relevancia sin duda, porque es el momento en que se hace el interrogatorio, que se investiga, que se entrevista a unos perfiles, se cuenta con activos que te ayudan, que te aportan datos. Un informante. Al tener un colaborador se utiliza mucho HUMINT. El OSINT sin duda se utiliza mucho por parte de los cuerpo de seguridad, porque muchas veces ellos tienen base de datos y acceso a informaciones que nosotros desde fuera no tenemos. Pero hay mucha información que no está ni en esa base de datos.

A lo mejor el tema el tema de matrículas y todo eso también entraría dentro de ¿no?

Entraría, entraría mucho en IMINT, que es la inteligencia de imágenes, que te serviría bastante bien también para análisis de imágenes y la parte de GEOINT se utiliza, pero a nivel militar se utiliza mejor. Se utiliza más enfocado, sin duda.

¿Y consideras que existe un perfil OSINTER definido o que tiene que reunir una serie de características concretas? ¿Cómo sería como el perfil ideal, por así decirlo, de un OSINTER?

Pues a nivel técnico no hay un perfil definido como tal. Por ejemplo, he trabajado con varios y varios y varios perfiles, gente que viene de carrera, de biología, de periodismo, de salud, y hoy se dedican a al mundo OSINT, entonces no está tan vinculado. Pero sí que hay dentro del mundo OSINT varios perfiles. Por ejemplo, con conocimientos más técnicos, desarrollo de herramientas, con conocimiento de lenguaje de programación como Python. Ese sí que tiene un enfoque más grande en relación con un perfil más técnico. Sin embargo, hay perfiles que se parecen mucho al perfil investigativo de toda la vida. El perfil periodista que tiene esta curiosidad, esta perspicacia de ir más allá de lo que sale en la noticia, y es muy bueno en extraer información de páginas web de investigar perfiles…

También intuyo que, por ejemplo, si alguien es analista de inteligencia en una empresa privada, por ejemplo, deberá tener conocimiento del funcionamiento de las

empresas. Un poco dependiendo del ámbito, también deberá tener esta base del funcionamiento de la institución en la que está.

Exacto. Eso igual para fuerzas y cuerpos. Yo, por ejemplo, si estoy en la parte militar debo tener esos perfiles de conocimientos y si estoy en la parte operativa también necesito tener esos conocimientos.

Como bien se sabe, existen varios tipos de fuentes abiertas, según lo que es el procesamiento de la información: primarias, secundarias o terciarias. Obviamente yo así de primeras pienso que las fuentes primarias son siempre las más utilizadas a las que se recurre, pero ¿en algún caso es más interesante recurrir a secundarias o incluso terciarias, o siempre se va a buscar ir a por primarias?

Siempre se empieza por las fuentes primarias. Depende de cómo se evoluciona, se utiliza para validar información. Las fuentes secundarias se utilizan para validar las informaciones que hemos obtenido de manera inicial, para saber que se trata del mismo perfil que se está buscando y para validar también que esta información sea correcta. Por ejemplo, en LinkedIn pone que su cumpleaños es el 7 de marzo y yo no puedo utilizar otras fuentes para validar. Como fuerzas y cuerpos, tengo acceso a base de datos específicas que me va a facilitar encontrar esa información, como el registro de DNI de un perfil. Entonces sí, se van complementando.

Y en cuanto a los métodos de obtención de información relacionada con la interacción con el objetivo: pasiva, semipasiva o activa, ¿cuál predomina en cada cuerpo de seguridad?

De manera general se utiliza de modo pasivo. Que el investigado no sepa que está siendo investigado. Porque depende de cómo se utilice la investigación le va a saltar ahí alguna alerta de que está siendo investigado.

Depende mucho, porque claro, dentro, por ejemplo, dentro de Policía Nacional o dentro de Guardia Civil hay departamentos, hay oficinas y jurisdicciones que van enfocadas cada una en una cosa. Por ejemplo, tenemos dentro de Policía Nacional o dentro de Guardia Civil divisiones de investigación sobre terrorismo y ciberterrorismo. Entonces yo sí que tenía más allá del pasivo, o sea de un intermedio o un incluso más activo.

Si, en cuanto te metes a un foro o te infiltras, eso ya sería semipasivo porque interactúas en cierto modo, ¿no?

Exacto. Dejaría de ser pasivo, pasaría a ser un semipasivo o incluso activo, porque a partir de un momento que empiezas a interactuar y reaccionar a una publicación con un like, un comentario, pues, ya deja de ser totalmente pasivo y pasa a llamar incluso la atención de que estás ahí.

Entiendo que en todos los ámbitos se usa OSINT, lo que es investigación en fuentes abiertas, pero ¿hay operaciones concretas en las que el OSINT sea como la herramienta central o siempre va acompañada de otras cosas?

Siempre va apoyada. Como herramienta central, yo creo que no hay ninguna, siempre me apoya de otras fuentes, porque ese acceso les da la información y la oportunidad de tener base de datos e informaciones que son muy útiles y son muy confiables, son muy fiables las informaciones de base de datos cerradas que tiene fuerza de cuerpo de seguridad. Por ejemplo, pueden tirar desde para investigar sobre un DNI y tener informaciones de este DNI que un investigador o un detective desde la calle, no tiene tanta información.

¿Y existe algún protocolo general? Bueno, existe el ciclo de inteligencia del CNI, ¿los cuerpos de seguridad siguen ese ciclo o cada uno tiene otro ciclo u otro protocolo, eso como como está organizado?

No tengo muy claro cómo funciona. A nivel general, se utiliza el ciclo de inteligencia de manera general, pero no tengo muy claro cómo funciona esta división porque es una información muy hermética, no suelen decirlo. Pero de manera general, yo, por ejemplo, en mis formaciones lo que les enseño es esto, utilizar el ciclo de inteligencia. Los 6 puntos del ciclo de inteligencia y vamos evaluando cada uno de ellos.

Si. Ese lo extrapolas al ámbito que quieres, ¿no? entiendo.

Exacto.

También me ha gustado introducir un apartado relacionado con dificultades actualmente que nos encontramos haciendo OSINT incluso teniendo herramientas y teniendo conocimientos. ¿Cuáles son las principales dificultades en una investigación usual a las que nos hacemos frente?

La validación de datos es una dificultad. Hoy cada vez más la gente pone datos falsos en sus perfiles. Esto también nos afecta a nivel de información, porque se necesitaría validar esos datos y esto acaba siendo muchas veces muy cansado. Tengo que buscar este dato, todo enlace que voy encontrando tengo que validar para saber si de verdad se trata de la misma persona. Va muy vinculado al nivel técnico que tiene el target. Si estoy lidiando con un estafador, a lo mejor todas informaciones que él se va dejando de pistas son falsas, pero si estoy tratando de un cibercriminal que tiene conocimiento técnico, él sabe construir sus Sock Puppets, sus cuentas falsas, sabe mantener un perfil de alguna manera bastante oculto, utiliza VPNS, utiliza sistema de defensa, etcétera que va dificultando que su información real esté expuesta. Entonces creo que de ahí viene la principal dificultad.

Y aquí se me acaba de ocurrir una, una duda que tengo. ¿En este apartado la contrainteligencia, qué papel tiene?

Es muy importante también, de acuerdo con el nivel. Si se trata, por ejemplo, de investigación de terrorismo de ciberterrorismo, que es muy complicada, a nivel de contrainteligencia se pueden investigar, se puede ir detrás del perfil que está ahí metido en el grupo, etcétera. Entonces por eso la importancia de poder mantener su OPSEC, su operativo de seguridad muy bien calibrado, muy bien funcionales para poder impedir que los datos del investigador sean expuestos. Es muy importante.

Y ahora que está teniendo tanto auge la inteligencia artificial y todo eso, ¿qué retos crees que pueden surgir a futuro para el OSINT? ¿La inteligencia artificial, cómo va a afectar o la automatización de herramientas? Todo esto, ¿cómo ves el futuro?

Facilita para algunos temas, para generar contenidos, puede facilitar la adquisición de perfiles, mantener los perfiles, alimentar los perfiles. Esto es un punto positivo. Por otro lado, lo que está pasando aquí, los estafadores están utilizando para mejorar desde sus scripts de ataques sus lectores de entrada sea por un SMS o sea por un correo

electrónico. Por otro lado, ellos están utilizando Deepfake, el pasar por la persona a partir de la foto, montar la cara y suplantar la identidad. Creo que esto va a ser uno de los principales retos. Investigar supuestas deepfakes, personas falsas, impersonalización y ver de verdad que está quién está por detrás.

¿Y algún reto así, más? Que se te ocurra.

