U N I V E R S I D A D A U T Ó N O M A D E M A D R I D

La SEI
School of Economic Intelligence & International Relations
Escuela de Inteligencia Económica y RRII
Universidad Autónoma de Madrid

Septiembre 2023

Volumen 15
ISSN 2660-7352
Editados por la Escuela de Inteligencia Económica y RRII
Editor Jefe / *Chief Editor*: Ángel Rodríguez García-Brazales

REPORTS DE INTELIGENCIA ECONÓMICA Y RELACIONES INTERNACIONALES

Psicología en la obtención de información de fuentes humanas online: Un enfoque comparativo de SOCMINT, HUMINT virtual e ingeniería social

Sofía Sánchez Margolles

El factor humano es clave en operaciones de inteligencia y ciberseguridad, representando una de las principales fuentes de información online. El presente estudio pretende analizar cómo la psicología puede contribuir al diseño de operaciones de obtención de información de fuentes humanas en línea. Para ello, los resultados son divididos en una comparativa de características y procedimientos de HUMINT online, ingeniería social y SOCMINT; y la aplicación de procesos psicológicos en las diferentes fases de HUMINT virtual.

Título: *Psicología en la obtención de información de fuentes humanas online: Un enfoque comparativo de SOCMINT, HUMINT virtual e ingeniería social*

Autor: Sofía Sánchez Margolles[1]

Volumen nº: 15. **Páginas**: 1-26

Fecha: 13 de septiembre de 2023

ISSN 2660-7352

Reports de Inteligencia Económica y Relaciones Internacionales

Editor jefe: Ángel Rodríguez García-Brazales

Editada por la:

Escuela de Inteligencia Económica y Relaciones Internacionales

Universidad Autónoma de Madrid

Campus de Cantoblanco

C/. Francisco Tomás y Valiente, nº 5, Módulo 10, despacho 303

28049 MADRID (SPAIN)

[1] Contacto: Luis Santos Sanz. Escuela de Inteligencia Económica y Relaciones Internacionales. Universidad Autónoma de Madrid. E-mail: sofiasmargolles@gmail.com

Contenidos

Resumen

El factor humano es clave en operaciones de inteligencia y ciberseguridad, representando una de las principales fuentes de información *online*. El presente estudio pretende analizar cómo la psicología puede contribuir al diseño de operaciones de obtención de información de fuentes humanas en línea. Para ello, los resultados son divididos en una comparativa de características y procedimientos de HUMINT *online*, ingeniería social y SOCMINT; y la aplicación de procesos psicológicos en las diferentes fases de HUMINT virtual. Se concluye que, pese a la escasez de publicaciones disponibles en abierto sobre los temas tratados, los conocimientos y técnicas de la psicología pueden ser de gran utilidad en operaciones HUMINT *online*.

Summary

The human factor plays a pivotal role in intelligence and cybersecurity operations, representing one of the primary sources of online information. The present study aims to analyse how psychology can contribute to the design of online operations for gathering information from human sources. To achieve this, the results are divided into a comparative analysis of characteristics and procedures of online HUMINT, social engineering, and SOCMINT, as well as the application of psychological processes in different phases of virtual HUMINT. It is concluded that, despite the scarcity of openly available publications on the topics addressed, the knowledge and techniques of psychology can be highly valuable in online HUMINT operations.

1. Introducción

En inteligencia, obtener la información necesaria en el momento adecuado marca la diferencia. La digitalización masiva ha permitido el acceso a cantidades ingentes de datos, dando lugar a la creación de nuevas tecnologías que facilitan su gestión y análisis. Sin embargo, si bien la tecnología es una herramienta necesaria, no es suficiente.

Pese a que el suministro masivo de información de internet permite, por lo general, un mayor acceso a diversas fuentes también plantea nuevos riesgos en la obtención de inteligencia, especialmente aquellos relacionados con la imposibilidad de análisis de todos los datos disponibles y la dificultad de recopilación de información de calidad (Dobák y Tóth, 2021). Aunque OSINT tiende a ser la principal fuente a la que se recurre en una operación de obtención de información, algunos autores afirman que de por sí sola no garantiza un análisis extensivo de una potencial amenaza (Giannetakis et al., 2020). Asimismo, la importancia creciente de OSINT en las últimas décadas no ha disminuido la relevancia de otras fuentes tradicionales como HUMINT (Gioe, 2017), sino que ofrece una nueva dimensión en la que aplicar sus técnicas.

Puesto que el mundo *online* no puede ser separado de la dimensión física y, considerando que la gran mayoría de las actividades *online* tienen un componente humano (Dobák y Tóth, 2021), el factor humano no debe ser descuidado en contextos virtuales. De hecho, ignorar las vulnerabilidades de las personas, que además representan el eslabón más débil de una cadena de seguridad (Mitnick y Simon,

2005; Mouton et al., 2014; Scheeres, 2008), ocasiona pérdidas económicas y fugas de información privilegiada tanto a nivel empresarial como estatal. Aunque la separación de las áreas tecnológica y humana, especialmente común en las estructuras organizacionales de agencias de seguridad nacional (Dobák y Tóth, 2021), dificulta la convergencia entre ambas, conocer dichas vulnerabilidades y saber cómo emplearlas a nuestro favor es una herramienta clave en inteligencia que no puede ser ignorada (Rodríguez y Sánchez, 2023).

El uso de fuentes humanas para la obtención de información con objetivos de inteligencia (HUMINT) no es novedoso. De hecho, algunos autores consideran las operaciones HUMINT como la forma más antigua de hacer inteligencia (Dillon, 1998; Sayre, 2004). Sin embargo, el universo *online* permite una multitud de nuevas posibilidades de uso de las herramientas HUMINT tradicionalmente empleadas en contextos cara a cara (Fialka, 2018). En la práctica, las relaciones virtuales representan un mecanismo infrautilizado de obtención de fuentes humanas (Koren, 2015). Las redes sociales ofrecen a su vez oportunidades que, combinadas con el uso adecuado de conocimientos y técnicas de psicología social y cognitiva, pueden facilitar el desarrollo de nuevas operaciones de elicitación con un menor riesgo para el agente de inteligencia que las lleve a cabo (Koren, 2015). No obstante, aunque se trate de dos contextos interrelacionados, el mundo virtual posee una serie de características que lo distinguen del mundo "real" o físico a las que los procedimientos HUMINT tradicionales deben ser adaptados.

Aunque la aplicación convencional de HUMINT no ha sido aún ajustada por completo a los avances tecnológicos, en los últimos años se ha comenzado a hablar de HUMINT virtual, una modalidad de obtención de información de fuentes humanas empleando el medio *online* que algunos autores consideran una "evolución inevitable" del HUMINT tradicional que, además, puede complementar las operaciones cara a cara reduciendo el riesgo al que se exponen los operativos o agentes de inteligencia (Koren, 2015). Asimismo, y al igual que ocurre con su versión tradicional, el HUMINT virtual permite el acceso a información no disponible en fuentes abiertas e incluso a áreas u organizaciones en las que resulta difícil, a la vez que arriesgado, introducir personal de inteligencia (Dobák y Tóth, 2021).

Las técnicas y objetivos de esta nueva modalidad de HUMINT son muy similares a aquellos característicos de la ingeniería social e inteligencia de redes sociales (SOCMINT), llegando incluso a solaparse en ocasiones. Sin embargo, a lo largo de la literatura parece haber cierta confusión entre términos, lo que dificulta el entendimiento y la coordinación de técnicas comunes a las tres. De hecho, conocer las similitudes y diferencias entre estas disciplinas permitiría al personal de inteligencia emplear las herramientas de ingeniería social y SOCMINT en operaciones de HUMINT virtual.

Uno de los puntos en común entre SOCMINT, HUMINT virtual e ingeniería social es la importancia del factor psicológico en sus operaciones. Algunos autores coinciden en que los avances en ciencias del comportamiento deben ser considerados en los grupos conjuntos de investigación e inteligencia para realzar los efectos de HUMINT *online*, afirmando incluso que el manejo de fuentes en la actualidad debería basarse en teorías de psicología social (Dhami, 2011) e incluir un mayor uso de técnicas de persuasión (Crous, 2009), lo que implica una necesidad de entrenamiento de los agentes de inteligencia en esta disciplina (Dhami, 2011).

Tanto las aportaciones de la psicología en inteligencia, como la relación de los humanos con la tecnología, son dos temáticas que ya han sido estudiadas en el pasado (por ejemplo: Dhami, 2011; Dorado Roldán, 2019; Giannetakis et al., 2020). Aun existiendo algunas referencias sobre operaciones HUMINT (por ejemplo: Army, 2006), la publicación en abierto de este tipo de estudios resulta poco común, ya que suele tratarse de información clasificada, por lo que no se dispone de una guía teórico-práctica que combine todos esos aspectos entre sí.

1.1. Objetivos

Este estudio se propone explorar el proceso de obtención de información por parte de fuentes humanas *online* y analizar qué aportaciones se pueden realizar desde el campo de la psicología para diseñar de manera más eficiente dichas operaciones. Para ello, se han discernido dos objetivos principales:

- Analizar las diferencias y similitudes entre SOCMINT, HUMINT virtual e ingeniería social *online*, para entender cómo pueden ser aplicadas a operaciones de inteligencia *online*.

- Estudiar cómo el conocimiento y las herramientas de la psicología pueden ser aplicados en el proceso de obtención de información de fuentes humanas de manera virtual.

Para desarrollar una aplicación integrada de la psicología y las últimas tecnologías para obtención de información *online*, se debe comprender cómo se solapan las disciplinas de SOCMINT, HUMINT virtual e ingeniería social. Tanto en la literatura como en la práctica suelen confundirse entre sí, a la vez que se intenta realizar una distinción clara sin considerar, con frecuencia, que los medios empleados en una de ellas pueden ser de utilidad en las demás.

En concreto, este estudio se centra en optimizar el proceso de obtención de información de fuentes humanas en operaciones activas encubiertas en internet, para lo que se realizará una comparativa de los procedimientos y las fases de HUMINT e ingeniería social a los que, posteriormente, se aplicarán aquellos procesos psicológicos que puedan resultar de utilidad.

Hay que destacar que, aunque las técnicas de psicología incluidas en este informe pueden ser empleadas en otro tipo de operaciones de inteligencia (por ejemplo, operaciones de influencia, desinformación o PSYOPS), su aplicación puede no ser trasladable debido a la diferencia de objetivos, recursos y agentes implicados. Por otra parte, por muy determinante que resulte el factor psicológico, no es el único elemento que debería ser considerado, sino que otros aspectos lingüísticos, legales, tecnológicos, etc. deben tenerse presentes.

2. Metodología

Los materiales empleados en esta revisión consisten una gran variedad de publicaciones obtenidas de diferentes bases de datos y buscadores. Debido a la reducida cantidad de publicaciones sobre el tema obtenida en un primer rastreo, no se estableció una acotación temporal de la búsqueda. Es decir, se han tenido en cuenta todas aquellas publicaciones relevantes, al margen del año en el que fueran publicadas. Tampoco se realizó un filtrado de las fuentes según el idioma de las publicaciones, aunque la mayoría de las obtenidas están en español e inglés. Sin embargo, sí se tuvo en cuenta su disponibilidad, ya que solo se pudo acceder a aquellas desclasificadas, publicadas en abierto o permitidas con la identificación de la Universidad Autónoma de Madrid.

Debido a la combinación de disciplinas en este trabajo, se emplearon una gran variedad de términos de búsqueda relacionados con inteligencia y psicología, entre los que se encuentran: *SOCMINT, social media intelligence, HUMINT, human sourced intelligence, social engineering, social engineering attacks, psychology, psychological processess.* Estos términos fueron introducidos en las búsquedas tanto en español como en inglés.

