Comunicación presentada en el Congreso Análisis de Inteligencia y Prospectiva.
Grupo de Estudios en Seguridad Internacional. Universidad de Granada, 8-9 de abril de 2019

OSINT: características, debilidades y engaño

OSINT: Characteristics, weaknesses and deception.

YAGO RODRÍGUEZ RODRÍGUEZ

RESUMEN: Averiguando a través de las lecciones históricas cuales son los pilares y características que moldean el OSINT, entenderemos mejor esta forma de inteligencia, y en particular sus grandes debilidades y posibilidades de explotación ante actores dispuestos a aprovecharlo para provocar el engaño.

PALABRAS CLAVE: OSINT, características, engaño, diversión, historia

ABSTRACT: By learning from the history we can discover the main characteristics that shape OSINT, and so we will be able to better understand this form of intelligence and especially its weaknesses that can be exploited to accomplish deception of enemy intelligence.

KEYWORDS: OSINT, characteristics, deception, diversion, history

INTRODUCCIÓN

El objeto de este trabajo es llevar a cabo una reflexión profunda sobre el OSINT mediante el método deductivo, a fin de enumerar sus características más esenciales y con base en ello comprender sus ventajas y sus desventajas, sus fortalezas y sus debilidades. Confrontaremos lo deducido con las operaciones de engaño, contrainteligencia o diversión, basadas en el OSINT, para indagar en una de las facetas menos tratadas del mismo, a la que nominaremos contraosint.

Comenzaremos por una explicación teórica de lo que es el OSINT, a continuación contaremos parte de la historia del OSINT en bruto, y la pondremos en relación con las operaciones de inteligencia, engaño, diversión y similares, dentro de esto daremos especial relevancia a la operación *Bodyguard*, por su envergadura y sus objetivos estratégicos y operacionales en plena Segunda Guerra Mundial. Toda esta historia en bruto, la refinaremos para extraer aquellos que consideremos los caracteres más importantes del OSINT actual, y finalmente reflexionaremos acerca de ellos en el marco de eso que, explicativamente, hemos dado en llamar contraosint.

¿QUÉ ES EL OSINT?

En 2001 el *Allied Joint Intelligence* de la OTAN, documento AJP-2.0.2001 definía el OSINT como: "La inteligencia derivada de una amplia gama de recursos abiertos, como la radio, la televisión, los periódicos, los libros; a los que el público tiene acceso".

El *National Defense Authorization Act for Fiscal Year 2006, Public Law 109-163*, sección 931 de Estados Unidos definía el OSINT como "[…] la inteligencia que se produce a través de información disponible para el público, que es obtenida, explotada y diseminada en el tiempo y para la audiencia apropiada, a fin de satisfacer una petición de inteligencia concreta"

En el *Handbook of Intelligence Studies*, publicado en 2006 se definía así: "[…] información que no está clasificada, que ha sido intencionadamente descubierta, separada, tamizada y diseminada a una audiencia seleccionada a fin de responder a una pregunta específica."

Podríamos aportar muchas más definiciones de lo que es el OSINT, y todas coincidirán en hablar de "fuentes abiertas" y "accesibilidad al público", otras añadirán la definición del objetivo de cualquier forma de inteligencia, que es satisfacer una necesidad de conocimiento, lo que naturalmente depende de que la reciba a tiempo la persona correcta.

Partimos de lo anterior para plantear que el OSINT es un concepto más intuido que definido, y que probablemente nunca podrá ser plenamente delimitado, en este sentido no hemos de agarrarnos a definiciones teóricas, sino a saber que

todos tenemos a nuestra disposición herramientas para acceder fácilmente a datos e información que son útiles para elaborar inteligencia.

En las otras ramas de la inteligencia, como la inteligencia de señales (SIGINT), la inteligencia mediante imágenes (IMINT), la inteligencia humana (HUMINT), parece que se ha acudido más al medio o a la técnica por la que se sustrae la información para delimitar los conceptos. Por ejemplo, el HUMINT se funda en lo que podemos averiguar a través de las relaciones entre seres humanos, en el SIGINT, nos basamos en lo que nos dice el análisis de las señales radioeléctricas, y en el IMINT de las imágenes.

Opuesto a la lógica de las otras formas de inteligencia entra en juego el OSINT, que no alude al medio o a la técnica, sino a la posibilidad de acceso a fuentes de las que obtener inteligencia. Todas las formas de inteligencia utilizan sus fuentes, y la facilidad de acceso a las mismas puede ir desde lo fácil hasta lo difícil, desde lo público hasta lo secreto, y por tanto en puridad podríamos decir que el IMINT, el SIGINT o el HUMINT pueden, a veces ser OSINT.

No hay más que pensar en las emisiones de radio de la BBC, que cualquiera con conocimientos y un equipo de radio puede recolectar para ver si por ejemplo, se están introduciendo mensajes mediante esteganografía. ¿Sería este análisis de señales de una radio pública OSINT? Al contrario, si estamos hablando de una televisión local enemiga que emplea señales de corto alcance y queremos poder monitorizarla, tendremos que llevar a cabo una riesgosa operación encubierta para instalar una línea de receptores, transmisores y repetidores para que transmitan a centenares de kilómetros ¿sería esto un simple OSINT?