Bueno, las propias empresas están cada vez más restringiendo información. No te dan información sobre los usuarios por motivos de privacidad. Ya no piden tantos datos. Antes, por ejemplo, el Facebook te pedía la vida entera; ahora a lo mejor para tener una red social sólo necesito un correo electrónico y un número de teléfono de validación, y algunas le impide el número de teléfono y entonces, y esto a la hora de investigar, de poder ir detrás de un perfil que está atacando, y cometiendo algún crimen virtual, está cada vez más complicado realizar esta investigación reversa.

Mi libro comenta un poco exactamente eso, de la misma manera que nosotros nos protegemos utilizando nuestro propio OPSEC, VPN, proxy, etcétera, los propios criminales hacen lo mismo, entonces estamos ahí compitiendo con iguales.

Vale por mi parte, creo que no se me queda nada, la verdad que no tengo ninguna pregunta más, así que se me ocurra ahora mismo. Si tienes alguna duda o algo más que me quieras comentar.

No, estamos a disposición para lo que necesites con mucho placer.

Pues nada, muchas gracias por todo. Un saludo. Adiós Chao.

No, gracias, gracias a ti Andrea, adiós.

11.3.4 Transcripción entrevista 4

Buenos días, Roberto. ¿Qué tal me escuchas?

Hola, Buenos días, ¿qué tal? Sí perfectamente Andrea, un placer.

Igualmente. Para mí es un placer contar con vuestra, con vuestra ayuda. Si quieres empezamos. Cuéntame un poco, pues trayectoria y qué relación tienes tú con las fuentes abiertas.

Mi trayectoria. Tengo 18 años de carrera.

Ahora estoy en excedencia dentro de las fuerzas y cuerpo de seguridad en Argentina. Toda mi vida me he dedicado a lo que es delitos complejos y crimen organizado. Soy perito informático y telefónico forense.

Y bueno, con el paso de los años me di cuenta de que uno idealiza Europa de cierto modo. Nos damos cuenta de que tenemos las mismas flaquezas que en Argentina en muchos aspectos, que los jefes no entienden ciertas necesidades o que las entienden mientras no son jefe y después cuando suben, no.

Realmente las entienden, pero estamos escasos de recursos, tanto de recursos humanos como de recursos tecnológicos.

Entonces, por lo general, las distintas unidades siempre tienen que hacer mucho trabajo de distintas cosas.

En el caso mío yo en los 18 años fui perito, ya te digo, perito informático, pero también hacía todo lo que era investigaciones online.

Por otro lado, en cuanto al OSINT, es algo fundamental.

¿Por qué? Porque en muy pocos casos te habilitan judicialmente para que vos tengas una interacción con el investigado. En Argentina, la figura de Lo que se conoce como el infiltrado se llama agente revelador. El agente revelador es el que se encarga por medio de técnicas OSINT, primero lo ideal es no tener contacto con la gente que estas investigando, pero cuando es en casos de delitos complejos y crimen organizado, necesitas tener más información de este tipo de gente, ya cruzas esa barrera y comienzas a hacer OSINT activo (hasta ahí era pasivo). Por lo general el activo tiene ya una interacción con el objetivo, pero será lo mínimo posible para la investigación. Es como en cualquier tipo de organización, un infiltrado físico, pero en este caso un infiltrado en el mundo virtual.

Entiendo que se empezaría de forma pasiva, pero luego siempre bueno o casi siempre se termina con la activa para verificar la información. ¿No?

Dependiendo el caso y dependiendo de que judicialmente te lo habiliten. Es muy raro que te lo habiliten, pero ya te digo, yo en la unidad en la que trabajaba era bastante especial, porque era precisamente delitos complejos y crimen organizado, entonces sí teníamos

más contacto directo con los jueces y fiscales. Obviamente tienes que fundamentar muy bien por qué necesitas que sea un reconocimiento activo y que debas tener contacto con la otra parte, pero no deja de ser que es OSINT. Durante mucho tiempo se reconoció Open Source Intelligence, inteligencia de fuentes abiertas y demás, pero este último tiempo está viendo esa tendencia donde ya se está reconociendo que el OSINT es tanto activo como pasivo. O sea, el pasivo del que estás todo el tiempo en escucha, el normal y común que conocemos todos; y después el activo es en el que, bueno, directamente estás en contacto con el objetivo.

¿Es el ideal? No. ¿Se podría recomendar a unidades que no están especializadas y no tiene experiencia? Tampoco. O sea, hay que tener mucha preparación en ese aspecto.

Después de OSINT nada, yo creo que uno de los puntos que yo siempre digo, es que lo hacemos en el día a día. El OSINT inconscientemente ya lo hacemos, lo hace hasta un adolescente, cualquier persona ya hace OSINT asique.

¿Y allí en Argentina, aparte de HUMINT, IMINT, OSINT, os centrabais en alguna disciplina más en investigaciones?

Se usa mucho SIGINT porque, bueno, ya te digo, yo era perito telefónico, entonces todo lo que es la parte de señales y se usa mucho el GEOINT, pero a la hora de ya pasar el informe completo para la gente que tiene que hacer todo lo que es la parte de campo, todo lo que es la parte de por ejemplo una redada, previamente se hace un GEOINT Este último tiempo se está utilizando más del medio de los drones y demás. Antes no se utilizaba tanto, ahora se utiliza un poco más en cuestiones de que puedes tener un reconocimiento más completo de lo que es el lugar donde vas a hacer el allanamiento.

Después nada, lo normal el HUMINT común, ingeniería social, IMINT, OSINT, SOCMINT… Eso es lo normal que se utiliza.

¿Y ves alguna diferencia entre las fuerzas de cuerpos de seguridad de Argentina y la de aquí de España en ese ámbito?

Sinceramente no. Creo que incluso las de Sudamérica, no solamente las de Argentina, está hasta más evolucionado por la falta de recursos.

¿Por qué? Porque el OSINT dentro de cuerpos y fuerzas de seguridad se usa como una cuestión de cuando no tienes recursos para hacer ciertas cosas, como, por ejemplo, acá se pueden comprar software o hardware que se encargan de hacer muchas cosas que allá no tenemos. En Sudamérica no se tiene el presupuesto muchas veces. Entonces sí, las técnicas y demás dentro de las unidades del -INT están más o menos parecidas, pero en cuestiones del OSINT en sí está más avanzado en Sudamérica creo. Después a nivel normal de una comisaría regional de un destacamento regional y demás, están acá mucho más avanzado que allá. En cuestiones de las técnicas de investigación, porque el trabajo es distinto, entonces acá, como que están más preparados desde la formación en un montón de aspectos que allá. Por ejemplo, allí alguien de un destacamento en un pueblito, no va a tener que usarlo nunca, acá por lo menos tiene la preparación y la formación.

Claro, también por necesidad, ¿no? Al final si aquí se necesita mucho más, pues al final se desarrolla inevitablemente.

También me interesa mucho el apartado de actualidad. ¿Qué retos nos encontramos? Pues a lo mejor la masificación, o incluso la desinformación, la inteligencia artificial, ¿todo esto cómo crees que va a evolucionar en cuanto al OSINT? ¿va a dificultar? ¿Son barreras, son retos…? ¿Qué visión tienes a futuro? Sobre OSINT centrado en fuentes abiertas.

En todo lo que es referente a inteligencia artificial, creo que vamos a estar mejor, creo que va a ser mucho más fácil y mucho más sencillo, siempre y cuando sepamos usar las herramientas de inteligencia artificial.

¿Es un reto? Sí, como siempre, todo avance siempre va a suponer un reto. Y va a haber gente que se va a quedar en el camino porque, o no quiere seguir estudiando, o porque no está adaptado o porque no le gusta la inteligencia artificial y muchos aspectos, pero creo que no va a ser peor.

Si tenemos que entender que, nosotros, como investigadores que utilizamos técnicas OSINT, tenemos acceso a inteligencia artificial, la gente que estamos investigando también la tiene. Entonces los retos van a estar por ese lado, el poder estar a la vanguardia de todo lo nuevo.

Nosotros lo que utilizamos para enriquecer los perfiles son ciertas cuestiones que se podrían llamar “cutres”, donde las fotos no eran tan reales y demás. Hoy en día, hasta se pueden crear vídeos que, sinceramente, son reales. Incluso a los peritos informáticos se nos pasan de largo y no podemos detectarlos.

Entonces los retos son muchos, pero hay que estar a la vanguardia siempre. Yo creo que va a ser para mejor toda la cuestión está de lo que se viene de nuevo en el OSINT. Está muy, muy bueno, a mí me gusta mucho.

¿Y la información que da la IA se consideraría como información falsa o qué tipo de información es? No sé si me estoy explicando.