Inicialmente se realizó una búsqueda exploratoria de la que se extrajeron múltiples artículos, de los cuales solo se han empleado aquellos pertinentes respecto al objetivo de estudio. Posteriormente, se llevó a cabo una segunda búsqueda para obtener aquellas publicaciones referenciadas en los artículos obtenidos anteriormente que resultaran de utilidad. Por último, con el objetivo de aportar un contexto y favorecer la integración de los resultados, también se han empleado publicaciones adicionales no obtenidas de la búsqueda bibliográfica inicial.

3. Resultados

De acuerdo con los dos objetivos propuestos para este estudio, los resultados han sido divididos en dos apartados principales. Por un lado, en el análisis de conceptos se lleva a cabo un estudio detallado acerca de las disciplinas de SOCMINT, HUMINT virtual e ingeniería social, con el objetivo de comprender cómo sus objetivos, herramientas y procesos se solapan entre sí. Esto facilita un posterior análisis de las fases establecidas por diferentes autores para las tres disciplinas, puesto que el segundo apartado de aportaciones psicológicas será ordenado de acuerdo con la clasificación de fases que mejor se adapte al ciclo de HUMINT virtual. Es decir, en la segunda parte de los resultados se expondrán los procesos y herramientas derivadas de la psicología que puedan resultar de utilidad en la obtención de información de fuentes humanas por medios virtuales.

3.1. Análisis de conceptos

Aunque la literatura tiende a separar los conceptos de HUMINT y SOCMINT, ambos están intrínsecamente relacionados en la práctica de obtención de información *online*. En el caso de la ingeniería social la diferenciación suele ser aún mayor, debido principalmente a que esta se considera por lo general un ciberataque ilegal (Dobák y Tóth, 2021). A continuación, se presenta una breve descripción de cada una de estas disciplinas, incluyendo además cómo se relacionan entre sí.

Por último, se realiza una comparativa de las diferentes clasificaciones de fases de HUMINT e ingeniería social, con el objetivo de identificar la clasificación que mejor se adapte a la práctica real de obtención de información de fuentes humanas por medios virtuales.

3.1.1. Inteligencia de Redes Sociales (SOCMINT)

Aunque inicialmente era denominada SOCINT (Lisa Institute, s.f.), la inteligencia de redes sociales o SOCMINT es un tipo de inteligencia derivada u obtenida de redes sociales (Omand et al., 2012). Es una disciplina que suele acompañar a OSINT pero, mientras que SOCMINT está exclusivamente dirigida al ciberespacio y permite obtener información tanto abierta como privada, OSINT no puede ser reducido exclusivamente al ámbito virtual y solo permite el acceso a información abierta para todo el público (Dobák y Tóth, 2021). Además, SOCMINT requiere la creación de un perfil en al menos una de las múltiples redes sociales con el objetivo de obtener información (Erdész, 2018), mientras que en OSINT no es estrictamente necesario.

Pese a todo, y aunque la literatura coincide en que SOCMINT incluye los mismos procesos de obtención de información tradicionales aplicados a las RRSS (Erdész, 2018), los límites de su definición no están completamente claros (Antonius y Rich, 2013). De hecho, en ocasiones se requiere un conocimiento profesional básico sobre HUMINT para la correcta realización de SOCMINT (Dobák y Tóth, 2021), puesto que en ambos casos la información obtenida proviene de fuentes humanas. La inteligencia de redes sociales es, en definitiva, un claro ejemplo del rol primordial de la tecnología en la obtención de información sobre personas, siendo su integración con HUMINT considerada esencial para ciertos tipos de operaciones, como, por ejemplo, aquellas relacionadas con amenazas terroristas (Lombardi et al., 2015).

3.1.2. Inteligencia de Fuentes Humanas (HUMINT)

HUMINT se refiere al conjunto de métodos y herramientas que permiten la adquisición de información de fuentes humanas (North Atlantic Treaty Organization [NATO] Standardization Office, 2021). También ha sido definida como la disciplina de inteligencia que incluye cualquier tipo de información que

pueda ser recogida por medio de fuentes humanas (Giannetakis et al., 2020), empleando sus vulnerabilidades (Rodríguez y Sánchez, 2023). Aunque para la definición de HUMINT existe un mayor consenso, quizá por tratarse de la forma más antigua de hacer inteligencia (Dillon, 1998; Sayre, 2004), hay diferentes aproximaciones y usos de ella. Mientras que algunas de las escasas publicaciones disponibles en abierto sobre esta temática se centran en HUMINT como método de interrogatorio o reclutamiento de informantes, este estudio se centrará en operaciones de elicitación *online*, ya sean de contacto único (*one shot*) o contacto continuo. En otras palabras, se busca establecer un contacto virtual con una fuente humana que será influenciada con el fin de que aporte la información deseada, sin que dicha fuente llegue a saber de las intenciones o la procedencia del operador HUMINT.

La diferenciación de los dos actores clave en HUMINT tradicional, agente y fuente, también puede ser aplicada a su versión virtual y, por lo tanto, se emplearán dichos términos para referirse a la persona perteneciente al servicio o unidad de inteligencia y a la persona objetivo de la operación, respectivamente.

Como se ha mencionado previamente, HUMINT virtual no implica necesariamente nuevos métodos, sino una adaptación adecuada de las herramientas tradicionales al ciberespacio (Dobák y Tóth, 2021). Mientras que las disciplinas de OSINT y SOCMINT implican adquirir de manera pasiva datos sobre individuos y/u otros objetivos, HUMINT requiere interactuar de manera directa (en persona o virtualmente) con una fuente humana (Giannetakis et al., 2020). Por lo tanto, HUMINT *online* no solo requiere la creación de una cuenta con una identidad falsa en RRSS, sino que esta cuenta debe ser empleada para establecer contacto con la persona objetivo (Erdész, 2018), lo que implica nuevas dinámicas y retos a los que no se enfrentaría un analista que solo haga uso de SOCMINT.

La aplicación de técnicas de HUMINT tradicionales a su versión *online* no solo es posible, sino que también conlleva ciertas ventajas, en tanto que reduce el riesgo del agente y permite el acceso a grupos sociales a los que resultaría difícil llegar cara a cara (Koren, 2015). Asimismo, los jóvenes conocidos como "nativos digitales" pueden tener una mayor habilidad en la aplicación de HUMINT en el ciberespacio, lo que parece ser debido a, entre otras razones, sus patrones de pensamiento adaptados al mundo *online* (Sano, 2015). No obstante, al tratarse de una disciplina relativamente novedosa, las vulnerabilidades humanas explotadas tradicionalmente en HUMINT pueden no ser aplicables a técnicas *online* (Sánchez Margolles, 2022). De la misma manera, las habilidades requeridas para un agente HUMINT cara a cara difieren de las necesarias para llevar a cabo una operación *online* exitosamente, debido a las diferencias entre relaciones virtuales y *offline* (Koren, 2015).

3.1.3. Ingeniería social

La ingeniería social es el acto de, por medio de un conjunto de técnicas y métodos basados en la influencia, manipular a una persona con el objetivo de obtener información confidencial, acceso a sistemas de seguridad, o la propagación de programas de *malware* (Hadnagy, 2010; Mitnick y Simon, 2002). En ocasiones se hace referencia también a la ingeniería social inversa, cuya única diferencia es que es la víctima la que inicia el contacto con el atacante tras haber sido influida por el mismo para que lleve a cabo esta acción, dando lugar a una mayor confianza con el atacante (Koren, 2015).

La ingeniería social comparte ciertas características con HUMINT virtual, ya que explota las vulnerabilidades de un ser humano, especialmente las psicológicas, para obtener información privilegiada. Los ataques sociales pueden ser tanto directos (interactuando directamente con la fuente, en persona o por teléfono) o indirectos (por ejemplo, haciendo *phishing*) (Tóth, 2020). Además, en ingeniería social también se realiza una diferenciación de roles similar a la empleada en HUMINT, excepto porque al agente u operativo de HUMINT se le aplica el término "atacante" y a la fuente se le llama "víctima". Este matiz de diferencias entre los nombres de roles de ambas disciplinas pone en evidencia

la principal diferencia entre ambas, y es que el concepto de ingeniería social tiene una explícita connotación ilegal, cosa que no ocurre con HUMINT. Sin embargo, esta no es la única disparidad entre ambas disciplinas. La ingeniería social ha sido principalmente estudiada desde la ingeniería, debido a la relevancia del aspecto tecnológico en los ataques sociales (aunque estos pueden ser llevados a cabo empleando diferentes medios, ya sean *online*, presencialmente, por teléfono, etc.), mientras que la inteligencia de fuentes humanas tiende a poner el foco en el aspecto humano, más que en el tecnológico. Al margen de las diferencias entre ambas, no se puede hablar de HUMINT virtual sin tener en cuenta la ingeniería social. La inteligencia de fuentes humanas podría ser considerada como una forma de obtención legal de información privilegiada por medio de un *insider*, término empleado en ingeniería social para hacer referencia a una persona en posesión de información corporativa que emplea para obtener beneficios personales (Huerta, 2001).

3.1.4. Fases de HUMINT virtual

Debido a la naturaleza clasificada de las operaciones HUMINT se dispone de una cantidad reducida de estudios que traten este tipo de inteligencia, por lo que la documentación en abierto sobre los procedimientos y fases de esta es limitada. De aquellos estudios en los que se presenta una propuesta de fases, ninguno de ellos trata específicamente las operaciones de elicitación *online*, centrándose en cambio en interrogatorios o reclutamiento de activos cara a cara (Army, 2006). No obstante, también se dispone de propuestas de fases de ingeniería social que pueden ser adaptadas para su uso en HUMINT virtual.

Por un lado, varios autores han formulado diferentes ciclos para explicar el proceso de HUMINT de entre cuatro y siete fases. En este informe ha sido escogido como referencia el ciclo empleado por Dorado Roldán (2019), puesto que es el que más se adecúa a los objetivos planteados. Dicho ciclo fue obtenido de una combinación de varias fuentes (Army, 2006; Zunzarren, 2014) y se compone de siete fases que serán explicadas en detalle en el siguiente apartado: orientación de la operación, *screening*, planificación y preparación, aproximación, elicitación, salida y *debriefing*. Aunque otros autores han realizado otras propuestas de fases, estas pueden ser incluidas en su mayoría dentro de este ciclo. Por ejemplo, Lowenthal (2011) sugiere que la adquisición de una fuente HUMINT se puede dividir en cuatro fases: identificación de la fuente potencial (equivalente a la fase de *screening*), desarrollo de la colaboración (que incluiría aproximación y elicitación), reclutamiento (no aplicable a las operaciones de elicitación) y despido (análoga a la fase de salida). Otros autores, en cambio, sugieren que la mayoría de los investigadores sobre HUMINT utilizan alguna variación de los siguientes seis pasos: detección (*screening* de la fuente), evaluación (*screening* y planificación de la operación), desarrollo (incluiría principalmente aproximación, pero también elicitación), reclutamiento (no aplicable en operaciones de elicitación), manejo (podría incluirse en elicitación) y validación (práctica no incluida explícitamente en la propuesta de Dorado Roldán, pero que en este estudio se integrará en la fase de *debriefing*) (Giannetakis et al., 2020; Koren, 2015).

Por otro lado, las fases establecidas en los procesos de ingeniería social por Mitnick y Simon (2002) también resultan altamente similares: investigación sobre la persona objetivo (*screening*), desarrollo de la confianza (aproximación), explotación de la confianza (elicitación) y el uso de la información obtenida (en inteligencia este paso estaría localizado en otra fase del ciclo, no necesariamente en obtención de información). Steinmetz et al. (2021), en cambio, incluyen en su propuesta de fases de ataques sociales la evaluación de las habilidades del operador y el momento de la operación (que han sido incluidas en la fase de planificación), y la ocultación (refiriéndose a las medidas para evitar las sospechas de la víctima, y que serán incluidas en la fase de salida).