Podríamos plantear muchas más preguntas ¿obtener acceso a un congreso que funciona por invitación, gracias a una relación personal es OSINT? Si la renta media anual en un país africano es de 100 dólares, ¿podríamos considerar OSINT que un ciudadano de este país pague 30 euros por acceder al congreso que nos ocupa?

Por tanto, el OSINT no está del todo delimitado, pero para la mayor parte de los casos, se considerará OSINT; u OSCINT, como a veces se expresa, a la radio, la televisión, los congresos, los documentos académicos o similares, a menudo conocidos como literatura gris, las bibliotecas, ciertos servicios por suscripción, como *IHS Jane's* o todo aquello que esté al alcance de cualquiera con un *Personal Computer* y conexión a internet.

Por su parte, el libro de bolsillo de la OTAN (NOSINTH) establecía dos categorías de fuentes abiertas: de un lado, el OSINT, que se concebía como el resultado de introducir el Open Source Information (OSINF) en el ciclo de inteligencia, de otro lado el OSINT validado (V-OSINT), que se trataba de inteligencia de origen OSINT que se consideraba altamente fidedigna.

Finalmente conviene saber que habitualmente se habla de OSINF y OSIND, esto es información y datos de fuentes abiertas respectivamente, en alusión a ambas categorías de conocimiento.

HISTORIA DEL OSINT: INTELIGENCIA Y ENGAÑO

Eclesiastés, en la Biblia dijo: "Lo que pasó, eso pasará; lo que se hizo, eso se hará: no hay nada nuevo bajo el sol. Si de algo se dice: Mira, esto es nuevo, eso ya sucedió en otros tiempos mucho antes de nosotros."

En realidad, esto mismo le ocurre al OSINT, y aunque nos afanemos en intentar apuntar una primera vez, lo cierto es que ya en la antigua Roma existían documentos públicos, pregones, y foros donde cualquiera podía enterarse de los rumores que circulaban, y es muy posible que los generales de la antigüedad consultaran con los comerciantes las condiciones políticas y rumores de los que los mercaderes se habían enterado en sus expediciones comerciales.

La esencia del OSINT moderno, las fuentes abiertas, es la misma de siempre, sin embargo el accidente en muchos casos ha cambiado, y dichos cambios bien podrían tener más importancia que una pretendida esencia del OSINT, de ahí que la historia de la existencia de fuentes abiertas desde que el hombre es hombre tampoco nos resulta de tanto interés.

En cuanto al OSINT moderno, en los años 30 la Universidad de Princeton llevó a cabo grandes avances en materia de monitorización de radio de onda corta extranjera gracias al *Princeton Listening Center* y a partir de 1941 el *Foreign Broadcast Intelligence Service* basándose en los trabajos anteriores, comenzó a monitorizar la radio enemiga para obtener inteligencia. Por su parte, el *Interdepartamental Commitee for the Acquisition of Foreign Periodicals* también se dedicó a obtener publicaciones del Eje (Mercado, 2001).

Se tiende a considerar que el OSINT actual nació en 1942, cuando se creó la rama *Research and Analysis* del *Office of Strategic Services* (OSS), la que se encargaba de recopilar toda la información abierta, haciendo traer periódicos del Eje gracias a una nutrida red de embajadas y consulados, escuchando las emisiones de las radios públicas extranjeras, o en general accediendo a librerías y fuentes de información oficiales (CIA, 2013).

A mediados de 1942, el director de la sección de Lejano Oriente del OSS, Charles Fah advirtió de que el trabajo de monitorización de la radio extranjera era indispensable para el OSS y constituía la mayor fuente singular existente de información. (Mercado, 2004)

El del OSS destaca por ser el ejemplo más conocido, en el que expresamente se valoran todas estas fuentes bajo el término "*open sources*", aunque en realidad todos los bandos del conflicto, incluidos japoneses y alemanes sabían del valor de estas formas de inteligencia, por lo que dedicaban esfuerzos a su recolección.

Los Aliados eran conscientes de los esfuerzos germanos y no tardaron en usar a la prensa como una fuente de desinformación, suministrando información falsa, como cifras de producción de material de guerra, para que se enviaran a Berlín, pero aún así no siempre se podía controlar a la prensa (Fah, 1946).

Ejemplificando lo anterior, pensemos que lo que determinaba la filosofía de diseño de los blindados, o la asignación de recursos a cada tipo de equipo en la Alemania de Hitler dependía de la percepción que tuvieran de la producción industrial de Aliados y Soviéticos, de tal forma que la información errónea, una vez procesada daba lugar a un producto de inteligencia viciado, que podía llevar a adoptar decisiones equivocadas.