Directamente información falsa creada por la IA. O sea, el tema de desinformación es un reto muy grande para la gente que se encarga de hacer OSINT y para desmentir un montón de cuestiones. Todo lo generado por IA es falso, el tema es depende de qué lado lo veamos. Yo lo estoy viendo desde el lado del investigador, a mí me sirve muchísimo para crear perfiles y demás para poder seguir a los malos, pero ¿qué pasa? Que los malos también lo pueden hacer. Incluso la gente que hace desinformación, si bien son malos, pero no lo hacen con la meta de vender droga o de traficar gente.

Si y que simplemente, es entorpecer más que otra cosa, ¿no?

Claro, es entorpecer. Eso es, es como decimos en Argentina, es embarrar la cancha como en el fútbol. Entonces, al entorpecer eso, es un reto mucho más grande para los que se encargan de investigar la parte de desinformación, el periodismo que se encarga de desinformación, que utiliza muchísimo OSINT. Pero también como salen herramientas, o sea, como salen algunas medidas para hacer cosas, también salen las contramedidas. Entonces, creo que la gente que se encarga de la parte de desinformación está bastante bien entrenada y tiene metodologías como para llevarlo y que por más IA que se utilice tienes un montón de otros medios como para corroborar esa esa veracidad de la información.

Vale por mi parte, creo que no se me queda nada, la verdad que no tengo ninguna pregunta más, así que se me ocurra ahora mismo. Si tienes alguna duda o algo más que me quieras comentar.

No, estamos a disposición para lo que necesites con mucho placer.

Pues nada, Roberto, muchas gracias por todo, gracias a los dos. Si no nos vemos en los sintomáticos, allí estaré. Un saludo. Adiós Chao.

No, gracias, gracias a ti Andrea, cualquier cosita acá estamos, dale. Vale, te esperamos, dale, chao.

11.3.5 Transcripción entrevista 5

Buenos días. Como te comenté en el documento de colaboración y confidencialidad, la información sólo la voy a custodiar yo y simplemente extraeré la información que me sea útil. Cuéntame tu trayectoria profesional y tu relación con las fuentes abiertas.

Soy comandante de la Guardia Civil. Bueno, yo llevo en la Guardia Civil, ingresé en el año 2003 en oficiales.

Bueno pues en razón de fuentes abiertas desde que ingresé en la Jefatura de información, que fue en el año 2012 a principios, estuve durante 7 años de segundo jefe y de jefe del Grupo de ciberterrorismo, con lo cual nos encargábamos no solamente de la parte de ciberterrorismo como tal como amenaza; sino también de los apoyos técnicos a otras unidades de investigación, incluyendo un OSINT digamos más extenso o más profundo, o con más conocimientos.

Posteriormente me fui al centro de inteligencia de Fuerzas Armadas. También se hace uso evidentemente de OSINT, sobre todo para llegar a determinados países en los que no tienes despliegue, desde leer periódicos, boletines y cosas similares.

Y actualmente estoy en el centro de excelencia contra artefactos explosivos improvisados, soy jefe de la sección de Predicción, que es la parte de inteligencia y lo utilizamos sobre todo para ver técnicas, tácticas y procedimientos. Es decir, cómo están evolucionando, por ejemplo, las incidencias, el uso de drones, cómo están cambiando las, las técnicas o cómo está evolucionando desde un escenario a otro.

Nos basamos mucho en fuentes abiertas es una herramienta imprescindible hoy en día para tener una inteligencia básica.

Y aquí, bueno, yo investigando he visto que reunido, pues estaba como muy clara la estructura de inteligencia con el MI5 MI6. Aquí en España, ¿cómo está estructurada la parte de inteligencia nacional?

Eso da para un doctorado, o sea, es decir, existe una estructura de inteligencia, pero no está muy bien definida realmente.

Existe una estructura de inteligencia, de hecho, en la ley del CNI, si no recuerdo mal hace referencia a la Comunidad de inteligencia, pero esa Comunidad de inteligencia luego no está definida en ningún lado.

Básicamente inteligencia se suele llamar a los servicios de inteligencia declarados como tales. Normalmente es el CNI, en este caso en España, el CIFAS y el CITCO, aunque hagan cosas distintas también, y luego a los servicios policiales se manda información, que es lo mismo, pero históricamente no se les llama de inteligencia, sino que se les llama de información. Yo, por ejemplo, pertenezco a información. Está la comisaría General de Información de la Policía Nacional y es básicamente lo mismo, evidentemente con enfoques distintos.

No está definida una estructura como tal, lo que sí que hay una división de lo que se hace en el ámbito de inteligencia y lo que no se puede hacer. Desde el ámbito de inteligencia, digamos puro, se hacen informes, se analizan amenazas, pero, por ejemplo, no se judicializan casos. El CNI no puede judicializar un caso, eso solamente lo podemos hacer a las CFSE, solamente lo podemos hacer nosotros, Guardia Civil o la Policía Nacional y luego los mossos y tal en sus competencias. Pero el CNI no puede detener. Son enfoques distintos: nosotros hacemos un análisis de la amenaza más enfocado en la seguridad ciudadana y ellos pueden hacer un análisis de la amenaza más orientado a la seguridad nacional, pero como entidad nacional, no más orientada a la Seguridad Pública, colaboran. Es decir, pues una guerra económica, pues ahora nosotros a nivel policial nos importa poco, pero sí es una cosa que afecta al país. Eso sí que sería una cosa que trabaja o debe trabajar el Centro Nacional de Inteligencia, como responsable de la información al presidente del Gobierno y al Gobierno.

Luego hay una estructura de contra inteligencia. El Centro Nacional de inteligencia, es la autoridad de contra inteligencia, el problema es que no se sabe quién más está ahí abajo. La contrainteligencia se puede definir como el ámbito de las amenazas, sobre todo el servicio de inteligencia exteriores, que eso es una tarea básicamente del CNI, en la que los demás somos colaboradores y si tienes que detener a una persona, evidentemente lo tenemos que hacer nosotros, pero digamos que la voz cantante llamándolo así es el Centro Nacional de inteligencia.

La secretaria de Estado, la directora del CNI, pero no sabemos qué hay debajo, cuál es el resto de la estructura. No está definida en ningún lado. Entonces vamos más por hechos consumados que por una estructura definida y reglamentada.

Y existen múltiples disciplinas de inteligencia como el HUMINT, GEOINT, SIGINT. IMINT, en la Guardia Civil, por centrarnos un poco en un área, ¿cuáles son las que más se usan en tu ámbito?

Nosotros por historia HUMINT lo tenemos muy, muy muy muy trabajado. Para nosotros es fundamental, tenemos una estructura, unas muy buenas estructuras de HUMINT y trabajo de fuentes. También hay unas dudas. Si revisas doctrina militar, HUMINT tiene dos tipos de operaciones: las de contacto y las de no contacto. Por ejemplo, un seguimiento, los militares lo consideran HUMINT, nosotros no lo consideramos HUMINT, es una acción operativa. Nosotros HUMINT solamente lo consideramos cuando se trabaja con fuentes, cuando yo capto a una persona o a un colaborador para que me dé información o me ayude a algo, pero que hay un contacto de persona a persona. Nosotros los equipos de fuentes que se llaman, solo trabajan con personas. Todo lo demás para nosotros son equipos operativos que hacen vigilancia, se hacen contra vigilancia, hacen seguimientos, para nosotros no es HUMINT, sin embargo, en Fuerzas Armadas, sí.

SIGINT lo mismo, depende de cómo lo interpretemos, como intervenciones telefónicas o balizamiento, por ejemplo, pues para nosotros son medidas de investigación básicas.

Y OSINT es una disciplina de obtención, pero está más orientada a la inteligencia básica. Por ejemplo, para hacer OSINT no necesitas autorización judicial, lo utilizas para generar inteligencia básica y hacerte una idea global, hacerte una idea global de la amenaza, o investigar a una persona concreta. Pero claro, todo sin vulnerar ningún derecho.

Cuando pasas esa fase de instrucción y ya tienes que vulnerar derechos, tienes que pedir autorización al juez y te las tienen que autorizar, pues ya vamos a otras medidas. Ahí es donde seguramente se mezclan una figura que es muy importante para nosotros, que es el agente encubierto virtual. Realmente por definición, no es OSINT, esa discusión la he tenido mucha gente. Es decir, yo en el momento en el que vulnero determinadas barreras de defensa que un mapa lo pueda tener, ya no es OSINT. En el momento que yo uso el

engaño, por ejemplo, para entrar dentro de un foro, es OSINT, pero lo he conseguido mintiendo.