En definitiva, se han propuesto diferentes fases dentro del ciclo de obtención de información de una fuente humana en HUMINT e ingeniería social que, debido a las similitudes explicadas anteriormente entre ambas disciplinas, pueden ser agrupadas o incluidas dentro del ciclo empleado por

Dorado Roldán (2019). En el siguiente apartado se explican las herramientas y procesos psicológicos que pueden ser empleados en cada una de las fases de HUMINT virtual.

3.2. Aportaciones de la psicología a HUMINT virtual

Al tratarse de un componente intrínseco de la naturaleza humana, la psicología está presente en todas las interacciones y relaciones personales. Por limitaciones de tiempo y espacio, en este estudio se tratarán únicamente los procesos psicológicos que se han considerado como relevantes en los contactos *online* entre agente y fuente. Las herramientas que se exponen a continuación no resultan excluyentes entre sí, ni son necesariamente las únicas disponibles, ya que en función de la operación se deberá tener en cuenta otras disciplinas y técnicas.

Con objeto de ordenar y facilitar la comprensión de los conceptos y su empleo, cada herramienta de la psicología se ha incluido en la fase de HUMINT más apropiada, lo que no implica necesariamente que no pueda ser empleada en otras partes del ciclo. Por último, debido a los requisitos y recursos diferentes en cada operación, los conceptos y su uso serán descritos someramente para facilitar su adaptación a cualquier misión HUMINT que así lo requiera.

3.2.1. Orientación de la operación

La fase de orientación de la operación consiste en la clarificación y operativización de objetivos (Zamorano et al., 2023). De la misma manera, es en esta etapa donde se realiza la consideración inicial del riesgo del operativo teniendo en cuenta que, siendo cierto que las amenazas a las que se ve expuesto el agente son menores al tratarse de una operación "*online*" (Koren, 2015), nunca es cero. Puesto que esta fase tiene como fin el esclarecimiento de los objetivos, y todavía no se ha escogido una fuente y un agente, no se han encontrado investigaciones previas en las que se estudien procesos psicológicos de utilidad alineados con el propósito de este informe.

3.2.2. Screening

Una vez han sido dilucidados los objetivos, se procede al mapeo y selección de las fuentes humanas. Para ello, se estudia qué fuentes potenciales tienen acceso a la información que se pretende obtener y su idoneidad en función de la cercanía con el recolector, el grado de disposición a colaborar y el riesgo de que el agente sea descubierto (Zamorano et al., 2023). Koren (2015) diferencia dos dimensiones de la posibilidad de acceso a la información: la posición, es decir, que la fuente esté localizada geográficamente en el área donde suponemos que se encuentra la información, y acceso propiamente dicho o, en otras palabras, la pertenencia a la organización o grupo que dispone de esa información. En HUMINT virtual la posición no cobra tanta importancia como el acceso debido a la conectividad de regiones geográficamente distantes, por lo que será la pertenencia al grupo *target* lo que defina, en estas operaciones, la idoneidad de la fuente.

Por otro lado, cuando se haya escogido un perfil de redes sociales como fuente, el operativo de inteligencia tiene que esclarecer si se trata de un perfil hostil o no hostil y cuántas personas hay detrás de esa cuenta (Seisdedos, 2023). Un análisis lingüístico, de las horas de publicación y de los dispositivos empleados son técnicas empleadas para discernir cuántas personas reales hay detrás de este perfil (Seisdedos, 2023).

Tras haber esclarecido qué personas cumplen los criterios establecidos, se procede a un perfilado de la personalidad y de los sistemas motivacionales de las potenciales fuentes, lo que permitirá al operativo discernir las vulnerabilidades de la persona objetivo y aportará información clave para la planificación de las siguientes fases.

3.2.2.1. *Perfilado de personalidad*

Aunque son múltiples los autores que hacen referencia a la importancia de la obtención de perfiles para su explotación en operaciones HUMINT (Dhami, 2011; Lowenthal, 2011), son pocas las referencias disponibles que expliquen cómo hacerlo. En aquellos estudios sobre HUMINT donde se trata este tema, se tiende a utilizar el modelo PEN de Eysenck (1970), debido principalmente a que este se compone únicamente de 3 rasgos cuya combinación da lugar a únicamente ocho perfiles. Además, este modelo es considerado por algunos autores como el mejor disponible para realizar perfiles (Sánchez-Muñoz et al., 2018).

Para obtener indicadores indirectos del perfil de la fuente, se emplearán tanto OSINT como SOCMINT (Dorado Roldán, 2019). El comportamiento en redes sociales, al igual que los perfiles, mensajes y vídeos disponibles en los que se observa el comportamiento de la fuente, resultan especialmente útiles (Yee et al., 2011). Sin embargo, en caso de ser posible, también es recomendable la obtención de indicadores mediante la observación en contextos reales.

El modelo PEN de Eysenck (1970) se compone de tres rasgos de personalidad principales: extraversión, neuroticismo y psicoticismo. Las personas altas en psicoticismo se asocian con un mayor desapego emocional, agresividad, menor empatía y menor miedo. Por otro lado, las puntuaciones altas en alta extraversión según el modelo PEN se caracterizan por ser activas, enérgicas, sociables y en busca de nuevas sensaciones. Finalmente, las puntuaciones altas en neuroticismo implican mayor nerviosismo, ansiedad, hipersensibilidad emocional y cambios de humor frecuentes. Es importante destacar que el neuroticismo actúa como un amplificador de los otros dos rasgos, intensificando sus efectos. De la combinación de estos tres rasgos (en función de si las puntuaciones de cada 1 de ellos son consideradas altas, por encima del centil cincuenta, o bajas, por debajo de este centil) se obtienen un total de 8 perfiles. El objetivo del perfilado en el *screening* es comprender con qué perfil se corresponde la fuente escogida o potencial para, posteriormente, diseñar un intento persuasivo *online* adaptado a su personalidad (Rodríguez y Sánchez, 2023), teniendo en cuenta las vulnerabilidades y los riesgos derivados de la combinación de rasgos de la persona objetivo.

A pesar de que la mayoría de las vulnerabilidades derivadas de la personalidad que se pueden observar en contextos cara a cara pueden ser aplicadas también a contextos virtuales, se han observado ciertos matices con respecto a la vulnerabilidad persuasiva *online* y *offline*. En concreto, aunque generalmente parece que las puntuaciones altas en el rasgo de neuroticismo implican una mayor susceptibilidad a la persuasión, una revisión reciente sobre la literatura acerca de la vulnerabilidad a ingeniería social *online* señaló que la baja ansiedad de los individuos con bajo neuroticismo implicaría una mayor vulnerabilidad a los ataques sociales, mientras que la ansiedad de las personas altas en neuroticismo sería un factor de protección (Sánchez Margolles, 2022).

En caso de poder elegir entre varias fuentes potenciales, el perfilado permite comprender cuál de ellas sería la más vulnerable en un intento persuasivo en la operación HUMINT virtual. En la revisión bibliográfica previamente mencionada, se concluye que el perfil más vulnerable a intentos de ingeniería social *online* (que, como ya se ha explicado, están altamente relacionados con la obtención de fuentes humanas para inteligencia) es el de una persona con bajo neuroticismo y alta extraversión, combinados con altos niveles en la dimensión de impulsividad del psicoticismo y bajos niveles en la dimensión de agresividad (Sánchez Margolles, 2022).

3.2.2.2. *Perfil motivacional*

El modelo psicológico más empleado para hablar de motivación en operaciones HUMINT es el modelo de Gray (1981), relacionado con el modelo PEN de Eysenck. Gray propuso tres sistemas motivacionales de la personalidad basados en fundamentos biológicos de los rasgos del PEN: el Sistema de

Activación Conductual (BAS), el Sistema de Inhibición Conductual (BIS) y el sistema de Ataque-Huida (FFS). El BAS, vinculado con altos niveles de extraversión neurótica, se activa en respuesta a señales de recompensa, promoviendo respuestas de acercamiento. Por otro lado, el BIS responde a señales de castigo, inhibiendo la actividad. Un BIS hiperactivo se ha relacionado con introversión neurótica (baja extraversión y alto neuroticismo). Por último, la infra activación del sistema FFS, que ha sido asociada al rasgo de psicoticismo, puede generar respuestas de agresividad e impulsividad. Conocer el perfil motivacional y de personalidad de la fuente permite la posterior planificación de la aproximación y la elicitación.

Además del perfil motivacional en función del modelo de Gray, también resulta beneficioso conocer cuáles son las motivaciones de la persona objetivo para estar presente en redes sociales (Koren, 2015). Conocer las razones por las que una persona está presente en internet también expone sus vulnerabilidades y permite a los servicios de inteligencia explotarlas. Pai y Arnott (2012) proponen que las redes sociales ofrecen a las personas la posibilidad de reciprocidad, de una mejora en la autoestima, de una forma de sentir que pertenecen a algo o de satisfacer su hedonismo. Otro de los motivos más comunes para estar presente en internet es buscar una pareja sentimental, ya que las relaciones *online* permiten explorar fantasías de manera más abierta y con menos riesgo (Jones, 2010), facilitando la posibilidad de que aquellas personas que sufran ciertas dificultades para desarrollar su intimidad en persona puedan establecer una relación (Jones, 2010) sin tener que invertir mucho económica o emocionalmente (Jones, 2010). Conocer estas razones personales también permite al operativo generar una serie de pretextos que se adecúen a ellas, con la finalidad de iniciar y mantener una relación lo más natural posible con la fuente. Por ejemplo, si el objetivo emplea a redes sociales únicamente con motivos laborales, la aproximación podría orientarse en función de estos motivos, por ejemplo, planificando un contacto relacionado con el trabajo de la fuente.

3.2.3. Planificación y preparación

Una vez que se haya seleccionado una fuente, será necesario planificar las particularidades de la operación. En este sentido, es importante haber obtenido el conocimiento necesario acerca de las características y vulnerabilidades de nuestro objetivo durante la fase de *screening* (Steinmetz et al., 2021), para así llevar a cabo la distribución de recursos, establecer el eje de acercamiento y desarrollar una estrategia de abordaje adecuada (Zamorano et al., 2023).

Durante esta tercera fase, se planifica lo máximo posible tanto de la aproximación como de la elicitación, incluyendo a su vez la selección del agente o agentes que llevarán a cabo el contacto y el diseño de la identidad falsa representada en redes sociales (Steinmetz et al., 2021). Además, se deberán tener en cuenta otros aspectos culturales y conductuales de la fuente para el establecimiento de pretextos y segundas identidades que faciliten la consecución de los objetivos de la operación.

3.2.3.1. *Selección del/a agente*

En un estudio reciente llevado a cabo por Macêdo et al. (2023), se destaca que los agentes de inteligencia son el foco principal de las operaciones de obtención de información de fuentes humanas. En este sentido, es crucial evaluar las habilidades de las que disponen los agentes, así como el entrenamiento técnico y la experiencia previa. No todos los operativos son capaces de llevar a cabo esta tarea, ya que se requiere una base de habilidades básicas que exigen aptitudes para las relaciones humanas, siendo capaces de interactuar de manera natural, estimulando a sus receptores y dirigiendo adecuadamente la conversación para que hablen sobre los temas deseados (Giannetakis et al., 2020).

Un operativo eficiente requiere un conjunto de habilidades básicas que exigen una alta disposición hacia las relaciones interpersonales y la capacidad de dirigir adecuadamente las conversaciones

sobre temas relevantes. Específicamente, los agentes requieren un adecuado entrenamiento en habilidades sociales (Giannetakis et al., 2020; Johnson, 2010). Las habilidades sociales no se refieren a un rasgo o capacidad innata de algunos individuos, sino a "un patrón de conductas específicas en situaciones sociales concretas" (Méndez Carrillo et al., 2014, p. 339). Es decir, pueden ser entrenadas y, de hecho, este entrenamiento está bastante investigado para aplicaciones de psicología clínica.