Al comienzo de la invasión alemana de Rusia en junio de 1941, la *Werhmacht* estaba introduciendo el nuevo y capaz cañón contracarro PaK 38 de 50 mm, aunque las cantidades del mismo fueron exiguas hasta bien entrada la guerra, sin embargo los noticieros alemanes tendían a mostrar siempre a las unidades mejor equipadas, por lo que este tipo de armas aparecían con mucha más frecuencia en los medios que en el campo de batalla.

Los soviéticos pronto sobreestimaron la cantidad de PaK 38 en servicio, y sabiendo de sus capacidades vieron la necesidad de aumentar el grosor del blindaje de los carros de combate T-34. Para remediar este problema, y pese a estar en pleno traslado de la industria pesada desde Europa hasta los Montes Urales, se ordenó añadir una suerte de blindaje añadido consistente en planchas de 20 a 35 mm de espesor en todo el arco frontal de los T-34, lo que complicó su fabricación. (Healy, 2018)

Cuatro meses después de empezar a producir T-34 con este blindaje, se dio la contraorden de cesar su fabricación, al comprobarse la escasez de PaK 38, y por tanto la eficacia del blindaje original del T-34 contra la mayor parte del arsenal alemán.

Ahora bien, aunque la prensa puede convertirse en un vector para las operaciones de engaño planificadas, también se convierte en un arma de doble filo, al poder revelar informaciones críticas, lo que además ocurre con mayor frecuencia si se trata de un país con prensa libre, donde ejerce como un contrapoder, y no como una herramienta más del estado.

El 7 de junio de 1942, el día después de la victoria estadounidense en la batalla de Midway, *The Chicago Tribune* aireó en su portada que la Marina de Estados Unidos había sabido de los planes japoneses “varios días antes de que la batalla se produjera”, lo que de haber sido leído por los nipones seguramente les habría llevado a saber que sus códigos de comunicaciones habían sido rotos (Mercado, 2004).

Volviendo al OSINT y a las actividades de contrainteligencia, podemos citar la treta alemana previa a la batalla de Kursk, en 1943 (Carell, 2008). Por entonces, el general Von Manstein, uno de los más reputados expertos en guerra acorazada fue enviado a Bucarest para imponer la Medalla de Crimea de Oro

al mariscal rumano Ion Antonescu, por su apoyo en la batalla de Sebastopol el año anterior.

Pronto, todos los noticieros se hicieron eco de la importante noticia, ¡Von Manstein se dirigía a Bucarest! No era posible que la gran ofensiva alemana de verano fuera inminente mientras un general de su talla estuviera en Rumanía. Pero aquel mismo día, Manstein fue enviado a Rastenburg, el cuartel general de Hitler en Prusia Oriental, a fin de acordar la fecha definitiva para el lanzamiento de la que sería la batalla de Kursk.

Para camuflar el movimiento de Manstein, los alemanes enviaron una nota de prensa alertando de que el avión del general había sufrido un percance y tardaría unas 24 horas en llegar a Rumanía. Tras la reunión en Rastenburg, Manstein acudió a Bucarest para imponer la condecoración a su aliado rumano, entretanto toda la prensa y los noticieros se hicieron eco de la presencia del general en la capital, cuando en realidad este la abandonó a toda prisa para ponerse al mando del 4º Ejército que encabezaría la ofensiva sólo unos días después.

En ocasiones, se disponía de agentes o de informantes colocados en puestos clave de la jerarquía enemiga (Carell, 2008), como fue el caso de los soviéticos o de los ingleses, cuyos agentes les avisaron, por ejemplo, de la visión alemana respecto al desembarco aliado en Europa, o respecto a la inminente invasión de la Unión Soviética en junio de 1941. Pero en estos casos, bien porque no se consideraban fuentes fiables, bien porque el decisor las desechaba, bien porque sus informes no llegaban en tiempo y forma a las manos adecuadas, todo ese HUMINT perdía su utilidad.

A mediados de los años 50, los oficiales de inteligencia norteamericanos pudieron averiguar el empeoramiento de las relaciones entre la China comunista y la URSS simplemente gracias a la lectura de sus respectivas propagandas (Mercado, 2004).

Posiblemente el caso más flagrante de desastre militar fruto de la poca atención al OSINT enemigo fue el de la invasión de Bahía Cochinos, que se produjo en junio de 1961 y que había sido previamente aireada en conversaciones en espacios públicos por parte de miembros de las fuerzas invasoras, de diversos periódicos estadounidenses, y hasta por Radio Moscú, que alertó de la inminencia del desembarco “en una semana”, acertando de pleno (Beschloss, 1991)

Gracias a todas estas filtraciones Fidel Castro, el decisor, pudo tomar las decisiones correctas, ejecutando una serie de sabotajes en Miami y posicionando sus fuerzas de reserva en tiempo y forma para enfrentar a las fuerzas de desembarco anticomunistas, quienes fueron aniquiladas.