De forma pura, eso no es OSINT. De hecho, nosotros hacemos todo eso y utilizando identidades y funciona muy bien, sobre todo en foros yihadistas, etcétera, etcétera, pero todo eso lo hacemos con autorización judicial. Nosotros creamos una identidad entera virtual y asociada a una identidad creada judicialmente con toda su documentación y vamos dando paso a paso. Igual que cuando infiltramos a una persona en una organización, que también lo hacemos con una autorización judicial. Es lo mismo infiltrar en una organización, en una reunión o en una reuniones en un piso, que en un foro. En realidad, es básicamente lo mismo, siempre que tenga que usar el engaño. Hay una línea gris, una zona gris que bueno, depende de cómo se interprete es OSINT o no lo es. Entonces Van cambiando todo ese tipo de cosas, por definición eso es impuro y es muy importante y tenemos unos grupos de trabajo y sacamos operaciones bastante importantes con esto y te dan un entorno también de cómo va evolucionando la amenaza, sobre todo en qué tipo de objetivos declara. Si los objetivos que está declarando evidentemente son en Mali, pues bueno, podemos avisar a las entidades malienses trabajar con ellas, pero no es una amenaza sobre España. De repente llaman a acuchillar policías en Europa, OSINT es fundamental para, pues para establecer un fondo, un marco general para ver la evolución de la amenaza. Por ejemplo, para nosotros es muy, muy, muy importante una cosa que es básicamente OSINT que es la evolución de la propaganda yihadista, eso sigue por OSINT. Porque por definición la propaganda tiene que estar abierta, entonces para eso nosotros tenemos equipos que hacen el seguimiento de la evolución de la propaganda o en determinadas zonas, qué mensaje se mandan. ¿Hay referencias a Europa, no hay referencias a Europa, hay referencias a España? No las hay. pues bueno, cuidado que nuestro nivel de amenaza acaba de subir. Y eso es puramente OSINT, porque el mero hecho de que esa propaganda ya es que lo define como OSINT, como Open Source.

Esas son las más claras.

Bueno, también podemos utilizar un poquito de GEOINT alguna vez, pero muy, muy, muy, muy poco, depende cómo lo interpretes, immint, geoint, pues se utiliza por ejemplo para algún despliegue o una cosa concreta, pues tenemos que hacer una operación en un caserío pues evidentemente, tenemos que utilizar toda la información geográfica por dónde entrar, qué hacer, si ponemos un helicóptero, si no o si patrullas. Bueno, eso se

utiliza.

IMINT un poquito por el tema de drones, pero a lo mejor tampoco lo deberíamos definir más como IMINT, porque IMINT para mí, vale es verdad que lo vemos como una actividad de obtención, pero en realidad tiene que darle un punto de algo, ¿no?

El IMINT normalmente se utiliza para sacar unas imágenes en el tiempo real o unas fotografías y hacer un análisis de lo que te encuentras, una evolución, una estructura o cómo está evolucionando unas obras o qué están haciendo en un sitio u otro. Cuando solamente necesitas una imagen en tiempo real para hacerte una idea de tu operación, llamarlo IMINT …

Sí que no hay tanta investigación detrás de la foto como tal.

Correcto, exacto.

Si lo ves puramente pues sería IMINT, porque al final es una imagen que tienes que analizas, pero es una fase que digamos de conducción. Entonces, en la fase de conducción no tiene mucho sentido llamarle IMINT.

Y luego me interesa también, centrándonos un poco en fuentes abiertas OSINT, ¿cómo definirías como el perfil ideal para un OSINTER, para un investigador en fuentes abiertas?

Pues mira, aquí tenemos dos enfoques, ¿vale? Un enfoque, que es el que hacemos nosotros, que para mí es correcto, y otro enfoque que hacer, por ejemplo, Fuerzas Armadas normalmente.

Hay dos tipos de estructuras, una que tienen las Fuerzas Armadas, en la que los equipos OSINT son equipos a disposición de cualquier analista convirtiéndose en equipos independientes y, por tanto, deben ser personas muy generalistas.

La otra es como lo estemos establecido nosotros en la Guardia Civil, por amenazas. No tenemos un equipo OSINT, tenemos muchos equipos OSINT especializados, el equipo trabaja con la amenaza directamente. Nosotros, por ejemplo, en la Guardia Civil lo tenemos estructurado con 3 unidades centrales: la número 1, que es terrorismo nacional y otras cosas (odio, etcétera), la UC2, que es donde estoy yo, que es terrorismo

internacional y la UC3 que son otras amenazas, no terroristas, normalmente pues tráfico de armas, bandas juveniles de carácter violento o 50000 cosas que pueden llegar, sociolaboral, etcétera. Lo que hemos descubierto es que al final un OSINT hace mejor su trabajo si sabe lo que está buscando y se dedica a eso concretamente. Porque las fuentes de información del yihadismo no se parecen nada a las fuentes de información, que a lo mejor alguien de las Fuerzas Armadas tiene que mirar en el equivalente al Boletín Oficial del Estado de qué está contratando un país. Es una fuente de información que la gente desconoce y es muy valiosa.

Evidentemente, los servicios de inteligencia extranjeros están mirando nuestro Boletín Oficial de Estado y la plataforma de contratación del Estado porque te levanta el orden de batalla, es decir, si estás comprando no estás comprando que tienes o que dejas de tener. Toda esa información que casi toda es pública pues te dice, cuáles son las políticas las prioridades, las capacidades, la inversión, etcétera, etcétera. Eso es muy importante a nivel de inteligencia básica.

Eso es una cosa y eso es lo que te decía, si te dedicas a terrorismo o te dedicas a movimientos ultra, más que temas concretos de búscame esto en un foro, lo que necesito es una monitorización de ese foro continua para ver variaciones, para ver cosas. Entonces, si ordeno como un requerimiento de información o una orden de obtención, pues es un caso concreto dame información, un caso concreto dame información. Sin embargo, si lo tengo integrado en mi estructura, yo tengo unas personas que continuamente están monitorizando la amenaza. Yo creo que eso es más fiable. Qué pasa que debes tener gente que a lo mejor no sea tan generalista. Por ejemplo, tenemos un problema con el idioma, el idioma para nosotros es un problema.

Ese tipo de cosas, el que la gente sea hábil buscando, sea hábil evolucionando, tenga un conocimiento de cómo funciona técnicamente un foro o cómo funcionan las páginas, sobre todo para poder digamos evolucionar o mejorar su calidad.

Sobre todo, aunque no lo parezca, debe tener un conocimiento de qué es la amenaza o cómo funciona. O sea, no es un mero obtenedor no es una herramienta, sino forma parte del equipo de análisis, lo que pasa que tiene unas capacidades técnicas, pues más avanzadas o distintas, pero tiene que conocer la amenaza. Bajo mi punto de vista, eso es lo que le da el toque de calidad y técnicamente no hace falta que sea muy complejo. Es verdad que tiene que investigar, pues a lo mejor tiene que conocer algo de criptodivisas,

pues se tiene que hacer una monitorización de un bitcoin que es básicamente público, una cartera o se encuentra con tener que distinguir un número de cuenta de un número de una Wallet de criptomoneda… Esto lo tiene que identificar rápido y tiene que conocer muy rápido los procedimientos de quién lo tiene que investigar o a dónde lo tiene que derivar. Pero vamos, me preocupan casi más las estructuras que las personas.

El OSINT no es un tema complejo, evidentemente se puede ser complejo hasta el infinito, como todo, pero la actividad o sin básica, no es muy compleja, no es muy muy difícil. Pero creo que una de las cosas más importantes es el conocimiento de la amenaza que está o la amenaza o el interés que tenga de análisis.

Hace años, cuando en Estados Unidos empezaron los policías a tener pilotos de helicóptero, porque empezaron a meter helicópteros, lo que hacían era coger pilotos de helicópteros y formarlos como policía. Entonces, bueno, ya está. Se ha aprendido que es mucho mejor tener un policía que sabe patrullar y formarlo como piloto de helicóptero, porque al final el helicóptero es un medio, no es un fin. ¿Entonces, al final para que utiliza el helicóptero? para patrullar. Sí, no sé cómo patrullar, no me vale de nada el helicóptero.

Pero el objetivo básico, el último, mejor dicho, no es el OSINT, es la amenaza, el OSINT es una herramienta más; igual que un operador HUMINT, un manipulador, tiene que saber que le tiene que preguntar a la persona, tiene saber cuál es la amenaza, cuáles son sus gaps de información, para buscar y seleccionar una persona que le puede dar esa información. Como no conozca la amenaza, que una persona sea muy buena tratando personas, no vale de nada porque no le va a poder exprimir la información que es de interés para la unidad. No sé si te he contestado o me he ido por los cerros de Úbeda.

En cuanto a la adquisición de información. ¿Con que método lo soléis hacer? Pasivo, semipasivo o activo o depende de la operación o primero se empieza por pasivo y luego se pasa esa barrera…

Hay fases, se utilizan los 3.