Por otro lado, el agente debe disponer de otras características psicológicas. A lo largo de la literatura, se han considerado diversas variables como especialmente relevantes en la selección de los agentes, resaltando la capacidad para abordar problemas de naturaleza diversa en contextos heterogéneos (Giannetakis et al., 2020). Esta capacidad está relacionada con la inteligencia humana, que puede ser operativizada como factor g (Colom Marañon, 2018). La medición de la inteligencia de los agentes previa a su selección es una medida que no ha sido muy estudiada en las publicaciones encontradas en abierto, pero que debe ser considerada en la fase de planificación.

Finalmente, el perfilado de personalidad y motivacional también es una herramienta relevante al escoger el agente que va a llevar a cabo la operación. Algunos autores afirman que la personalidad del agente desempeña un papel igual de decisivo que la de la fuente, destacando que los perfiles más adecuados para el trabajo de un operativo están caracterizados por la extraversión y la estabilidad emocional o bajo neuroticismo (Russano et al., 2014a; Russano et al., 2014b).

3.2.3.2. *Diseño de la segunda identidad y pretexto*

El diseño de una segunda identidad es un aspecto esencial en las operaciones HUMINT para ocultar el verdadero propósito de la interacción y para proteger la verdadera la identidad del agente, reduciendo así el riesgo al que se enfrenta. Para ello, es de especial relevancia considerar tanto la personalidad que se desea crear para la identidad ficticia (Zamorano et al., 2023), como las huellas que van a ser liberadas en la web para respaldarla y la coherencia entre ambas.

Por un lado, la personalidad de la identidad ficticia deberá ser escogida teniendo en cuenta el perfil y las vulnerabilidades de la fuente. La combinación de rasgos representada en la segunda identidad puede, a su vez, ser empleada para representar con mayor facilidad uno u otro principio de Cialdini (2001). Cialdini formuló seis principios que describen las estrategias que pueden utilizarse para influir en el comportamiento de las personas: reciprocidad (la tendencia a devolver los favores y acciones positivas recibidas), autoridad (la predisposición a obedecer a personas que tienen un mayor estatus), escasez (la valoración aumentada de productos u oportunidades que son limitados), coherencia y compromiso (la inclinación a actuar de acuerdo con nuestras creencias y compromisos previos), simpatía (la disposición a aceptar las demandas de quien nos agrada o con quien nos sentimos conectados) y validación o sanción social (seguir el ejemplo de los demás o ajustarse a las normas sociales). Por ejemplo, si se quiere generar simpatía en la fuente, puede diseñarse una identidad con su mismo perfil de personalidad, generando simpatía por semejanza. Otro ejemplo sería el diseño de una identidad alta en psicoticismo que, con su conducta dominante, pudiera incentivar la percepción de autoridad ante una fuente con un psicoticismo bajo.

Por otro lado, las operaciones de HUMINT virtual suelen ser de larga duración, en parte porque en promedio la creación y publicación de contenidos para redes sociales lo más auténticos posibles lleva varios meses antes de poder hacer uso de un perfil activo sin despertar sospechas de la fuente. Durante este período, se deben alimentar los perfiles sociales con todo el material necesario para que reflejen la historia de cobertura o pretexto. El pretexto escogido no solo tiene que ser coherente con la personalidad de la segunda identidad, sino que tiene que poder mantenerse durante el tiempo que dure la operación (Steinmetz et al., 2021).

3.2.3.3. *Factores culturales*

La importancia de los factores culturales en las operaciones HUMINT es evidente en varios aspectos. El agente no solo debe poder hablar el idioma de la fuente, sino también saber adaptarse a los códigos de comportamiento y las reglas de comunicación de su cultura en particular (Dhami, 2011). Además, al planificar operaciones HUMINT *online*, el personal de inteligencia debe evitar el etnocentrismo, ya que en caso de no hacerlo se podrían cometer fallos que dificulten la consecución de los objetivos. Por ejemplo, los procesos de atribución difieren entre culturas colectivistas e individualistas. En las culturas colectivistas, es más probable que se atribuya el comportamiento de una persona a causas situacionales en lugar de disposicionales o de personalidad, lo que resulta en una menor vulnerabilidad de las fuentes de origen oriental a la creación de disonancias por parte de los agentes HUMINT (Nagayama Hall y Barongan, 2002). Sin embargo, estas culturas muestran una mayor tendencia a la conformidad (Smith y Bond, 1998), lo que hace que sean más susceptibles al uso de este proceso como herramienta de aproximación o elicitación.

3.2.3.4. *Conducta en el mundo virtual*

Conocer las particularidades del comportamiento en contextos *online* es de gran valor al llevar a cabo la planificación de una operación HUMINT virtual (Dhami, 2011). Por ejemplo, Crandall et al. (2008) observaron que las personas tienden a conectarse más frecuentemente en redes sociales con aquellos perfiles de gente que consideran más similares a ellos, y suelen ser más fácilmente persuadidas por personas que les resultan familiares, especialmente vecinos o amigos (Hui y Buchegger, 2009).

El anonimato es otro factor que hay que considerar en la conducta virtual, ya que se ha observado que en contextos anónimos las personas son capaces de hacer cosas que no harían si su identidad fuera pública, llegando incluso a dejar de sentirse responsables por sus acciones (Oceja, 2021). Sin embargo, hay que destacar que los grupos *online* anónimos parecen ser más vulnerables la influencia (Postmes et al., 2001), especialmente al emplear mensajes asertivos y exagerados (Miller y Brunner, 2008). La asertividad es, de hecho, un tipo de conducta practicado en el entrenamiento de habilidades sociales y caracteriza a los "líderes *online*", personas con una marcada capacidad de generar respuestas de otros y con redes sociales expansivas y recíprocas, además de una membresía más prolongada en grupos *online* (Huffaker, 2010). La operación HUMINT podría verse beneficiada del uso de una identidad de "líder *online*" y de la selección de un agente que pueda representar sus características.

Por último, se han observado diferencias de género en las relaciones sociales *online*. De acuerdo con Lee (2005), la confianza expresada verbalmente resulta más efectiva en mujeres. Sin embargo, los resultados de estudios sobre influencia *online* a grandes rasgos no deben ser aplicados de la misma manera en todas las operaciones, ya que cada fuente presenta unas características y vulnerabilidades únicas que deben ser consideradas para garantizar la obtención de la información deseada.

3.2.4. Aproximación

Tras haber diseñado las características básicas de la operación, se inicia el primer intento de aproximación virtual con la fuente. El objetivo principal de la etapa de aproximación es el de establecer el *rapport* (la relación de confianza) con la persona objetivo (Army, 2006), manipulando las interacciones sociales para así construir una relación que posteriormente facilite la obtención de información requerida (Dorado Roldán, 2019; Gonzales, 2013; Steinmetz et al., 2021). Aunque la obtención de confianza es común a todas las operaciones HUMINT, la forma de conseguirla será diferente para cada fuente en función de sus características y vulnerabilidades. Se han propuesto diferentes técnicas que pueden ser empleadas para conseguir los objetivos de esta fase, siendo la persuasión personalizada o *matching* la más estudiada.

Adicionalmente, se incluirá una somera descripción de otras posibles herramientas derivadas de la psicología que resultan de utilidad en esta fase.

3.2.4.1. *Confianza y Desconfianza*

Aunque se suelen entender como los dos extremos de un mismo espectro, se ha observado que la confianza y la desconfianza son dos variables diferentes pero relacionadas entre sí (Dhami, 2011). Las interacciones pueden despertar desconfianza o reducir la confianza, por lo que el agente de inteligencia debe no solo conseguir que su objetivo confíe en él sino también evitar llevar a cabo acciones que generen desconfianza. Reducir la incertidumbre y el riesgo percibido por la persona objetivo serviría tanto para evitar la desconfianza como para aumentar la confianza de esta (Dhami, 2011).

El concepto de desconfianza implica una percepción de intencionalidad nociva y está caracterizado por niveles de miedo, escepticismo, cinismo, vigilancia y control (Dhami, 2011). Además, sesgos como el error de atribución, las percepciones de los valores e intenciones de la otra persona y su supuesta pertenencia a un grupo (Dhami, 2011) son otras variables manipulables por el operativo que facilitan la reducción de desconfianza.

Por otro lado, u conocimiento profundo de la fuente, la muestra de empatía y respeto y el uso de escucha activa resultan de gran ayuda al establecer el *rapport* (Alison y Alison, 2017; Alison et al., 2013; Redlich et al., 2015). Aunque es uno de los factores más determinantes del éxito de una operación con fuentes humanas, por sí sola la confianza no garantiza la obtención de la información deseada (Marin y Gabbert, 2022), por lo que es necesario considerar otras herramientas, como el *matching,* que faciliten el posterior desarrollo adecuado de la fase de elicitación (Rodríguez y Sánchez, 2023). Koren (2015) sugiere que aplicar técnicas de ingeniería social inversa, que implican que la víctima sea la que inicie el contacto, puede generar mayores niveles de confianza.

Otra de las técnicas más empleadas para que la fuente empiece a confiar en el agente es el *self disclosure* o la revelación de información personal (Dorado Roldán, 2019), especialmente si se tratan temas que generen una sensación de semejanza. El *self disclosure* puede ser explicado por el principio de Cialdini de reciprocidad (2001), y es uno de los principales pasos para el desarrollo de una relación (Dhami, 2011). Se han observado diferencias de género en la revelación de información personal, ya que las mujeres tienden a hablar más de sí mismas que los hombres (Dhami, 2011).

3.2.4.2. *Persuasión personalizada*

La persuasión se refiere a la comunicación dirigida a cambiar las actitudes de un receptor mediante la transmisión de un mensaje específico (Blanco et al., 2017). En contextos de HUMINT, la persuasión es empleada para generar confianza, a la vez que la confianza facilita la persuasión y la posterior obtención de información. La persuasión personalizada, es decir, adaptada al receptor, se conoce como *tailoring* o *matching* personalizado (Hawkins et al., 2008; Teeny et al., 2020; Webb et al., 2013). El *tailoring* resulta una herramienta útil debido a que se ha observado que, por norma general, los mensajes resultan más persuasivos cuando son congruentes con las características y necesidades del receptor (Hirsh et al., 2012). Aunque el *matching* se puede realizar adaptando otras variables de la comunicación (como el contexto o el emisor) al receptor (Teeny et al., 2020), al tratarse de operaciones exclusivamente virtuales, el contenido se centrará en el *tailoring* con el mensaje. Es importante tener en cuenta la elaboración del receptor según el Modelo de Probabilidad de Elaboración (Petty y Cacioppo, 1986) para determinar qué variables serán más apropiadas en función de los procesos persuasivos que desencadenen (Teeny et al., 2020). Sin embargo, debido a las limitaciones de este informe, no se podrá desarrollar en detalle la complejidad de las interacciones entre variables y procesos persuasivos en función de la probabilidad de elaboración, aunque su estudio representa una de las principales líneas futuras de investigación.

En la fase de aproximación a la fuente, el *tailoring* se utiliza para generar o cambiar la actitud del receptor hacia el agente de inteligencia y fomentar la confianza (Rodríguez y Sánchez, 2023). Las variables más comunes a las que se adapta el mensaje persuasivo en esta fase incluyen, por un lado, factores perceptivos, emocionales y cognitivos, como el foco atencional preferente (PALIO: personas, acciones, lugares, información u objetos), el registro sensorial dominante (VAKO: visual, auditivo, kinestésico y olfativo) y el tamaño de procesamiento de la información (Zunzarren, 2014). Ajustar el discurso a estos factores generaría en el receptor una sensación de semejanza con el agente, fomentando la simpatía hacia él.