A medida que pasa el tiempo, el OSINT y el OSINF se tornan más útiles y amplios. Por ejemplo, en plena guerra de Vietnam todo el mundo era consciente, gracias a los noticieros, de la situación interna en Estados Unidos, y probablemente el mando norvietnamita pudo tomarle el pulso a la política

interna del país, para saber que estaba siguiendo la estrategia adecuada, a pesar de que militarmente todo parecía una gran derrota ¿Hubiera sido la persistencia de los norvietnamitas la misma si no hubieran tenido acceso a la información sobre la situación interna norteamericana?

Más adelante, a partir de la guerra del Golfo de 1991, aparecieron canales de noticias internacionales como la CNN, capaces de informar en todo el mundo de los grandes acontecimientos en cosa de minutos.

Precisamente fue a lo largo de los años 90 cuando se fraguó la gran revolución que hemos experimentado en el siglo XXI. La aparición y la popularización de las computadoras unidas a esa conexión global llamada "internet", abrieron un nuevo mundo de posibilidades al OSINT.

El conocimiento generado en tiempos pretéritos empezaba a digitalizarse y a poder consultarse fácil y rápidamente, asimismo las relaciones de todo tipo empezaban a tener un importante soporte en internet: desde foros militares donde los veteranos mantenían una comunidad, hasta redes sociales que facilitaban el acceso a las opiniones de auténticos expertos, pasando por las viejas radios, televisiones o diarios que también eran consultables.

El gran mérito de internet era convertir a cada usuario en una fuente de información accesible, haciendo una puesta en común afluente del gran mar de información, dando lugar a un aumento espectacular de las posibilidades de obtención y haciendo que dentro del ciclo de inteligencia la fase crítica fuera el procesamiento de la información adecuada, y no tanto su mera obtención.

En plenos años 90 el *National Foreign Intelligence Board* de Estados Unidos advirtió que sobre el presupuesto anual de 28 a 35 mil millones de dólares dedicados a procesar y obtener productos clasificados, sólo el 1% era gastado en OSINT, mientras que esta forma de inteligencia proveía el 40% de los productos de todo origen, a su vez el *Deputy Director of Science and Technology* de la CIA elevaba la cifra al 70%. (Steele, 1997)

El general estadounidense Tony Zinni, perteneciente al Cuerpo de Marines, mientras comandaba el CENTCOM aseveró que el 80% de lo que necesitaba saber procedía de fuentes abiertas, y si sabía donde buscar, podía llegar a cubrir el 96% de las necesidades.

En 1997, el general Peter Schoomaker, al mando del *Special Operations Command* (SOCOM) decidió la creación del J-23, que estaría encargado de satisfacer los requerimientos de las fuerzas especiales empleando herramientas propias del OSINT, de esta forma la unidad fue dotada de veintidós empleados y cinco millones de dólares anuales. Con este magro presupuesto, el SOCOM, acostumbrado a trabajar en operaciones muy sensibles pudo satisfacer el 40% de sus requerimientos (Steele, 2003).

En la actualidad el OSINT, se ha popularizado más que nunca, de tal forma que en internet cualquier usuario con unos mínimos conocimientos puede

averiguar muchas cosas, y no digamos si un grupo de usuarios con habilidades se organizan: no tenemos más que recordar el caso de Bellingcat.

Bellingcat fue fundada por Elliot Higgins, quien no era más que un ingeniero en paro en el Reino Unido, que empezó con un pequeño blog en el que se hacía trazado de material de guerra, y en especial armas químicas empleadas durante el conflicto de Siria, pero su mayor éxito vino con el derribo del avión civil MH-17 al sobrevolar Ucrania, un suceso con fuertes connotaciones políticas y diplomáticas, especialmente por la cifra de holandeses fallecidos.

El equipo de Bellingcat se puso manos a la obra, analizó miles de vídeos que aparecieron en la red aquellos días, y tras un exhaustivo trabajo aportaron pruebas clave que apuntaban a que un sistema antiaéreo ruso BUK había sido el autor del derribo. Estas pruebas fueron empleadas para el informe técnico del gobierno holandés, siendo tan o más importantes que las presentadas por los servicios de inteligencia estatales.

Otro ejemplo de OSINT lo podemos encontrar en el Estado Islámico, quien a la hora de entrenar a los tiradores de sus misiles contracarro no ha dudado en obtener información de los carros de combate enemigos, de esta forma ha adiestrado a sus soldados para que apunten a las zonas en las que se ubica la munición, ya que un impacto ahí tiende a producir una explosión catastrófica.

No tenemos más que ver las clases teóricas del vilayato del Sinaí, o los lugares de impacto de los misiles yihadistas sobre los Leopard 2A4 turcos para darnos cuenta del OSINT existente detrás.

Un último ejemplo de OSINT, que demuestra ser un arma de doble filo, es el del asesor de seguridad nacional de Estados Unidos John Bolton, quien en plena crisis con el gobierno venezolano de Maduro apareció con una nota manuscrita inocentemente visible en la que ponía “5.000 troops to Venezuela”.