El pasivo, por supuesto. El pasivo es muy general, como te he dicho, pues en el tema de propaganda y demás. Hay una discusión doctrinal y legal de si el semiactivo y el activo son OSINT o no. Porque al final interactúas, nosotros mantenemos el criterio de que, si tú tienes un perfil de observación en una red social y miras lo que está abierto, pues eso,

es legal y no está haciendo nada. Si tú interactúas con una persona, aunque sea con likes y tal, ya digamos que vinculas tu nombre o tu perfil, tu nick o lo que sea, evidentemente nadie te obliga a que sea de verdad, porque de hecho en la vida real no son reales.

Otro ejemplo, hacerte amigo para que puedas ver lo que él no enseña en público. Ahí hay serias dudas de que eso lo puedas hacer como OSINT por qué al final estás utilizando engaño. No es lo mismo entrar en la casa de una persona porque te invita porque eres amigo, que porque te deja entrar porque eres el reviso del gas que estás utilizando un disfraz. ¿Hasta dónde está esa mentira?

Pues ahí hay dudas, digamos doctrinales o legales; porque en su contrario lo que te dicen es bueno también puedes ligar con una persona, ir a su casa y mentirle con tu nombre, que si estás casado o no estás casado y 50000 cosas.

El pasivo siempre, el activo y el semi activo también los utilizamos nosotros, lo que pasa que vamos además a una más, que es la interacción activa totalmente con "suplantación" de identidad. Pero todo eso va con orden judicial en una investigación y la creación de la figura del agente encubierto virtual que solamente fuerzas y cuerpos de seguridad lo podemos usar.

En cuanto a lo de los agentes encubiertos, hubo una reforma, creo recordar que fue en el 2015, esta me la sé porque estuve en parte del grupo de trabajo de la reforma, en la que se introdujo el agente encubierto digital y eso es activo, puro. Ahí se utiliza ese engaño.

Normalmente, por ejemplo, la captación de yihadistas, normalmente ellos hacen una búsqueda, una especie de phishing, ven la gente que se mueve en las redes sociales, pero posteriormente los van integrando en grupos cada vez más cerrados para hacer esa limpieza de la gente que es más radical o cercana a unas ideas extremistas yihadistas, o bien para intentar detectar fuerzas y cupos de seguridad y servicios de inteligencia.

Entonces, si tú no superas esas barreras, evidentemente te quedas fuera y ya te han detectado. Entonces, tienes que prepararlo, etcétera, etcétera, y entrar. Eso se hace con autorización judicial, una persona, digamos, por el mero hecho de que esté muy interesado, pues en un foro privado en el que por ejemplo se hable de fabricación de artefactos explosivos de forma casera, pues bueno, no dejas de tener un pequeño engaño en el que fuerzas ahí a que te deje entrar donde no te hubieran dejado entrar si supieran quién eres. Entonces, hay cosas que están ahí en límite. Nosotros teníamos todas las fases,

el OSINT pasivo es la mejor y es la base de todo esto. Hamás tuvo publicaciones, revistas, periódicos, publicaciones especializadas, hay un montón de cosas que te dan mucha información de inteligencia básica. Por ejemplo, los otros países de movimientos, ideologías de todo tipo, pues normalmente la ideología de un grupo que puede ser una amenaza. Por ejemplo, ultras, es pública porque ellos necesitan publicar esa ideología para captar adeptos. Otra cosa que si luego se van a cargar a una persona lo van a matar, le van a meter la paliza, eso no lo publiquen. Pero su ideología sí, todo eso también es una información muy buena para ir definiendo, pues actividades de investigación o qué es un movimiento activista, político o de cualquier otro tipo, sin ningún peligro o cuál puede saltar la barrera. Ejemplo, Greenpeace pueden realizar actividades incluso ilegales. Es decir, tú tienes que saber, tienes que intentar si se publica de alguna forma van a intentar entrar en una central nuclear es un delito, por mucho que ellos sean activistas, pero no son delincuentes, pero algunos sí cometen delitos. Por lo cual son delincuentes y hay que seguir y hay que intentar adelantar esa barrera de seguridad, si podemos evitar por unas patrullas que entren en la central nuclear, pues nos ahorramos todo el resto de problemática que podemos tener.

Y al final de todo, desde la prevención.

Sí. Prevención sí es. Al final si yo adelanto la barrera, pues me interesa saber qué acciones se van a hacer. Eso pasa con las manifestaciones, que siempre hay dudas. Bueno, es que las manifestaciones, las manifestación en sí, misma no es un problema, no es una cosa delictiva ni mucho menos. La manifestación, que está coordinada, debe tener una estructura de seguridad, se montan unos o antidisturbios o una protección policial por si caso. Si luego tú tienes conocimiento de que hay una serie de ultras embebidos en la manifestación que van a intentar asaltar el congreso, eso sí lo puedes saber, tu configuración de despliegue no es el mismo. Eso es importante a nivel de prevención.

Vale, y luego en cuanto a las fuentes que usáis (primaria secundarias terciarias) Bueno, entiendo que todas ¿no?

Todas. Evidentemente si vas a fuentes primarias es lo ideal. Las fuentes secundarias hay que tener mucho cuidado, pasa mucho con la prensa. Al final muchas veces la prensa es una fuente secundaria porque suele beber de las primarias que pueden ser o los servicios

de seguridad o los gobiernos o las agencias de noticias. Entonces luego te coges 5 periódicos distintos y dices bueno es que dice lo mismo, y es que tienen la misma fuente.

Entonces hay que tener mucho cuidado con las secundarias y las terciarias, porque lo que pueden hacer es envenenar o falsear el análisis que tú haces. Eso es muy importante, sobre todo, por ejemplo, con los informes de inteligencia. Tienes que ver si la fuente de lo que te dice cada país, porque al final dices es que 5 países me dicen lo mismo, bueno, cuidado, ¿dicen lo mismo con medios propios o dicen lo mismo porque están, digamos, integrando información de un tercero que ya los ha llevado por este camino?

Ya que al final acaba siendo desinformación.

Se debe tener mucho cuidado. Este es el punto focal. Está todo inventado, es decir, la desinformación que es muy de OSINT y muy tal, pero al final está inventado. Tú lo que tienes que hacer es una campaña de influencia entonces lo que haces es intentar que determinadas informaciones, sea a través de prensa o de otros medios de personas que escriben libros o revistas especializadas. Si llevas al final un tiempo trabajando un tema, por eso es importante especialización en el tema concreto, tú ves ya cada autor de que te cojea. Sabes que tiene unos sesgos interiorizados.

Es como los periódicos, o sea, no tienes que leer uno, tienes que leer varios y cada uno tiene su sesgo. Todos tienen un sesgo. El que sea, político, social, deontológico, el que sea, tú tienes que conocerlo. Por eso, cuando te especializas en una materia tus productos son de más calidad, porque no mueres en ese sesgo que es imposible que sepas.

Además, haciéndolo con traductores automatizados, porque no eres capaz de ir a la fuente primaria, es otro tema. Por ej. China ahora en guerra comercial en tal, en influencia geoestratégica. ¿Cuánta gente habla chino? El idioma es muy importante porque te impide ir a la fuente primaria de la información y normalmente vas a informes masticados ya por otros que introducen su sesgo de información.

El idioma es una cosa muy importante, ahí nos está ayudando mucho la inteligencia artificial y demás. De hecho, la barrera del idioma es un problema porque normalmente, el problema no es tanto de traducción como de interpretación. Yo puedo traducir con un Google, pero es que hay determinadas cosas que no significan lo mismo o no tiene las mismas connotaciones en un idioma que en otro.

Entonces, cuando nosotros tenemos a nuestros traductores, que normalmente son intérpretes, pues te puede decir, bueno, es que este hace referencias, pero es que esta palabra, tiene connotaciones totalmente distintas, necesito el contexto para saber de qué están hablando.

Eso te lo da un intérprete, no un traductor. Eso es muy importante también. Es una barrera muy importante que tenemos para llegar al final a desgranar una ideología, el idioma.

Vale, y en cuanto al ciclo de inteligencia, ¿se usa el del CNI, o tenéis uno propio?

El ciclo de inteligencia en realidad es una herramienta muy básica, el rosco con sus cuatro fases. Lo que sí que cambia un poco, sobre todo cambia mucho, en función de las estructuras cambian las fases de obtención y de elaboración. Si yo tengo integrados mis equipos OSINT, pues las sub-fases pueden cambiar. Si yo tengo mi unidad y mis capacidades, doy una orden de obtención, digamos, le digo a mi gente vigílame esto. Si no las tengo integradas, tengo que hacer una petición de tarea a otras unidades que tienen su propio ciclo de obtención.