Otras variables estudiadas en este contexto son la necesidad de cierre cognitivo, la necesidad de cognición y el *self monitoring*. La primera se refiere a la motivación del receptor por evitar la ambigüedad y buscar respuestas definitivas (Blanco et al., 2017); para los individuos con niveles bajos en esta necesidad resulta persuasiva la repetición del mensaje, mientras que con aquellos con niveles altos será más efectivo el uso de la vía central y la variable *expertise* (Petty y Briñol, 2012). Por otro lado, la necesidad de cognición, el grado en el que las personas disfrutan pensando (Cacioppo y Petty, 1982), también puede ser explotada a través del *matching*. Presentar ideas como opciones atractivas para aquellos a quienes les gusta pensar mucho es una estrategia que, en concreto, resulta efectiva con aquellos que tienen una alta necesidad de cognición (Bakker, 1999; See et al., 2009). Finalmente, las personas con alto *self monitoring* presentan una tendencia a adaptar su comportamiento al entorno social (Teeny et al., 2020) y pueden ser más persuadidos por mensajes que resalten los beneficios sociales (DeBono, 1987; Lennon et al., 1988; Paek et al., 2012) y por la variable de validación social (Rodríguez y Sánchez, 2023). Sin embargo, las fuentes que presenten menor *self monitoring* pueden ser más persuadidas por argumentos relacionados con el rendimiento del objeto (DeBono, 1987; Lennon et al., 1988; Paek et al., 2012).

Las emociones también son objeto de *tailoring*, ya que pueden aumentar la capacidad persuasiva de los mensajes cuando se utilizan adecuadamente. Se puede adaptar el contenido emocional del mensaje al estado de ánimo del receptor, ya sea teniendo en cuenta la valencia general de la emoción (Cho y Choi, 2010; Wegener et al., 1994), utilizando una emoción específica que se ajuste a la situación (DeSteno et al., 2004; Griskevicius et al., 2009) o adaptando el mensaje para que sea equivalente a la base (emocional o cognitiva) de la actitud del receptor (Edwards, 1990; Fabrigar y Petty, 1999). Asimismo, el *arousal* o activación emocional del receptor también debe ser considerado, seleccionando un mensaje con un *arousal* alto para aquellos que presenten una alta activación emocional (Di Muro y Murray, 2012; Rucker y Petty, 2004; Yan et al., 2016).

3.2.4.3. *Psicología de las relaciones*

Para el correcto desarrollo de la operación, es fundamental desarrollar una relación natural que pueda mantenerse exclusivamente en el ámbito digital (Koren, 2015; Macêdo et al., 2023). Hay que destacar que, aunque las relaciones cara a cara suelen implicar una mayor intimidad (Scott et al., 2006), se ha observado que las relaciones virtuales pueden experimentar vínculos igual de fuertes que las presenciales (Grieve et al., 2013; Peris et al., 2002). En otras palabras, las relaciones exclusivamente *online* son posibles y permiten conseguir vínculos semejantes a los *offline*, pero los operativos deben considerar las diferencias entre ambas y anticiparse a los posibles problemas específicos de las relaciones virtuales. Por ejemplo, en los contactos *online*, la proximidad física se sustituye por factores como la familiaridad, la similitud (demográfica y psicológica) y la atracción física (Dhami, 2011). Estas variables pueden ser manipuladas de antemano durante la creación de la segunda identidad y la aproximación progresiva a la fuente.

La teoría de la Penetración Social (SPT) y la Teoría de la Reducción de la Incertidumbre (TRI) son modelos comunes empleados en inteligencia para comprender las relaciones virtuales (Koren, 2015). La SPT, propuesta por Altman y Taylor en 1973, sostiene que las interacciones se inician en función de un análisis del coste-beneficio de revelar información y que las relaciones derivadas de ellas

se desarrollan a medida que se lleva a cabo un intercambio gradual de información. La TRI (Berger, 1986), en cambio, argumenta que la capacidad de predecir el comportamiento del otro contribuye al desarrollo de la relación, gracias a la simpatía generada por la reducción de incertidumbre (Berger, 1986). En consecuencia, de la aplicación de ambas teorías se deduce que, en la aproximación a la fuente, el agente puede reducir la incertidumbre de su objetivo como medio para inclinar la balanza del análisis coste-beneficio, y así fomentar la simpatía, la confianza y el revelado de información clave.

3.2.4.4. *Otras técnicas*

Son muchas las características y factores que hay que tener en cuenta en la aproximación a una fuente, por lo que resultaría imposible desarrollarlas todas en detalle en este informe. Por ejemplo, las fuentes humanas tienden a confiar más en los agentes de inteligencia que demuestran conocimientos y competencia en el campo relevante. Sin embargo, el *expertise* es una variable cuyo efecto persuasivo depende de la elaboración del receptor, pudiendo dar lugar a uno u otro proceso psicológico (Blanco et al., 2017). En otras palabras, en HUMINT hay que tener muy presentes los procesos persuasivos que pretendemos generar y su efecto en el objetivo de la operación.

Por otro lado, según el sistema motivacional dominante (BIS o BAS), las personas son más vulnerables a castigos o refuerzos. Las fuentes extravertidas con neuroticismo alto serán más susceptibles a los refuerzos, mientras que los individuos con una combinación de introversión y neuroticismo serán más fácilmente influidos por una expectativa de castigo (Zamorano et al., 2023). El agente puede hacer uso de aquello que sea más útil para obtener el interés de la otra persona o mantener la relación a futuro.

Adicionalmente, los agentes que lleven a cabo la operación se verían beneficiados del conocimiento de sesgos cognitivos. Por ejemplo, realizar peticiones pequeñas e ir aumentando poco a poco el coste de estas generará un sesgo de aumento de compromiso en la fuente, dificultando que se niegue a cumplir las peticiones que le haga el agente.

Por último, las variables psicosociales como la identidad social, las bases morales y políticas y las tendencias culturales también son de especial utilidad (Cavazza et al., 2010; Feinberg y Willer, 2015; Fleming y Petty, 2000; Forehand et al., 2002; Laustsen, 2017; Lavine y Snyder, 2000; Luttrell et al., 2019; Meyers-Levy y Sternthal, 1991; Whillans et al., 2017; Wolsko et al., 2016). Mostrar en el perfil de la segunda identidad la pertenencia a un grupo común con la fuente, ya sea de género, etnia, nivel socioeconómico u orientación política fomenta la percepción de endogrupo con el agente, fomentando una actitud positiva hacia él y aumentando la confianza.

3.2.5. Elicitación

Una vez se ha establecido la confianza con la fuente, el siguiente paso es la obtención de la información necesaria para lograr los objetivos de la operación. Durante la elicitación, se busca emplear la actitud favorable de la fuente hacia el agente para obtener la información deseada sin recurrir a amenazas o coacción (Steinmetz et al., 2021). Algunos autores afirman que esto implica solicitar ayuda u ofrecer incentivos a la fuente, para lo que resulta especialmente importante conocer las posibles motivaciones de la persona objetivo para revelar información (Steinmetz et al., 2021). Algunas de las razones más comunes observadas en operaciones de elicitación con fuentes no hostiles son: la rivalidad con el grupo del cual se desea obtener información, diferencias religiosas o patriotismo (Johnson, 2010; Shepherd, 2009) y la necesidad de prestar ayuda (Noble, 2009).

En este contexto, la psicología puede desempeñar un papel relevante mediante la utilización de técnicas que aprovechen las vulnerabilidades individuales y procesos psicosociales como la conformidad y la obediencia. Durante toda la fase es de vital importancia evitar que la fuente se dé cuenta de que está siendo manipulada, ya que el agente de inteligencia correría un alto riesgo de comprometer la operación. En el caso de perfiles caracterizados por su naturaleza suspicaz, como los altos en psicoticismo, se debe tener especial precaución (Rodríguez y Sánchez, 2023). A menos que sea estrictamente necesario o no se disponga de otra opción, se desaconseja en general seleccionar como fuente a personas con un psicoticismo extremadamente alto debido a su desconfianza inherente y sus tendencias antisociales (Rodríguez y Sánchez, 2023).

Asimismo, durante toda la operación será de especial importancia detectar señales de riesgo de mentira para evaluar la veracidad de la información obtenida durante la fase de elicitación.

3.2.5.1. *Tailoring*

El uso de técnicas de persuasión personalizada basadas en las vulnerabilidades de la personalidad de la fuente se centra en aplicar el Modelo de Probabilidad de Elaboración (ELM) (Eysenck, 1970) y los principios de RASCALS o Cialdini (2001). Estos últimos se emplean como moderadores que aumentan la efectividad persuasiva de los mensajes (Rodríguez y Sánchez, 2023). El ELM, propuesto por Petty y Cacioppo (1986), explica cómo las personas procesan la información persuasiva. El ELM propone un continuo de elaboración en función del grado de pensamiento del receptor que determina qué procesos cognitivos se utilizan y la influencia persuasiva de las variables empleadas. En alta elaboración, el receptor está dispuesto a pensar y analizar en profundidad y la persuasión se da a través de la vía central. Por otro lado, en situaciones de baja elaboración, donde el receptor tiene poca disposición o capacidad para pensar, la persuasión se da a través de la vía periférica. En caso de encontrarse en un nivel medio de elaboración, las variables comunicativas pueden aumentar o reducir la elaboración del receptor.

A continuación (Tabla 1), se muestra un resumen de las principales vulnerabilidades de los diferentes perfiles de personalidad según el modelo PEN que pueden ser explotadas con objetivos de elicitación de información en inteligencia (Rodríguez y Sánchez, 2023).

Tabla 1: *Resumen de las estrategias persuasivas por perfiles (Rodríguez y Sánchez, 2023).*

Perfil	Principios de Cialdini	Variables del mensaje y ambiente	Elaboración y vía	Técnicas operantes sugeridas en el escenario
Alta Extraversión, Alto Neuroticismo, Alto Psicoticismo	Coherencia y compromiso, escasez, simpatía.	Ambiente estético y estimulante, urgencia temporal, alto riesgo-alto beneficio, tendencias de aproximación, componente social, búsqueda de sensaciones, orientación de dominancia, beneficios personales, poco esfuerzo, propuestas originales e innovadoras, curiosidad.	Baja elaboración, vía periférica.	Refuerzo positivo. Aproximación.
Alta Extraversión, Alto Neuroticismo, Bajo Psicoticismo	Todos.	Ambiente estético y estimulante, urgencia temporal, tendencias de aproximación, componente social, búsqueda de sensaciones, propuestas originales e innovadoras, curiosidad, subrayar normas, contenidos amenazantes,	Baja elaboración, vía periférica.	Refuerzo negativo (se puede complementar con un refuerzo positivo). Escape.

		apelar a la culpabilidad, suscitar empatía y familiaridad en la fuente, ambiente poco estimulante y adoptar una postura asertiva e intimidante para generar incomodidad.		
Alta Extraversión, Bajo Neuroticismo, Alto Psicoticismo	Coherencia y compromiso, simpatía y escasez.	Ambiente estético y estimulante, urgencia temporal, alto riesgo-alto beneficio, tendencias de aproximación, componente social, búsqueda de sensaciones, orientación de dominancia, beneficios personales, poco esfuerzo, propuestas originales e innovadoras, curiosidad, autoestima alta, argumentos sólidos y racionales.	Depende.	Ninguna, pero los refuerzos serían eficaces.
Alta Extraversión, Bajo Neuroticismo, Bajo Psicoticismo	Reciprocidad, coherencia y compromiso y simpatía.	Mensajes sociales, apelar a la bondad de la persona, suscitar empatía y familiaridad, ambiente estimulante (pero no excesivo), postura asertiva e intimidante para incomodar, apelar a normas.	Depende.	Ninguna, pero los refuerzos serían eficaces.
Baja Extraversión, Alto Neuroticismo, Alto Psicoticismo	Coherencia y compromiso, escasez, y simpatía.	Mensajes que apelen al control, que hagan referencia a tendencias de evitación, uso de mensajes con contenidos amenazantes, orientación a la dominancia, enfatizar sus beneficios personales, mensajes que con aspectos peligrosos, búsqueda de sensaciones, opciones que impliquen poco esfuerzo; mensajes con aspectos emocionales y ambiente estimulante para dificultar su procesamiento.	Baja elaboración, vía periférica.	Castigo y refuerzo negativo. Evitación.
Baja Extraversión, Alto Neuroticismo, Bajo Psicoticismo	Reciprocidad, coherencia y compromiso, validación social, autoridad, escasez.	Mensajes que apelen al control, a la culpabilidad, a tendencias de evitación, contenidos amenazantes, aspectos emocionales, subrayar normas, bajo riesgo- bajo beneficio, postura asertiva e intimidante, suscitar empatía, apelar a la bondad de la persona; ambiente estimulante para reducir elaboración.	Depende.	Castigo y refuerzo negativo. Evitación.
Baja Extraversión, Bajo Neuroticismo, Alto Psicoticismo	Ninguno es especialmente útil.	Argumentos sólidos y racionales no emocionales, orientación de dominancia, beneficios personales, búsqueda de sensaciones, opciones que impliquen poco esfuerzo, alta autoestima; ambiente estimulante para reducir rendimiento.	Alta elaboración, vía central.	Ninguno.