La operación Bodyguard

En los años anteriores al desembarco de Normandía, en junio de 1944, los Aliados se esforzaron por ejecutar operaciones de engaño y diversión estratégicas que tenían por finalidad debilitar la respuesta alemana contra la invasión mediante la dispersión general de la *Wehrmacht* por todas las zonas en que era posible un desembarco: desde Grecia hasta Noruega (Smith, 2014)

En segundo lugar, se buscó retrasar y debilitar la respuesta táctica y operacional contra las cabezas de playa, para lo que se debía confundir al enemigo sobre las intenciones y capacidades de las fuerzas invasoras aliadas.

De esta forma, el plan de engaño fue masivo e incluyó varias operaciones separadas, a saber, *Fortitude North* para distraer tropas enemigas en la península de Escandinavia, que sería apoyada mediante una serie de fintas militares y diplomáticas de Suecia mediante el plan *Graffham*. *Royal Flush* y *Cooperhead*, diseñadas para aparentar que la fecha de la invasión iba a ser posterior a la real, *Zeppelin*, para distraer tropas alemanas en el Mediterráneo

oriental, *Ironside*, *Vendetta* y *Ferdinand*, para distraer tropas alemanas en el Mediterráneo occidental, y *Fortitude South*, para imbuir en los planificadores alemanes la idea de que el desembarco de Normandía era una operación secundaria de diversión del auténtico desembarco en el estrecho de Calais (Terrell, 2002).

Se emplearon numerosas estratagemas. Permitir que el enemigo captara comunicaciones aparentemente valiosas, emitir mentiras a través de la prensa, emplear dobles de los grandes generales para aparentar estar interesados en distintos lugares para un desembarco, dejar cadáveres flotando a la deriva junto a falsos planes secretos para la invasión, aparentar poseer muchas más fuerzas de las realmente disponibles, simular un ejército fantasma dirigido por el general George S. Patton, cuya "huella radioeléctrica" era simulada por el *5th Wireless Group*, etcétera.

Especialmente eficaz fue *Fortitude South*, porque de un lado se explotó la creencia alemana de que el desembarco se produciría en el paso de Calais, y porque de otro lado introdujo la idea espuria de que en Normandía se iba a producir un desembarco de distracción de menor envergadura (Prieto del Val, 2015).

Bodyguard funcionó a la perfección en todos los sentidos, por ejemplo los alemanes estimaron que la fuerza Aliada disponible era de 92 a 97 divisiones, cuando en realidad eran 38 divisiones, asimismo en Grecia los alemanes mantuvieron 22 divisiones, en Noruega 12, en Dinamarca 6, y en Bélgica y Holanda, como reserva operacional para Calais-Normandía un total de 19 divisiones. Al final, para contener el desembarco sólo existía un número limitado de divisiones, muchas de ellas de baja calidad, junto a la costa (Terrell, 2002).

Como vemos, en conjunto se consiguió distraer a unas 40 divisiones por toda la línea costera del *Reich*, mientras que la gran reserva de 19 divisiones para contrarrestar el desembarco se encontraba a demasiada distancia de Normandía, y a raíz de los ataques aéreos y los despliegues erróneos en Calais no sería capaz de llegar en tiempo y forma a las playas de Normandía.

La sorpresa lograda fue absoluta, e incluso perduró varias semanas después del asalto anfibio, logrando que las figuras de bajas Aliadas fueran cinco veces menores de las previstas y sobre todo evitando el temido contraataque alemán sobre las playas.

CARACTERÍSTICAS DEL OSINT

Con base en la historia podemos dilucidar una serie de características del OSINT, que nos permiten conocer sus puntos fuertes y sus puntos débiles, y a partir de ahí elaborar nuestras reflexiones.

- *Eficiente.* Desde el punto de vista de la inversión de recursos y el equilibrio que mantienen con el tiempo y los beneficios generados, el OSINT es la forma de inteligencia que permite obtener más con menos y en el menor plazo.
- *Rápido.* Antes de internet, y aún más después, el acceso a la información abierta permite efectuar de la forma más ágil el ciclo de inteligencia.
- *Intermediado.* Cuando se hace OSINT se pesca en el mar de datos e información que otros han generado, de tal forma que las fuentes normalmente han pasado por al menos un intermediario, cuando no varios.
- *Dependiente*. La existencia de intermediarios también indica la presencia de dos extremos:, una fuente y un receptor, que respectivamente generan y sufren una dependencia, asimismo tienden a existir numerosos intermediarios en la forma de editores, periodistas, usuarios, medios, etcétera.
- *Accesible.* El reducido coste económico de los medios que permiten a los individuos llenar el mar de información, es el mismo coste reducido que permite a los buscadores de información hacer OSINT, así pues cualquier individuo u organización pequeña o grande, rica o pobre, puede hacer uso de esta forma de inteligencia con un mayor o menor grado de éxito,- pero casisiempre de éxito.