Hay dos ciclos de inteligencia básicos.

El americano de 5 fases y el que utilizamos todos los demás que es de cuatro. Pero al final llamarlo como quieras, porque al final es un proceso, muchas veces no es un límite de aquí hemos entrado y aquí salimos, sino que es un proceso.

Y sí que hay otra parte en la parte de estructuras, que es fundamental y cambia bastante el ciclo, pero internamente digamos, los sub-ciclos, que es cuando los analistas tienen acceso a los obtenedores o no tienen acceso. Es decir, hay veces que el ciclo de obtención es un ciclo que se pasa a unos elaboradores y luego, pues la valoración de la fuente, técnica, etcétera. Otras veces se permite que el elaborador tenga acceso a los obtenedores de OSINT, de tal forma que digamos que sea más dinámico y la valoración se haga entre todos. En algunos sitios o algunos sistemas se mantiene totalmente estanco porque dicen que así haces una valoración más aséptica.

Entonces, es verdad que hay muchas cosas que son muy subjetivas. En algunos sistemas, esta separación se mantiene estrictamente para asegurar una valoración más aséptica y objetiva, porque, aunque se pierde agilidad, se gana en objetividad

Si no, pues lo metes más ágil, más amigable, pero puede decaer en una falta de objetividad porque al final, si el elaborador viene influido por el obtenedor, al final no hace su labor exactamente bien. Entonces eso es un poco las diferencias que existen. Nosotros usamos el ciclo de inteligencia normal y corriente. Nosotros preferimos la valoración estrecha, que puede sacrificar un poco de objetividad inicial, pero se compensa con las revisiones y diligencias posteriores para asegurar la precisión y objetividad de los resultados.
Y los servicios de inteligencia más puros, digamos, suelen utilizar más diferencias o más cajitas separadas y estancas para garantizar esa objetividad.

Vale y en cuanto a retos, incluso teniendo herramientas, formación, etc. ¿qué retos hay en el mundo cyber que obstaculice o qué dificulte el OSINT?

Pues mira, la privacidad que está muy bien para unas cosas, pero a nosotros nos complica mucho. Está muy bien porque nosotros tenemos una parte de prevención que es que todo el mundo sea consciente de lo que publica, lo que no publica y que cada vez tengamos acceso a menos cosas si no eres amigo digamos de una red social. Eso nos complica porque antes todo el mundo publica en abierto y eso era maravilloso para nosotros.

Ahora esto lo va complicando, por eso tienes que dar un pequeño salto, normalmente de pequeña vulneración o de un pequeño engaño, etcétera para entrar. Los idiomas, como nos hemos globalizado eso es un reto increíble.

La inteligencia artificial va a ser un reto, una amenaza y un desafío. Porque por una parte te va a ayudar en muchas cosas, por ejemplo, las traducciones. Una herramienta bien trabajada es posiblemente que las traducciones, aunque a lo mejor no lleguen por lo menos en un tiempo razonable a una interpretación, pero van a ser mucho mejores que las anteriores, van a ser más rápidas, puedes automatizar muchas tareas.

¿Cuál es el problema? Las deepfakes. Es un problemón que vamos a tener muy grande, porque ahora ya es muy difícil, la propia inteligencia artificial te da herramientas para detectar, pero estamos en esa parte de esas falsedades, no sé cómo se llama cómo definirlo no, es decir tan bien realizadas, que te sale ahora un presidente o un ministro de una compañía y tienes unas horas en las que no sabes si es verdad o mentira. Es más, si está muy bien hecho y muy bien definido por un servicio de inteligencia, te llegará incluso la

duda de que un ministro de Defensa diga que va a mandar tropas a un país y que 2 horas después o 1 horas después, el propio Gobierno desmienta. Siempre queda el runrún de, "lo han desmentido porque se han visto la respuesta ciudadana, pero en realidad querían."

Esa esa duda, puede llegar a desestabilizar un país. Bueno, eso es un problema bastante importante.
Otro problema, las herramientas tecnológicas cada vez son más sofisticadas, pero son más caras. Nosotros tenemos un problema como servicio, como cuerpos de seguridad y como servicio de inteligencia, como siempre, vamos detrás de los malos, eso es evidente y eso no va a cambiar nada. ¿El tema es cuánto es el gap? ¿Cuántos pasos vas por detrás de ellos?

Y el problema es que, como las herramientas cada vez son más sofisticadas y caras y, además, la transparencia digamos que se da a los ciudadanos es mayor, se ralentiza muchísimo el proceso de adquisición. ¿Qué pasa? Cuando adquieres un producto, a lo mejor 1 año después ya no te vale. Eso estructuralmente, esa falta de agilidad en la contratación es un problema bastante grave.
España, además, es un país muy garantista para muchas cosas, con lo cual, bueno, el principio de publicidad … al final qué pasa, esto va tan rápido que cuando ves una herramienta dices la quiero hasta que la tienes, que ha pasado año y medio, eso no vale nada, vale mucho, pero no está, ya no es la primera.

Aquí hay una competición, porque las propias empresas, sobre todo en redes sociales, en telefonía y demás, lo primero que venden al ciudadano es seguridad, porque claro, no van a entrar a colaborar contigo porque dejan de vender, claro, porque la seguridad para todos los ciudadanos es muy buena, pero es que el malo también es un ciudadano. Entonces, ese ese límite para nosotros es muy complicado. Esa colaboración que debería haber, sobre todo con las redes sociales, con los servicios de mensajería, etcétera. para ellos es un problema, porque si colaboran contigo dejan de vender un producto. Pasó con BlackBerry, que era la referencia y nosotros hacía años que interveníamos. Cuando empezaron a salir las sentencias en las que se veía claramente que la Guardia Civil intervenía la mensajería, BlackBerry desapareció del mercado. Entonces pasó con Apple con el San Bernardino, con el iPhone, etcétera.

Entonces, claro, esa colaboración que a nosotros nos venía muy bien para hacer un OSINT más avanzado, vamos a llamarlo así para intentar entrar o conseguir más información de

los perfiles, desde dónde se conecta, qué IPS tienen, que no es exactamente OSINT, va más allá porque es una herramienta de investigación, pues te topas con que las empresas no quieren colaborar. Porque si trasciende, la ciudadanía deja de usarlas. Entonces bueno, eso es otro de los retos, es el que me faltaba por decir, que no es exactamente OSINT, pero va vinculado a ello porque no facilita la integración de las herramientas, tampoco.

Vale, ¿algo más que quieras comentarme?

Yo creo que más o menos hemos hablado de todo. OSINT es una cosa que se va a quedar. Sí que es verdad, y he tenido bastantes discusiones con gente, el OSINT es una herramienta básica, pero el OSINT no lo da todo, tú al final el toque de calidad lo tienes que dar con otros medios de obtención. OSINT es una herramienta base, pero no es el medio de obtención, por definición. OSINT te da la base, pero el toque de calidad te la da la fuente humana, la intervención, el SIGINT…

Eso es lo que te da el toque de diferencia respecto a lo demás, porque OSINT lo tienen todos. Debemos tener es tener en cuenta que la materia prima todo El Mundo la tiene por definición. ¿Dónde tenemos que darle el toque de calidad? En el primer analista. El analista operativo que le llamamos nosotros, que es el primer analista que coge eso y luego el analista ya de elaboración que integra toda esa información. Ahí es donde debemos tener la gente formada, más que en la parte técnica, bajo mi punto de vista, es la parte de entender qué está investigando.

Vale por mi parte, creo que no se me queda nada, la verdad que no tengo ninguna pregunta más, así que se me ocurra ahora mismo. Si tienes alguna duda o algo más que me quieras comentar.

No, estamos a disposición para lo que necesites con mucho placer.

Pues nada, muchas gracias por todo. Un saludo. Adiós Chao.

No, gracias, gracias a ti Andrea, adiós.

11.3.6 Transcripción entrevista 6

Buenos días. ¿Qué tal, me escuchas?

Hola, Buenos días, ¿qué tal? Sí perfectamente Andrea, un placer.

Nada, el placer es mío. Bueno pues empezamos. Cuéntame sobre tu trayectoria profesional y qué relación tienes con las fuentes abiertas.

Nosotros lo que es la obtención de información en fuentes abiertas la usamos con el objetivo de prevenir cuestiones de todo tipo que puedan afectar a la seguridad dentro del municipio. También, no estamos monitorizando constantemente fuentes abiertas, sino que lo hacemos en base a hechos concretos. Por ejemplo, ahora en mayo vienen las fiestas de San Isidro, que aquí concentran a mucha gente y tal, pues ponemos un poco el foco en las fuentes abiertas para ver qué información podemos obtener que pueda ser relevante para nosotros y poder anticipar los dispositivos que realizamos, no lo hacemos para investigar.