Baja Extraversión, Bajo Neuroticismo, Bajo Psicoticismo	Validación social, autoridad y simpatía.	Empatía, apelar a la bondad, mención de normas, autoestima alta; ambiente estimulante para dificultar rendimiento cognitivo.	Alta elaboración, vía central.	Ninguno, pero se podrían emplear castigos.

3.2.5.2. *Conformidad y obediencia*

La comprensión de los mecanismos de conformidad y obediencia permite a los profesionales de inteligencia aprovechar las normas y expectativas sociales para obtener información valiosa.

Por un lado, la conformidad se refiere a la tendencia de las personas a adaptarse a las normas y expectativas sociales aceptadas en un determinado entorno (Oceja, 2021). Los individuos pueden ser más propensos a proporcionar información si perciben que están cumpliendo con las expectativas establecidas por su grupo social. Esta influencia social, sumada a la necesidad de pertenencia y el temor al rechazo, pueden motivar a las fuentes humanas a conformarse y revelar la información solicitada. La conformidad, que es una forma indirecta de influencia social (Dhami, 2011), puede ser explicada por la necesidad de tener una representación precisa del mundo y ser aceptado por los demás (Dhami, 2011). La conformidad puede lograrse a través de diversas técnicas, como el uso de principios de Cialdini como reciprocidad, simpatía (mediante el halago o la atracción), validación social (destacando que otros también han cumplido) o escasez. A su vez, se puede hacer uso de otras tácticas derivadas de la aplicación de sesgos cognitivos, como la técnica del "pie en la puerta" (es decir, obtener conformidad ante una solicitud o asunto pequeño en primer lugar) y "puerta en la cara" (hacer una solicitud inicialmente exagerada o poco realista, con la expectativa de que sea rechazada para presentar una segunda solicitud más razonable, que era lo que se pretendía conseguir realmente) (Zunzarren, 2022). En general, las minorías tienden a conformarse a las mayorías, aunque también pueden influir en la mayoría al demostrar consistencia, independencia y similitud en una variedad de categorías sociales (Dhami, 2011).

La obediencia, por otro lado, se refiere a la disposición de las personas a cumplir con las órdenes de una autoridad, y puede ser explicada por factores como la difusión de responsabilidad, la percepción de la legitimidad y la socialización (Dhami, 2011). Es decir, mientras que la conformidad podría considerarse imitación, la obediencia está ligada a la jerarquía (Oceja, 2021). En operaciones HUMINT, la obediencia puede ser utilizada para obtener información valiosa que pueden estar bajo el control o la influencia de una organización o agencia. A través de la persuasión, mediante el establecimiento de relaciones de poder y el uso de incentivos o recompensas, las autoridades (reales o ficticias) pueden influir en las fuentes humanas para que proporcionen información relevante. Hay que destacar que la variable de *expertise* (empleada de acuerdo con los procesos persuasivos que se quieran desatar en función de la elaboración del receptor), la incertidumbre y la disonancia cognitiva son factores que favorecen la obediencia (Oceja, 2021) y que pueden ser manipuladas en beneficio de los operativos. En caso de pretender lo contrario, es decir, reducir la obediencia de la fuente, los estudios previos afirman que resulta de utilidad exponer a las personas a ejemplos de desobediencia, educar sobre las consecuencias adversas del cumplimiento y animarlas a cuestionar la autoridad (Dhami, 2011).

3.2.6. Salida

Una vez han sido dilucidados los objetivos, se procede al mapeo y selección de las fuentes humanas. Para ello, se estudia qué fuentes potenciales tienen acceso a la información que se pretende obtener y su idoneidad en función de la cercanía con el recolector, el grado de disposición a colaborar y el riesgo de que el agente sea descubierto (Zamorano et al., 2023). Koren (2015) diferencia dos dimensiones de la posibilidad de acceso a la información: la posición, es decir, que la fuente esté localizada geográficamente en el área donde suponemos que se encuentra la información, y acceso propiamente dicho o, en

otras palabras, la pertenencia a la organización o grupo que dispone de esa información. En HUMINT virtual la posición no cobra tanta importancia como el acceso debido a la conectividad de regiones geográficamente distantes, por lo que será la pertenencia al grupo *target* lo que defina, en estas operaciones, la idoneidad de la fuente.

Por otro lado, cuando se haya escogido un perfil de redes sociales como fuente, el operativo de inteligencia tiene que esclarecer si se trata de un perfil hostil o no hostil y cuántas personas hay detrás de esa cuenta (Seisdedos, 2023). Un análisis lingüístico, de las horas de publicación y de los dispositivos empleados son técnicas empleadas para discernir cuántas personas reales hay detrás de este perfil (Seisdedos, 2023).

Tras haber esclarecido qué personas cumplen los criterios establecidos, se procede a un perfilado de la personalidad y de los sistemas motivacionales de las potenciales fuentes, lo que permitirá al operativo discernir las vulnerabilidades de la persona objetivo y aportará información clave para la planificación de las siguientes fases.

3.2.6.1. *Debriefing*

Una vez obtenida la información deseada y tras haber conseguido una "salida" exitosa, en la última fase de *debriefing* se debe realizar un volcado de la información obtenida durante el contacto con la fuente (Zamorano et al., 2023). Por otro lado, tanto la información obtenida como la fuente de la que proviene deben ser validadas para evitar posibles errores que puedan comprometer la operación (Giannetakis et al., 2020). A pesar de que esta validación no suele incluirse ni en el ciclo de HUMINT ni en la propia fase de obtención de información, debido a su especial relevancia respecto a la información de fuentes humanas se ha considerado necesario mencionarla en esta última fase.

Por último, al igual que ocurre con la primera fase, los estudios publicados no hacen referencia a ninguna herramienta psicológica de especial relevancia en el *debriefing*. Sin embargo, en futuros estudios debería ser considerada la relación con los procesos cognitivos de memoria.

4. Discusión

Como se ha podido ver a lo largo de este estudio, el componente humano resulta de vital importancia en contextos de inteligencia y ciberseguridad. Los conocimientos y herramientas derivados de la psicología están intrínsecamente relacionados con HUMINT, aunque actualmente no se dispone de demasiados estudios que expongan cómo emplearlos en operaciones con fuentes humanas *online*, probablemente debido a la confidencialidad de este tipo de operaciones. Pese a que el alcance y la profundidad de este informe se han visto limitados por motivos temporales y de extensión, en él se han expuesto diversas maneras en las que las técnicas de ingeniería social y SOCMINT, combinadas con la psicología, pueden emplearse con objetivos de HUMINT *online*.

Dentro del ciclo de HUMINT, la investigación parece coincidir en la especial importancia del uso de la psicología en las fases de *screening*, aproximación y elicitación. Sin embargo, en un futuro se debería estudiar más a fondo la relación de los procesos de memoria y alteración de recuerdos con las fases de salida y *debriefing*. Los agentes de inteligencia que trabajen con operaciones de HUMINT virtual se verían beneficiados del uso de conocimientos sobre diferencias individuales, persuasión, técnicas de modificación conductual y procesos psicosociales.

4.1. Limitaciones

Cada operación presenta unas características únicas que deben ser consideradas. La psicología es una herramienta útil, pero no es la única que debe ser considerada al diseñar y ejecutar HUMINT virtual. Las expuestas aquí son solo herramientas que deben ser consideradas dentro de un conjunto más amplio de elementos y recursos de cada organización, incluyendo a su vez aspectos tecnológicos, legales y culturales, entre otros.

A nivel metodológico, hay que destacar como principales limitaciones la imposibilidad de acceso a publicaciones de carácter restringido y la escasez de estudios sobre el tema.

En contextos de obtención de información *online* que requieren interactuar con humanos, una de las principales limitaciones es el *self disclosure*, es decir, que la persona no quiera hablar de sí misma. Además, el anonimato en las redes sociales puede ser utilizado como una herramienta para engañar, y la identidad real de una persona no necesariamente coincide con la identidad que se muestra en línea, lo que dificulta la distinción entre la identidad real y las características exhibidas en línea. Otra posible limitación del HUMINT virtual es la falta de señales no verbales en la comunicación virtual. Sin embargo, este obstáculo ha sido compensado en parte por otros medios de comunicación, como los *emojis*. Aunque no se puede hacer uso de elementos como el tono de voz o el tiempo de respuesta para detectar mentiras o perfilar, los agentes de inteligencia pueden centrarse en otras características de la comunicación, como el análisis lingüístico o del mensaje, para suplir estas carencias.

4.2. Aplicaciones y futuras líneas de investigación

HUMINT virtual ofrece una perspectiva y una aplicación novedosa de las técnicas tradicionales de obtención de información de fuentes humanas a contextos *online*. Los hallazgos de este estudio son especialmente útiles en operaciones de inteligencia, pero también en ciberseguridad. De acuerdo con Chris Inglis, exdirector de National Counterintelligence and Security Center, "HUMINT es la Fuente más importante de inteligencia en ciberseguridad" (Öztürkci, 2023). El factor humano y el tecnológico no pueden ser separados, por lo que conocer qué vulnerabilidades pueden ser explotadas virtualmente ayuda a los profesionales de ciberseguridad tanto para protegerse de ataques de ingeniería social y otras ciberamenazas, como para diseñar estrategias de obtención de información. Además, las herramientas tecnológicas, por altamente efectivas que resulten, a veces pueden pasar por alto los matices que solo un analista o agente humano puede captar. La integración de capacidades humanas y herramientas tecnológicas puede mejorar significativamente la obtención y el procesamiento de información (Öztürkci, 2023).

En el futuro, a medida que las amenazas sean cada vez más complejas, el papel de la HUMINT se volverá aún más crítico, especialmente para comprender la psicología de los adversarios, anticipar sus movimientos y diseñar contramedidas efectivas. En definitiva, es una herramienta que permite a las agencias de inteligencia y empresas no solo a reaccionar ante las amenazas cibernéticas, sino también a adoptar una postura proactiva en su prevención.

5. Referencias

Alison, L., y Alison, E. (2017). Revenge versus rapport: Interrogation, terrorism and torture. *American Psychologist, 72*(3), 266-277. https://doi.org/10.1037/amp0000064

Alison, L. J., Alison, E., Noone, G., Elntib, S., y Christiansen, P. P. (2013). Why tough tac tics fail and rapport gets results: Observing rapport-based interpersonal techniques (ORBIT) to generate useful information from terrorists. *Psychology, Public Policy, and Law, 19*(4), 411-431. https://doi.org/10. 1037/a0034564

Altman, I., y Taylor, D. (1973). *Social penetration: The development of interpersonal relationships*. Holt.