  Ahora bien, como siempre ha ocurrido, lo accesible y lo público, y lo secreto y lo sensible tienden a repelerse, así pues no es de esperar que lo más comprometido y sensible pueda ser siempre averiguado de la forma más óptima mediante el OSINT.
- *Voluminoso.* El mar de información siempre ha sido grande, pero con la llegada de una red global en la que cualquier individuo es una fuente de información el volumen total se ha disparado hasta convertir a la fase de procesamiento, y no a la de obtención, en el mayor reto.

Las características anteriormente mencionadas nos permiten a su vez determinar cuales son los pilares más débiles del OSINT, y por tanto los más susceptibles de convertirse en fuentes de engaños u errores.

Está claro que se puede hacer OSINT, en poco tiempo, con pocos recursos y con un voluminoso acceso a distintas fuentes, si bien es cierto que no todas las materias están igual de bien cubiertas por las fuentes abiertas.

Por el contrario, existe una fortísima relación de dependencia entre el adquirente de la información, el suministrador y los medios o personas intermediarias, lo que a su vez se origina por el facilísimo acceso, que da lugar a la aparición de una gran cantidad de fuentes abiertas.

Por tanto, un concepto clave es el V-OSINT u OSINT verificado anteriormente comentado, ya que la cantidad de fuentes no es proporcional a la

posibilidad de comprobar su veracidad, y en realidad, cualquiera puede verter informaciones viciadas, de ahí la necesidad de seguir un buen proceso de verificación de las fuentes fiables, y de la aplicación del pensamiento crítico en el análisis.

CONTRAOSINT

Cuando se trata de llevar a un actor a tomar la decisión incorrecta es necesario comprender lo que significa el engaño, la simulación, la diversión, el enmascaramiento, la ocultación, la decepción e imbricar todas estas posibilidades en una serie de planes con objetivos finales concretos, los que tras haber estudiado al enemigo, llevaran a aumentar las probabilidades de que el decisor enemigo tome las decisiones que deseamos.

Como hemos visto, el ejercicio de argucias como las de *Bodyguard* tiene como objetivo influir directa o indirectamente, pero siempre de forma determinante en el decisor. Por tanto, es fundamental conocer al decisor último, en especial su psicología y sus preconcepciones, para poder idear las operaciones más eficaces.

Por ejemplo, casi siempre es más fácil reforzar las preconcepciones del contrario que inducirle nuevas preconcepciones o que hacer que las reemplace por otras, de esta forma en función de la capacidad que tengamos para realizar y sostener el engaño determinaremos si podemos aspirar a reforzar sus preconcepciones; que va a producirse el desembarco en Calais, a generarle nuevas ideas; que va a producirse un desembarco en Grecia y Noruega, o a que combine ambas; que va a producirse un desembarco de diversión en Normandía mientras el principal se produce en Calais (Terrell, 2004).

Ahora bien, el decisor no está sólo, y a él le condicionan los mecanismos de apoyo a la toma de decisiones, basados principalmente en los productos de inteligencia que a su vez proceden de fuentes de diverso origen y forma de obtención: MASINT, SOCINT, OSINT, HUMINT, SIGINT, etcétera.

Por tanto, para inducir en el decisor la respuesta deseada habrá que apuntar los esfuerzos a sus fuentes de inteligencia, ya que alterándolas, se alterará toda la cadena de apoyo a la toma de decisiones hasta el mismísimo decisor final.

Naturalmente, es imprescindible conocer lo mejor posible el funcionamiento de la obtención de información, el análisis de inteligencia enemigo, su psicología y sus preconcepciones, de tal forma que podamos determinar que tretas le serán recolectables y creíbles para la organización que represente nuestro objetivo.

Respecto a la recolección, de poco sirve una operación de engaño si el enemigo no la percibe por sus medios de obtención. Imaginemos que a nadie se le hubiera ocurrido ampliar la imagen de la carpeta en la que John Bolton

había apuntado "*5.000 soldiers to Venezuela*", la treta no habría llegado a su destinatario.

Respecto a la credibilidad, es necesario comprender al análisis y al analista enemigo en todas sus facetas para determinar que engaños serán más creíbles, pasando así todos sus filtros y precauciones.

Para ejemplificar todo lo anterior, si sabemos que nuestro enemigo tiene una gran confianza en ciertos agentes podremos suministrarles informaciones veraces que el enemigo pueda corroborar mediante otras fuentes, para reforzar su confianza, y posteriormente suministrarle las informaciones erróneas convenientes. También sabremos si nos conviene que nuestra fuerza aérea le impida emplear sus medios de reconocimiento aéreo, o si nos será útil dejarle llevar a cabo el reconocimiento de una zona para que se lleve una impresión errónea.

Es como si pretendemos cazar a un animal con un cepo: no podemos dejar este último en cualquier lugar, sino que deberemos ponerlo allá donde el animal beba, coma o viva, pero sin que su presencia sea tan obvia como para que sospeche que está ante una trampa.