Se puede utilizar para cuando hay quedadas a lo mejor de bandas latinas, cuando hay quedadas de coches tuning, que a lo mejor pueden afectar a la circulación de vehículos en el municipio porque se concentran mucha cantidad de coches y no están autorizadas ese tipo de concentraciones normalmente. Cuestiones de ese tipo.

¿Y aparte de las fuentes abiertas, utilizáis alguna otra disciplina de inteligencia como Humint, Geoint, Imint o algo?

A ver en policía, Humint siempre se utiliza. Te quiero decir de toda la vida. Geoint no tanto porque nosotros utilizamos el tema de análisis de hechos delictivos posicionados en un GIS. Sí que utilizamos el análisis, pero eso a posteriori. También tiene como objetivo la prevención, pero nosotros lo que hacemos es utilizar los sistemas de información geográfica para posicionar los hechos delictivos y, a partir de ahí, aplicarles herramientas de análisis que nos pueden dar una estimación de qué puede ocurrir en el futuro. Y entonces, pues si sabemos que en una determinada zona se están produciendo hechos delictivos, pues la prevención va enfocada a esa zona y no a otra. Todos esos informes que se realizan mensualmente se divulgan a todos los mandos para que ellos ya orienten los dispositivos de prevención en función de los recursos, en función del día de la semana, de horario, de disponibilidad, etcétera. Aunque hay algunos que ya vienen impuestos por los planes que tenemos, es decir, hay planes que están programados, donde, por ejemplo, el plan de fin de semana, pues el fin de semana hay que hacer dos controles o 3 controles enfocados a reducir la siniestralidad vial, por ejemplo, pues se hacen en zonas que ya están tasadas y que hemos estudiado previamente. No se hacen de forma aleatoria. El control si es aleatorio, pero la zona no es aleatoria.

Vale, y en cuanto al perfil del investigador en fuentes abiertas, ¿cuáles serían las características que debe cumplir, así a rasgos generales?

A ver, para mí el perfil de un agente que quiera trabajar con fuentes abiertas, primero le tiene que gustar mucho la tecnología, es decir, tiene que ser innovador en el sentido de que siempre es preferible utilizar herramientas o software que no conlleva ningún coste a software que conlleva coste. Evidentemente software con coste tenemos en el mercado mucha oferta, pero no podemos invertir constantemente o la prioridad no está en invertir en fuentes abiertas, en el caso de la policía local. Entonces siempre tiene que ser a través de la de la inquietud, de la innovación, de la gente que quiera trabajar ahí. El perfil que tenemos es gente que le gusta mucho el tema de las fuentes abiertas y que está o intenta estar al día en software, en nuevo software, normalmente libre, vale? y no software de pago, en principio. También tenemos software de pago, pero para otras cuestiones, por ejemplo, para análisis de vídeo software de análisis de imágenes que lo que hace es ahorrar tiempo en cuanto a buscar imágenes dentro de un sistema muy grande. Pues eso sí, es software de pago, pero no es fuentes abiertas, son fuentes cerradas.

O sea, ¿que se mantenga actualizado en todos estos avances tecnológicos?

Si, que sea una persona inquieta que le guste la innovación, que esté en constante desarrollo, que esté muy motivado a querer buscar o a querer conseguir el objetivo que se le ha marcado, es decir, porque si al final es una persona que busca con herramientas tradicionales y no va más allá, no tiene interés en buscar más, pues al final nos quedamos un poco en la superficie.

Vale, y luego, en cuanto a las fuentes de información primarias, secundarias y terciarias, ¿con cuáles trabajáis? Intuyo que, a lo mejor, ¿con todas?

A ver, nosotros trabajamos con todas las fuentes, no decimos que no a ninguna fuente, todo lo que sea información nos interesa. ¿Entonces, qué ocurre? Que lo que luego sabes que esa información nosotros hay que analizarla, valorarla y ponerla un poco en relación con todas las fuentes. Ver qué nivel de credibilidad tiene la información que estamos obteniendo y dar un porcentaje de credibilidad tanto a la fuente como a la información que nosotros elaboramos. Evidentemente el cien por cien, o sea,

esto va a ser así o es así cien por cien, nunca lo tenemos, nunca lo vamos a tener, pero nos tenemos que acercar al máximo sobre todo siendo muy rigurosos en la obtención de la información, en la valoración de la fuente en estas cuestiones porque nos va a dar un nivel de credibilidad que nosotros al final lo que estamos moviendo son recursos y eso cuesta dinero, ¿sabes? Te quiero decir, que nosotros montamos un dispositivo porque tenemos una información y no hayamos sido capaces de valorar la credibilidad de la fuente, el hecho, etcétera y montemos un dispositivo que luego no ocurre nada, pues supone un coste importante.

¿Y en cuanto a los métodos de obtención activa, pasiva, y semipasiva, cuál es el que más utilizáis?

A ver, nosotros lo que más utilizamos es una obtención activa. La pasiva no la utilizamos porque no tenemos medios para para poderla llevar a cabo. Entonces, la obtención siempre, ya te he dicho que es, marcamos un objetivo y nosotros somos los que buscamos la información.

Es verdad que tenemos, a ver si quieres llamarle obtención pasiva, pues sí que tenemos alertas en determinados buscadores donde nos da la información filtrada ya sobre conceptos o sobre cuestiones que son de nuestro interés, pero normalmente es una búsqueda activa.

Y luego, a grandes rasgos, ¿en qué momentos concretos hacéis uso de las fuentes abiertas? Como me has comentado un poco antes, pues eso tema de fiestas del municipio, ¿qué más?

Por ejemplo, siempre que hay algo, algún evento o alguna cuestión que va a congregar a muchas personas dentro de lo que es el municipio, siempre intentamos, bueno, siempre hacemos una búsqueda en fuentes abiertas.

Imagínate, un concierto de un determinado cantante o una determinada cantante en Alcobendas. Depende del número de personas que vaya a congregar, imagínate que va a congregar a 4.000 5.000, 6000 personas, o de ahí para arriba, nosotros siempre monitorizamos un poco la fuente para saber, bueno si es muy famoso no, pero sí qué tipo de cantante es, qué público suele venir a ese tipo de conciertos, qué problemáticas se dan

antes o después de los conciertos, qué problema ha habido en otras ciudades donde se han desarrollado ese tipo de conciertos… Te pongo un concierto, como ejemplo, pero podría ser un partido de rugby, un partido de fútbol, un partido de hockey...

Todo lo que tiene que ver con las fiestas patronales que en un determinado espacio congrega un número muy importante de gente durante varios días de la semana, pues para nosotros es importante.

¿Y existe algún protocolo general o algún ciclo específico que utilicéis para fuentes abiertas?

Todas las unidades tienen un protocolo específico. En el caso nuestro, en el área de la unidad de inteligencia para la convivencia, tiene un protocolo específico de qué y cómo se tiene que actuar en determinadas cuestiones. Si existe un protocolo interno.

¿Y en cuanto al ciclo de inteligencia, ¿cuál utilizáis el de cuatro fases, el de seis...?

Pues nosotros utilizamos el de cuatro fases, es decir, que lo intentamos simplificar. Sí que es verdad que también lo adaptamos un poco a las necesidades que nosotros tenemos. Intentamos seguir el ciclo, un ciclo sencillo, pero que si tenemos que aplicarle cualquier cuestión, como puede ser una reevaluación de la información o porque la información tiene sentido o tiene valor en tanto en cuanto no hay una información nueva que lo que tenemos elaborado nos lo tira atrás, entonces a veces esto es tan dinámico que lo que nosotros tenemos claro, o teníamos claro ayer por la tarde, pues igual durante la noche, o a lo largo de la mañana tenemos otra serie de información y eso cambia, ¿sabes?. Entonces hay que reevaluar y volver a elaborar un informe con datos concretos con información actualizada.

Te quiero decir que, es que en policía los informes que nosotros hacemos, o sea, si por ejemplo hacemos un informe de un grupo concreto o, imagínate un grupo, una banda juvenil o tal, una cosa es la filosofía de cómo funciona, cómo está estructurada y tal, y otra cosa es cómo está funcionando a día de hoy. Es decir, hoy en día puede haber un hecho que haya ocurrido ayer en Madrid, que cambie la dinámica, cambie donde se juntan, cambien las medias de seguridad que adoptan para que no sean detectados, incluso cambien en su forma de vestir, pues para evitar ser identificados en la calle, por ejemplo.

Entonces todo eso hace que lo que es el informe, que es muy bueno hoy o antes de ayer, pues hoy no tenga tanto valor. A medida que pasa el tiempo va perdiendo un poco el valor.