Antonius, N. y Rich, L. (2013). Discovering collection and analysis techniques for social media to improve public safety. *The International Technology Management Review, 3*(1), 42-53. https://doi.org/10.2991/itmr.2013.3.1.4

Army, U. S. (2006). *Human Intelligence collector operations*. Headquarters Department of the Army. https://irp.fas.org/doddir/army/fm2-22-3.pdf

Bakker, A. B. (1999). Persuasive communication about AIDS prevention: Need for cognition determines the impact of message format. *AIDS Education and Prevention, 11*(2), 150-162. https://psycnet.apa.org/record/1999-13402-005

Berger, C. R. (1986). Uncertain Outcome Values in Predicted Relationships: Uncertainty Reduction Theory Then and Now. *Human Communication Research, 13*(1), 34-8. https://doi.org/10.1111/j.1468-2958.1986.tb00093.x

Blanco, A., Horcajo, J., y Sánchez, F. (2017). *Cognición social*. Pearson Educación.

Cacioppo, J. T., y Petty, R. E. (1982). The need for cognition. *Journal of Personality and Social Psychology, 42*(1), 116- 131. https://doi.org/10.1037/0022-3514.42.1.116

Cavazza, N., Graziani, A. R., Serpe, A., y Rubichi, S. (2010). Right-wing face, left-wing faces: The matching effect in the realm of political persuasion. *Social Influence, 5*(1), 1-22. https://doi.org/10.1080/15534510903000090

Cho, H., y Choi, J. (2010). Predictors and the role of attitude toward the message and perceived message quality in gain- and loss-frame antidrug persuasion of adolescents. *Health Communication, 25*(4), 303-311. https://doi.org/10.1080/10410231003773326

Cialdini, R. B. (2001). The Science of Persuasion. *Scientific American, 284*(2), 76-81. https://doi.org/10.1038/sci-entificamerican0201-7

Colom Marañón, R. (2018). *Manual de psicología diferencial*. Ediciones Pirámide.

Crandall, D., Cosley, D., Huttenlocher, D., Kleinberg, J., y Suri, S. (2008). *Feedback effects between similarity and social influence in online communities*. KDD.

Crous, C. (2009). Human Intelligence Sources: Challenges in Policy Development. *Security Challenges 5*(3), 117-27.

Dillon, P. J. (1998). *A theory for human intelligence operations*. USAWC Strategy Research Project.

Di Muro, F., y Murray, K. B. (2012). An arousal regulation explanation of mood effects on consumer choice. *Journal of Consumer Research, 39*(3), 574-584. https://doi.org/10.1086/664040

DeBono, K. G. (1987). Investigating the social-adjustive and value-expressive functions of attitudes: Implications for persuasion processes. *Journal of Personality and Social Psychology, 52*(2), 279–287. https://doi.org/10.1037/0022-3514.52.2.279

DeSteno, D., Petty, R. E., Rucker, D. D., Wegener, D. T., y Braverman, J. (2004). Discrete emotions and persuasion: The role of emotion-induced expectancies. *Journal of Personality and Social Psychology, 86*(1), 43-56. https://doi.org/10.1037/0022-3514.86.1.43

Dhami, M. K. (2011). *Behavioural Science Support for JTRIG's (Joint Threat Research and Intelligence Group's) Effects and Online HUMINT Operations*. Defence Science and Technology Laboratory https://www.statewatch.org/media/documents/news/2015/jun/behavioural-science-support-for-jtrigs-effects.pdf

Díez Martín, G. (2023). Efecto de la Personalidad en la Susceptibilidad a los Falsos Recuerdos. *Drafts of Economic Intelligence, 5*(1), 1-15. https://escuela-inteligencia-economica-uam.com/draft-volumen-5-2022-2023/

Dorado, S. (2019). Técnicas operativas para la fase de aproximación a la fuente. *Reports de Inteligencia Económica y RRII, 1,* 1-25. https://escuela-inteligencia-economica-uam.com/reports-2019-2020/

Dobák, I., y Tóth, T. (2021). Old Methods in The Cyberspace? (CYBER-HUMINT, OSINT, SOCMINT, Social Engineering). *Belügyi szemle*, *69*(2), 195-212. https://doi.org/10.38146/bsz.2021.2.2

Edwards, K. (1990). The interplay of affect and cognition in attitude formation and change. *Journal of Personality and Social Psychology, 59*(2), 202-216. https://doi.org/10.1037/0022-3514.59.2.202

Erdész V. (2018). A SOCMINT helye, szerepe az összadatforrású hírszerzésben. *Felderítő Szemle, 17(4)*, 27-40. https://www.knbsz.gov.hu/hu/letoltes/fsz/2018-4.pdf

Eysenck, H. J. (1970). *The structure of human personality*. Methuen.

Fabrigar, L. R., y Petty, R. E. (1999). The role of the affective and cognitive bases of attitudes in susceptibility to affectively and cognitively based persuasion. *Personality and Social Psychology Bulletin, 25*(3), 363-381. https://doi.org/10.1177/0146167299025003008

Feinberg, M., y Willer, R. (2015). From gulf to bridge: When do moral arguments facilitate political influence? *Personality and Social Psychology Bulletin, 41*(12), 1665-1681. https://doi.org/10.1177/0146167215607842

Fialka, G. (2018). Emlékek az operatív technika világából - A titkos információgyűjtés technikai támogató rendszere. En I. Dobák y Z. Hautzinger (Eds). *Szakmaiság, szerénység, szorgalom* (pp. 197-202.). Dialóg Campus

Fleming, M. A., y Petty, R. E. (2000). Identity and persuasion: An elaboration likelihood approach. En Terry, D. J. y Hogg, M. A. (Eds.). *Attitudes, behavior, and social context: The role of norms and group membership* (pp. 171- 199). Erlbaum.

Forehand, M. R., Deshpande, R., y Reed, I. I. (2002). Identity salience and the influence of differential activation of the social self-schema on advertising response. *Journal of Applied Psychology, 87*(6), 1086-1099. https://doi.org/10.1037/0021-9010.87.6.1086

Gioe, D. V, (2017). The more things change: HUMINT in the Cyber Age. En Gioe, D. V. (Ed.). *The Palgrave handbook of security, risk and intelligence* (pp. 213-227). Palgrave Macmillan.

Giannetakis, P., Iannilli, L., y Caravelli, F. (2021). Cyber Humint. A Behavioral Analysis Perspective. *American Journal of Multidisciplinary Research & Development (AJMRD)*, *2*(11), 27-33. https://www.ajmrd.com/wp-content/uploads/2020/11/E2112733.pdf

Gonzales, W. G. (2013). *Does U.S. Army Humint Doctrine Achieve Its Objectives? What Have Iraq and Afghanistan Taught Us?* [Tesis doctoral, Naval Postgraduate School] Calhoun: The NPS Institutional Archive. https://apps.dtic.mil/sti/pdfs/ADA580160.pdf

Gray, J. A. (1981). A critique of Eysenck's theory of personality. En Eysenck, H. J. (Ed.). *A model for personality* (pp. 246-276). Springer.

Grieve, R., Indian, M., Witteveen, K., Tolan, G. A., y Marrington, J. (2013). Face-to-face or Facebook: Can social connectedness be derived online? *Computers in Human Behavior*, *29(3),* 604-609. https://doi.org/10.1016/j.chb.2012.11.017

Griskevicius, V., Tybur, J. M., Gangestad, S. W., Perea, E. F., Shapiro, J. R., y Kenrick, D. T. (2009). Agrees to impress: Hostility as an evolved context-dependent strategy. *Journal of Personality and Social Psychology, 96*(5), 980-994. https://doi.org/10.1037/a0013907

Hadnagy, C. (2010). *Social engineering: The art of human hacking*. Wiley.

Hawkins, R. P., Kreuter, M., Resnicow, K., Fishbein, M., y Dijkstra, A. (2008). *Understanding tailoring in communicating about health. Health Education Research, 23*(3), 454-466. https://doi.org/10.1093/her/cyn004

Hirsh, J. B., Kang, S. K., y Bodenhausen, G. V. (2012). Personalized Persuasion: Tailoring Persuasive Appeals to Recipients' Personality Traits. *Psychological Science, 23*(6), 578-581. https://doi.org/10.1177/0956797611436349

Huerta, P. (2001). El Insider Trading y el uso de la información privilegiada. *Derecho y Sociedad, 17,* 171-179.

Huffaker, D. (2010). Dimensions of leadership and social influence in online communities. *Human Communication Research, 36*(4)*,* 593-617. https://doi.org/10.1111/j.1468-2958.2010.01390.x

Hui, P., y Buchegger, S. (2009). *Groupthink and peer pressure: Social influence in online social network groups*. 2009 International Conference on Advances in Social Network Analysis and Mining, Atenas, Grecia. https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=8e402417635acb9a0535b0bb1341549abc4bb47c

Johnson, L. K. (2010). Evaluating "Humint": The Role of Foreign Agents in U.S. Security. *Comparative Strategy*, *29*(4), 308-332. https://doi.org/10.1080/01495933.2010.509635

Jones, C. (2010). Lying, Cheating, and Virtual Relationships. *Global Virtue Ethics Review*, *6*(1), 3-12. https://www.questia.com/library/journal/1P3-2061210371/lying-cheating-and-virtual-relationships

Koren, D. (2015). *Virtual HUMINT: conducting human intelligence operations in the virtual environment* [Tesis doctoral]. Naval Postgraduate School. https://upload.wikimedia.org/wikipedia/commons/4/4e/Virtual_HUMINT-_conducting_human_intelligence_operations_in_the_virtual_environment_%28IA_virtualhumintcon1094556397%29.pdf

Laustsen, L. (2017). Choosing the right candidate: Observational and experimental evidence that conservatives and liberals prefer powerful and warm candidate personalities, respectively. *Political Behavior, 39*, 883-908. https://link.springer.com/article/10.1007/s11109-016-9384-2

Lavine, H., y Snyder, M. (2000). Cognitive processes and the functional matching effect in persuasion: Studies of personality and political behavior. En Maio, G. R. y Olson, J. M. (Eds.). *Why we evaluate: Functions of attitudes* (pp. 97-131). Erlbaum.

Lennon, S. J., Davis, L. L., y Fairhurst, A. (1988). Evaluations of apparel classification on attitudes toward apparel shopping. *Perceptual and Motor Skills, 68*(2), 485-486. https://doi.org/10.2466/pms.1989.68.2.485

LISA Institute (s. f.). *SOCMINT o Inteligencia de Redes Sociales: definición, usos y beneficios*. Recuperado el 17 de junio de 2023, de https://www.lisainstitute.com/blogs/blog/socmint-inteligencia-redes-sociales

Lombardi, M., Rosenblum, T. y Burato, A. (2015). *From SOCMINT to Digital Humint: re-frame the use of social media within the Intelligence Cycle*. Fondazione de Gasperi

Lowenthal, M. M. (2011). *Intelligence: From Secrets to Policy, Part 14*. CQ Press.