Los Aliados sabían cuáles eran las principales fuentes de los alemanes y de hecho habían neutralizado o captado a todos sus agentes en Gran Bretaña, asimismo conocían los perfiles psicológicos, los sesgos de sus gerifaltes en materia de inteligencia y hasta habían desencriptado sus códigos de comunicaciones más complejos y secretos.

No sólo controlaban directamente buena parte de los medios de obtención enemigos, sino que conocían y manipulaban muy bien aquellos medios que no controlaban, como los receptores de señales o los aviones de reconocimiento de la *Luftwaffe*. Por último, comprendían perfectamente las dinámicas internas del *III Reich*, de tal forma que podían manipular a los germanos de múltiples maneras. Incluso se llegaron a facilitar informaciones veraces para que el almirante Canaris al mando del *Abewehr* pudiera presentar resultados ante sus superiores (Terrell, 2002).

Y aquí está el quid de la cuestión de las operaciones de engaño en la era actual. Puesto que el OSINT se ha convertido en la forma de inteligencia que provee la mayor parte de la información; Robert Steele habla de una regla general del 80%, podemos prever con mayor facilidad las fuentes a las que acudirá el enemigo; el lugar al que acude a beber el animal, y puesto que estas a menudo son de identidad no comprobable, o en todo caso, de segunda mano, planificar los engaños será más fácil al existir una mayor predictibilidad de la fuente y accesibilidad a la misma para el enemigo.

Si el OSINT satisface al menos el 80% de las necesidades de información en la mayor parte de los campos, y si internet ha dado lugar a la explosión de la información, sabremos que la mayor parte de lo que el enemigo cree saber

provendrá de direcciones digitales accesibles al público: blogs, vídeos en plataformas populares, redes sociales, foros, ciertos productos de pago…

Los filtros, la objetividad o el pensamiento crítico ayudarán a tamizar la información, pero a menudo llega un punto en el que una información no es corroborable, ni su origen se puede trazar, así que que el único control de veracidad real pasa por los sesgos del analista y de si este decide confiar o no hacerlo.

Imaginemos que existe un reputado foro ruso sobre blindajes en el que ya se publicaron documentos secretos y mediciones concretas, corroboradas y correctas sobre el blindaje de los blindados T-72B, y de repente en plena tensión entre Estados Unidos y Rusia, dicho foro publica documentos aparentemente fidedignos sobre el blindaje del T-90A ¿Deberíamos confiar en esta fuente?

¿Qué ocurre si anónimamente se suministra información falsa a una entidad de renombre, como el *New York Times*, o Bellingcat, que carecen de los filtros de una agencia de inteligencia, y resulta que la célula de OSINT de un ejército da dicha información por buena?

¿Eran creíbles los "*5.000 troops to Venezuela*" de la nota manuscrita de John Bolton?, ¿eran creíbles las informaciones dadas por los espías castristas y los medios de comunicación de EEUU acerca de la inminente invasión de Bahía Cochinos?, ¿o no sería más bien que al igual que en la SGM los estadounidenses estaban emitiendo información falsa, y su auténtico objetivo era desembarcar en otro lugar? En el momento en que sucedieron ambos casos respectivamente, ¿cómo de fiables habríamos juzgado usted o yo los hechos antedichos? El OSINT puede convertirse en un cuchillo de doble filo con facilidad.

Si los Aliados hubieran confiado en la triunfalista propaganda de los metrajes del III Reich, en los que siempre aparecían las unidades mejor equipadas y con la moral más alta, seguramente habrían sobrevalorado la capacidad de combate, el grado de mecanización o la producción industrial germana.

E aquí el gran problema, saber qué es fiable y qué no. En la era de la información, el OSINT ofrece oportunidades de hacer mucho, pero también puede convertirse en un arma de doble filo que facilite enormemente las operaciones de engaño enemigas.

El susodicho carácter abierto del OSINT lo hace fácil de explotar por un adversario habilidoso que sea capaz de prever las preguntas que el enemigo se hará. Se podrá pergeñar una red mediática y efectuar operaciones en foros por parte de usuarios anónimos para compartir información viciada y siempre bajo una apariencia de inocencia y azar, y con la imposibilidad de corroboración. Estas desventajas del OSINT son el fruto de su carácter accesible, dependiente e intermediado.

Todo lo anterior nos lleva a las siguientes consideraciones. De un lado, no se debe esperar a la situación de crisis para que repentinamente emerja toda una red aportando informaciones viciadas y de apariencia valiosa para el enemigo,

hacer contraosint, esto es contrarrestar los esfuerzos OSINT enemigos para impedirlos o usarlos en su contra, requiere ganar prestigio y confianza en la red y esto exige de tiempo y planificación. En su lugar, para ser creíble una red debe construirse desde el principio como una herramienta de engaño para el futuro, ganarse un prestigio para posteriormente aprovecharse de la confianza del analista enemigo.