¿Y ahora actualmente, cuáles son las principales retos y dificultades que nos encontramos en una investigación en fuentes abiertas?

A ver, hay dos partes: Una parte que no todo el mundo dentro de las organizaciones está sensibilizado o cree que es importante el obtener información de fuentes abiertas, eso sería una parte de cultural de las organizaciones, que evidentemente las organizaciones son muy grandes, siempre va a haber gente que cree que esto es interesante y gente que siga su dinámica normal y diga, no, yo voy a seguir como siempre, no, a mí no me traigas nada nuevo. Y eso sería una parte, la humana, la parte de cambiar y sensibilizar a la gente que eso tiene mucha importancia que cada vez más tiene más relevancia para el trabajo que nosotros hacemos dentro de la prevención. Y luego, la otra parte, sería la parte de inversión, es decir, que también quien tiene la capacidad de destinar fondos para para poder comprar programas, software, etcétera, pues tenga esa sensibilidad y quiera y crea que es bueno y quiera que se invierta en ese software, que no tengamos que estar utilizando diferentes software de fuentes abiertas que hoy software libre pues ya sabes que hoy puede estar funcionando un programa, mañana vas a tratar de trabajar con ese programa y el programa ya ha dejado de existir, no?. A ver, es verdad que la mayoría de los programas que tienen ya una tradición, pues bueno, pues no. Tienen la versión de pago, la versión libre, como muy recortada como puede ser Maltego o cualquier otro tipo de programa, pero te puedes encontrar otros programas que los puedes estar utilizando perfectamente dos años y al tercer año ese programa deja de existir y ya no lo puedes utilizar.

Si, Igual que herramientas que nacen y mueren, al final hay algunas que el tiempo de vida, por así decirlo, es muy, muy corto.

Sí.

Ahora que está tan en auge el tema de la IA y todo esto, ¿cómo crees que va a afectar en las investigaciones?

A ver, yo creo que la IA va a afectar. Vamos a ver, la IA es una realidad que queramos o no queramos ver, aparte de jugar con ella, podemos hacer muchísimas cosas. Entonces, yo sí que creo que la IA va a ser muy importante aplicada dentro de lo que son las bases de datos cerradas que tiene lo que es la policía, es decir, la policía al final todos los días recibe multitud de información y aunque esté muy organizada en una base de datos, o sabes cómo la tienes que llamar para poderla recuperar o, si no, puedes tenerla ahí y no la recuperas. Entonces, yo creo que la IA lo que va a hacer es facilitar mucho la búsqueda dentro de la información que tú tienes dentro de tu base de datos, independientemente que la puedas utilizar para bueno, pues para fuentes abiertas, que evidentemente, también lo puedes utilizar.

Si, como más para aspectos objetivos, ¿no? de ordéname esto o extráeme los que empiecen por tal número o cosas, así como más objetivas.

Sí, a ver, yo lo veo más ahí. Lo veo más ahí en el sentido de decir, oye, mira, necesito que me digas de mi base de datos que puede tener miles y miles de datos, que me digas este tipo de información, trates de relacionármela con días de la semana con no sé, que le hagas una búsqueda mucho más amplia que lo que es, por ejemplo, lo que podemos hacer ahora. Pues ahora lo tradicional es búscame a las personas que midan 1,80 entre 1,75 que habían sido detenidas en los últimos 5 años. No sé, o búscame todos los modelos de Ford que hayan estado implicados en tal hecho delictivo, para yo tener una lista de candidatos…que es a lo que se tendía o lo que se tiende.

No sé, yo creo que lA puede enriquecer mucho más la extracción de información de base de datos, tan amplia, con tanta información, que es imposible que tú la puedas relacionar, porque muchas veces aquí lo que ocurre es que pues me imagino que os pasa a vosotros como alumnos, no?, que cuando la gente está trabajando en un área o en el área de Policía Judicial o en el área de distrito, pues entre nosotros muchas veces hablamos y decían: oye, no te acuerdas de aquel coche o no te acuerdas de aquella persona que en aquel momento hizo un hecho delictivo que se parece al que estamos ahora viendo, y tal?, es decir, que es más el factor humano el que hace esa función de recuerdo que lo que es

la máquina, que es lo que es, el ordenador. Yo creo que ahí la IA sí que nos puede ayudar mucho, es decir, no solamente a generar informes, a buscar candidatos, a buscar información…, cualquier tipo de información que tú tengas en tu base de datos, pues te lo va a ordenar y luego tú ya determinarás si esa información es buena, que para eso estamos los humanos. Si esa información es buena y es útil, o esa información no es tan buena o no es tan útil.

Vale así un poco por terminar, cómo ves el futuro del OSIN

Yo creo que el OSINT, de una manera o de otra, siempre se ha hecho. Es decir, siempre se ha hecho OSINT. Ahora tenemos herramientas informáticas, pero antes se buscaban archivos. Siempre se han buscado fuentes de información, pues para de alguna manera actuar de la forma más controlada posible. Entonces, la forma de actuar en policía de lo más controlado posible es tener o tratar de abarcar todas las fuentes de información posible, cuanta más información tengas mucho mejor. Entonces, hoy día, pues es evidente que en las redes sociales se mueven muchísima información. Tú no puedes cerrar los ojos a las redes sociales, tienes que estar también pendiente en qué se está moviendo, qué se está hablando en las redes sociales, porque eso puede repercutir a intervenciones que tú puedas hacer de carácter preventivo, me estoy refiriendo en este caso. Si estamos hablando de investigaciones, pues sería otro tipo de trabajo totalmente diferente al que nosotros hacemos. Es decir, que evidentemente también tiene muchísima información porque al final en redes sociales, si tú estás controlando un objetivo, pues puedes ver con quien se relaciona, cuál es su nick… Si ha subido fotografías, puedes ver si son fotografías, aunque puedes tener dudas o no, si están generadas con inteligencia artificial o no, te puede posicionar en qué zona está. No sé, una serie de cuestiones que te pueden ayudar a resolver tu intervención, pero que no es nuestro caso, es más la prevención.

Vale, pues por mi parte, no tengo nada más que añadir. Si quieres preguntarme algo o comentarme algo más.

¿Tu como ves el futuro de OSIN?

Pues yo veo que hay mucho, mucho futuro. Que va creciendo y que cada vez como que este tema está más reconocido, más valorado. No sé, yo creo que está muy ahora

a la orden del día y que al final en todos lados se usa OSIN, inconsciente o consciente en todos los cuerpos y seguridad del Estado, en las empresas privadas, también un montón… también por el tema de estudios de mercados. Todo esto del área privada. No sé, yo creo que va a haber mucho trabajo y que va a seguir creciendo y se va a seguir desarrollando.

Yo estoy totalmente de acuerdo contigo, es decir, el OSINT no solamente tiene aplicaciones en fuerzas y cuerpos de seguridad. Yo creo que las empresas privadas ya hace tiempo se han dado cuenta que el tener información de su sector o de su área de negocio les da una posición de privilegio en cuanto a la toma de decisiones y eso es importante. Entonces yo sí que tengo muy claro que tiene una trascendencia muy importante, que es fundamental. De hecho, antes, te quiero decir, hace 10-15 años no encontrabas ofertas de empleo de estas características y ahora encuentras muchísimas, lo que pasa que hay más ofertas de empleo que gente en el mercado que pueda dar solución a las demandas que muchas veces hacen. Soy consciente de que también buscan fuerzas y cuerpos de seguridad este tipo de perfil para llevárselo a la empresa privada, no? porque al final tú tienes que ir llenando el hueco o la necesidad que tienes. Entonces sí que creo que, bueno, que el desarrollo a medio largo plazo va a ser brutal y que las personas que se dediquen a gestionar todo lo que es OSINT, a ser los analistas de alguna manera de la información, pues van a tener un papel muy relevante. Si que, por ejemplo, hay que tener claro que, por ejemplo, en nuestro caso, que los analistas lo que hacen es analizar la información. Que la toma de decisiones la toma la persona o las personas que tienen que tomar las decisiones sobre la organización, es decir, que los analistas nunca van o vamos a tomar decisiones estratégicas dentro de la organización, simplemente vamos a poner a disposición

Pero sí que tenemos que ser conscientes de que nuestros análisis sirven para eso, para tomar las decisiones, por lo por lo tanto, pues tenemos que ser los más objetivos y los más meticulosos posibles a la hora de plasmar en los informes la información que nosotros estamos recabando.

Pues nada, te animo a que sigas ahí profundizando y a ver si tienes suerte y encuentras trabajo.

Si, muchas gracias.

Pues nada, gracias Andrea. Venga, muchas gracias, que tengas suerte, hasta luego.

Adiós igualmente, gracias Chao.