Luttrell, A., Phillip-Muller, A., y Petty, R. E. (2019). Challenging moral attitudes with moral messages. *Psychological Science, 30*(8), 1136-1150. https://doi.org/10.1177/0956797619854706

Macêdo, A., Peotta, L., y Gomes, F. (2023). A Review of the Intersection Techniques on Humint and Osint. *International Journal on Cybernetics & Informatics (IJCI), 12*(1), 1-11. https://doi.org/10.5121/ijci.2023.120105

Marin, A., y Gabbert, F. (2022). The use of self-disclosure to build rapport with mock covert human intelligence sources (CHIS). *Journal of Policing, Intelligence and Counter Terrorism,* 1-16. https://doi.org/10.1080/18335330.2022.2108331

Méndez Carrillo, F. X., Olivares Rodríguez, J., y Ros López, M. C. (2014). Capítulo IX: Entrenamiento en habilidades sociales. En Olivares Rodríguez, J. y Méndez Carrillo, F. X. (Eds.). *Técnicas de modificación de conducta* (pp. 337-369). Biblioteca nueva.

Meyers-Levy, J., y Sternthal, B. (1991). Gender differences in the use of message cues and judgments. *Journal of Marketing Research, 28*(1), 84-96. https://doi.org/10.2307/3172728

Miller, M. D., y Brunner, C. C. (2008). Social impact in technologically-mediated communication: An examination of online influence. *Computers in Human Behavior, 24*(6), 2972-2991. https://doi.org/10.1016/j.chb.2008.05.004

Mitnick, K. D., y Simon, W. L. (2002). *The Art of Deception: Controlling the Human Element of Security*. Wiley.

Mitnick, K. D., y Simon, W. L. (2005). *The Art of Intrusion: the Real Stories Behind the Exploits of Hackers, Intruders and Deceivers*. Wiley.

Mouton, F., Malan, M. M., Leenen, L., y Venter, H. S. (2014, agosto 13-14). *Social engineering attack framework* [Acta de congreso]. 2014 Information Security for South Africa, Pretoria, Sudáfrica. https://doi.org/10.1109/ISSA.2014.6950510

Nagayama Hall, G. C., y Barongan, C. (2002). *Multicultural psychology*. Prentice-hall.

North Atlantic Treaty Organization [NATO] Standardization Office (2021). *NATO Glossary of Terms and Definitions AAP-06*. NATO. https://standard.di.mod.bg/pls/mstd/MSTD.blob_upload_download_routines.download_blob?p_id=2811&p_table_name=d_ref_documents&p_file_name_column_name=file_name&p_mime_type_column_name=mime_type&p_blob_column_name=contents&p_app_id=600

Noble, G. (2009). *Diagnosing Distortion in Source Reporting: Lessons for HUMINT Reliability from Other Fields* [Tesis de Master]. Mercyhurst College. https://www.files.ethz.ch/isn/99245/Distortion_Source_Reporting.pdf

Oceja, L. (2021). *Introducción a la psicología de grupos*. No publicado.

Omand, D., Bartlett, J., & Miller, C. W. (2012). Introducing Social Media Intelligence (SOCMINT). *Intelligence and National Security*, *27*(6), 801–823. https://doi.org/10.1080/02684527.2012.716965

Öztürkci, H. (2023, May 16). The Vital Role of Human Intelligence (HUMINT) in Cybersecurity. *Medium*. https://medium.com/@halil.ozturkci/the-vital-role-of-human-intelligence-humint-in-cybersecurity-cc7fa4355ccb

Paek, H., Choi, H., y Nelson, M. R. (2012). Product, personality, or prose? Testing functional matching effects in advertising persuasion. *Journal of Current Issues and Research in Advertising, 32,* 11-26. https://doi.org/10.1080/10641734.2010.10505282

Pai, P., y Arnott, D. (2013). User adoption of social networking sites: Eliciting uses and gratifications through a means–end approach. *Computers in Human Behavior*, *29*(3), 1039-1053. https://doi.org/10.1016/j.chb.2012.06.025

Peris, R., Gimeno, M. F., Pinazo, D., Ortet, G., Carrero, V., Sanchiz, M., y Ibáñez, I. (2002). Online Chat Rooms: Virtual Spaces of Interaction for Socially Oriented People. *Cyberpsychology & behavior*, *5*(1), 43-51. https://doi.org/10.1089/109493102753685872

Petty, R. E. y Briñol, P. (2012). The Elaboration Likelihood Model. En P. A. M. Van Lange, A. Kruglanski, y E. T. Higgins (Eds.). *Handbook of theories of social psychology* (vol. 1) (pp. 224-245). Sage.

Petty, R. E. y Cacioppo, J. T. (1986). *Communication and persuasion: Central and peripheral routes to attitude change*. Springer.

Postmes, T., Spears, R., Sakhel, K., y de Groot, K. (2001). Social influence in computer-mediated communication: The effects of anonymity on group behaviour. *Personality and Social Psychology Bulletin, 27,* 1242-1254. https://doi.org/10.1177/01461672012710001

Redlich, A. D., Kelly, C., y Miller, J. (1a. C.). *Systematic Survey of the Interview and Intelligence Community: FINAL REPORT TO THE FBI-HIG*. Recuperado 17 de junio de 2023, de http://archive.reid.com/pdfs/20120324.pdf

Rodríguez Redondo, R. y Sánchez Margolles, S. (2023). Explotación de vulnerabilidades psicológicas en inteligencia de fuentes humanas. *Reports de Inteligencia Económica y Relaciones Internacionales, 12*, 1-39. https://escuela-inteligencia-economica-uam.com/reports-2022-2023/

Rucker, D. D., y Petty, R. E. (2004). Emotion specificity and consumer behavior: Anger, sadness, and preference for activity. *Motivation & Emotion, 28,* 3-21. https://link.springer.com/article/10.1023/B:MOEM.0000027275.95071.82

Russano, M. B., Narchet, F. M., y Kleinman, S. M. (2014a). Analysts, interpreters, and intelligence interrogations: Perceptions and insights. *Applied Cognitive Psychology, 28*(6), 829-846. https://doi.org/10.1002/acp.3070.

Russano, M. B., Narchet, F. M., Kleinman, S. M., y Meissner, C. A. (2014b). Structured interviews of experienced HUMINT interrogators. *Applied Cognitive Psychology, 28*(6), 847-859. https://doi.org/10.1002/acp.3069.

Sánchez Margolles, S. (2022). Personalidad en Ingeniería Social: ¿Qué rasgos son más vulnerables? *Drafts of Economic Intelligence, 4*(2), 15-30. https://escuela-inteligencia-economica-uam.com/draft-volumen-4-2021-2022/

Sánchez-Muñoz, I., Calcerrada Alcazar, M. L., González Álvarez, J. L., y De Juan Espinosa, M. (2018). Persuasión y Personalidad. El receptor en la comunicación persuasiva. *Behavior & Law Journal, 4*(1), 9-20. https://doi.org/10.47442/blj.v4.i1.48

Sano, J. (2015). The Changing Shape of HUMINT. The Intelligencer: *Journal of U.S. Intelligence Studies, 21*(3), 77-80.

Sayre, R. A. (2004). *Some Principles of Human Intelligence and Their Application*. US Army School for Advanced Military Studies.

Scheeres, J. W. (2008). *Establishing the Human Firewall: Reducing an Individual's Vulnerability to Social Engineering Attacks.* [Tesis de master] Air Force Institute of Technologyhttps://www.semanticscholar.org/paper/Establishing-the-Human-Firewall%3A-Reducing-an-to-Scheeres/a2d3f4340b7db6f9d162adb53826060e294eb446

Scott, V., Mottarella, K., y Lavooy, M. J. (2006). Does Virtual Intimacy Exist? A Brief Exploration into Reported Levels of Intimacy in Online Relationships. *Cyberpsychology & behavior*, *9*(6), 759-761. https://doi.org/10.1089/cpb.2006.9.759

See, Y. H. M., Petty, R. E., y Evans, L. M. (2009). The impact of perceived message complexity and need for cognition on information processing and attitudes. *Journal of Research in Personality, 43*(5), 880-889. https://doi.org/10.1016/j.jrp.2009.04.006

Seisdedos, C. (2023). *Vigilancia estratégica*. No publicado.

Shepherd, R. (2009). *The Applications of Human Intelligence in Counterterrorism.* [Tesis doctoral] University of Calgary. http://dspace.ucalgary.ca/jspui/bitstream/1880/48904/1/2009_Shepherd_MSS.pdf.

Smith, P. B., y Bond, M. H. (1998). *Social psychology across cultures (2nd Edition)*. Hemel Hempstead: Prentice-Hall.

Steinmetz, K. F., Pimentel, A., y Goe, W. R. (2021). Performing social engineering: A qualitative study of information security deceptions. *Computers in Human Behavior*, *124,* 106930. https://doi.org/10.1016/j.chb.2021.106930

Teeny, J. D., Siev, J. J., Briñol, P., y Petty, R. E. (2020). A Review and Conceptual Framework for Understanding Personalized Matching Effects in Persuasion. *Journal of Consumer Psychology, 31*(2), 382-414. https://doi.org/10.1002/jcpy.119

Tóth T. (2020). Az egyes Social Engineering módszerek elhatárolása és rendszerezése. *Szakmai Szemle, 18*(1), 87-110.

Webb Hooper, M., Rodríguez De Ybarra, D., y Baker, E. A. (2013). The effect of placebo tailoring on smoking cessation: A randomized controlled trial. *Journal of Consulting and Clinical Psychology, 81*(5), 800-809. https://doi.org/10.1037/a0032469

Wegener, D. T., Petty, R. E., y Klein, D. J. (1994). Effects of mood on high elaboration attitude change: The mediating role of likelihood judgments. *European Journal of Social Psychology, 24*(1), 25-43. https://doi.org/10.1002/ejsp.2420240103

Whillans, A. V., Caruso, E. M., y Dunn, E. W. (2017). Both selfishness and selflessness start with the self: How wealth shapes responses to charitable appeals. *Journal of Experimental Social Psychology, 70,* 242-250. https://doi.org/10.1016/j.jesp.2016.11.009

Wolsko, C., Ariceaga, H., y Seiden, J. (2016). Red, white, and blue enough to be green: Effects of moral framing on climate change attitudes and conservation behaviors. *Journal of Experimental Social Psychology, 65,* 7-19. https://doi.org/10.1016/j.jesp.2016.02.005

Yan, L., Liu, M. T., Chen, X., y Shi, G. (2016). An arousal- based explanation of affect dynamics. *European Journal of Marketing, 50,* 1159-1184. https://www.emerald.com/insight/content/doi/10.1108/EJM-05-2015-0288/full/html

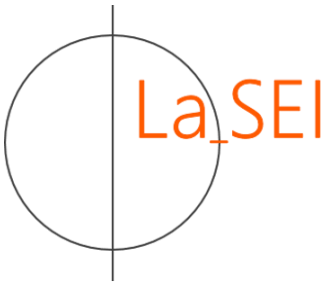
Yee, N., Ducheneaut, N., Nelson, L., y Likarish, P. (2011). Introverted elves & conscientious gnomes: the expression of personality in World of Warcraft. *Proceedings of the SIGHI Conference on Human Factors in Computing Systems*, 753-762. https://doi.org/10.1145/1978942.1979052

Zamorano, A., Dorado, S. y de Vicente, M. (2023) *Operaciones HUMINT con fines de inteligencia y persuasión.* No publicado.

Zunzarren Denis, H. (2014). *HUMINT: La parte operativa de la influencia.* No publicado.

Zunzarren Denis, H. (2022). *El pensamiento analítico.* No publicado.

Zunzarren Denis, H. y Aguirre, V. (2019). Influencia estratégica: ¿Cómo conseguir los cambios de actitud que me benefician? *Journal of Economic & Business Intelligence, 1*(5), 35-41. https://escuela-inteligencia-economica-uam.com/journal-volumen-1-2019-2020/.



Reports de Inteligencia Económica y Relaciones internacionales

[ISSN 2660-7352]

PUBLICACIONES DE LA ESCUELA DE INTELIGENCIA ECONÓMICA DE LA UAM


La_SEI
School of Economic Intelligence & International Relations
Escuela de Inteligencia Económica y RRII
Universidad Autónoma de Madrid