De otro lado, los servicios de inteligencia y contrainteligencia deberán determinar que información, datos o inteligencia se consideran críticos para nuestros intereses, a fin de enmascarados permanentemente. Por ejemplo, si no deseamos que un país enemigo pueda llevar a cabo un estudio sociológico de Cataluña a través de los perfiles de Facebook, deberemos sostener una permanente campaña de *bots* que simulen perfiles falsos para que de esta forma el producto de inteligencia final sea erróneo.

Por ejemplo, un estado dictatorial centralizado podría emitir datos falsos, o al menos auditarlos para publicar sólo aquello que interese, desde la tasa de fecundidad hasta la capacidad adquisitiva o el funcionamiento tribal. Si todos los datos e informaciones dados por las instituciones públicas se supeditan a la previa inspección de organismos de inteligencia, que formen parte de una estrategia integrada para transmitir en el observador foráneo ciertas ideas y conceptos preestablecidos, estaremos explotando al máximo y desde el principio las posibilidades del contraosint.

CONTRAOSINT

En esencia, la historia reciente nos permite deducir una serie de características comunes y casi omnipresentes en todo producto de inteligencia basado en fuentes abiertas, a su vez dichas características nos permiten comprender su naturaleza, y con ella, su talón de Aquiles.

El OSINT, es relativamente barato, accesible y rápido, lo que le hace cómodo y susceptible de ser usado para extraer numerosa información, pero también para hacer lo contrario, para lo que en general es “engañar”, y es que verter información falsa es muy fácil, aunque como todo, dependiendo de a quien se pretenda confundir hace falta dedicar mayor o menos esfuerzo en un engaño elaborado.

Pero en cualquier caso sabemos que los servicios de inteligencia acuden a ciertas fuentes con una alta probabilidad, y también sabemos que en muchos casos no pueden corroborar su origen, y en su lugar todo se basa en una especie de confianza generada a lo largo del tiempo, al fin y al cabo ¿Los ejércitos comprueban los datos que pueda dar IHS Jane´s? Probablemente no, simplemente se fían de IHS Jane´s.

Como en este mar de información y desinformación es tan fácil caer en el error, y como los mejores analistas y organizaciones buscarán fuentes fiables, preparar con el tiempo redes y ardides para convertirse en la fuente de los

potenciales adversarios es la mejor forma de aprovechar el OSINT adversario en nuestro favor.

Con objetivos políticos u estratégicos generales, no solo para eventos o cuestiones concretas, hemos de estudiar e integrar a gran escala planes planes para aprovechar las debilidades del OSINT, para servir a la política exterior, a la seguridad nacional, a la política de defensa y a otros muchos ámbitos.

Por último, los filtros, y la formación en pensamiento crítico de quienes se dediquen al análisis de inteligencia será fundamental para vivir en un entorno de inteligencia OSINT donde la verdad y el engaño son gemelos difíciles de distinguir.

NOTA SOBRE EL AUTOR:

Yago Rodríguez *es el autor de la investigación acerca de la presencia de armamento español en Yemen y Siria, habiendo trabajado con Armament Research Services.*

REFERENCIAS:

Beschloss, Michael (1991), *The Crisis Years Kennedy and Krushchev 1960-1963,* Harper Collins Publishers, pp. 109.

Carell, Paul (2008), *Tierra Calcinada: La guerra en el frente ruso 1943-1944*, Inèdita Editores, pp. 18-19, 118.

CIA News and Information, *The Office of Strategic Services, Research and Analysis Branch* (consultado en 2019). Disponible en https://www.cia.gov/news-information/featured-story-archive/2010-featured-story-archive/oss-research-and-analysis.html

Fah, Charles (30 de septiembre de 1946), INTELLIGENCE, revista Life, pp. 114.

Healy, Mark (2018), *T-34 Tank: Owner's Workshop Manual*, Haynes, pp. 123.

Mercado, Stephen (2001), *FBIS against the Axis 1941-1945*, Studies in Intelligence 11, Center for the Study of Intelligence CIA, pp. 33-43.

Mercado, Stephen (2004), *Sailing the Sea of OSINT in the Information Age*, Studies in Intelligence Vol. 48, No. 3, Center for the Study of Intelligence CIA, pp. 45, 46, 51.

Prieto del Val, Tomás Fernando (2015), *Engañar, Manipular y Alterar, Actividades Fundamentañes de la Operación "Guardaespaldas",* Instituto de Estudios Estratégicos, pp. 5.

Smith, Timothy (2014), *Overlord/Bodyguard: Intelligence Failure through Adversary Deception,* International Journal of Intelligence, No. 27, pp. 550-568

Steele, Robert (1997), *6th International Conference & Exhibit Global Security & Global Comp*, Vol. 2, Open Source Solutions, pp. 336.

Steele, Robert (2018), *Intelligence at a Cross Roads To Be Or Not To Be*, American Herald Tribune, notas 7 y 57. (Consultado en 2019). Disponible en https://ahtribune.com/us/2314-intelligence-at-a-cross-roads.html

Terrell, Richard (2002), *Deception Plan Bodyguard: Deception Modeling As a Means to Benchmark Risk*, Naval War College, pp. 9-11, 14.