GESI
GRUPO DE ESTUDIOS EN SEGURIDAD INTERNACIONAL
INTERNATIONAL SECURITY STUDIES GROUP

UNIVERSIDAD DE GRANADA

Publicado en *GESI* (http://www.seguridadinternacional.es)

Ene
19
2016

Una revisión del Ciclo de Inteligencia

por Javier Jordán -
Análisis GESI 2/2016

Resumen: Este análisis es la segunda parte de una serie de trabajos de orientación didáctica sobre la Inteligencia en seguridad y defensa. Centra su atención en el estudio crítico de las cuatro fases tradicionales del ciclo de inteligencia: dirección, obtención, elaboración y difusión.

Palabras clave: Inteligencia, Ciclo de Inteligencia, Estudios de Inteligencia, Servicios de Inteligencia.

*****

Continuamos con la serie de materiales didácticos [1] sobre inteligencia para la Seguridad y la Defensa. El ciclo de inteligencia es un modelo denostado, pero útil con precauciones a la hora de representar –de manera ideal– la inteligencia como **proceso**, según la diferenciación clásica de Sherman Kent, que vimos en un documento anterior.

Como sucede a menudo con los modelos, tiene la ventaja hacer fácilmente comprensible un fenómeno complejo, pero el inconveniente de simplificar en exceso la realidad. Esto explica la paradoja de que el ciclo sea criticado una y otra vez por los profesionales de la inteligencia, y que al mismo tiempo continúe siendo un tópico tradicional al iniciarse en este tipo de estudios.

En este documento vamos a combinar ambas perspectivas. Presentaremos el modelo ideal del ciclo de inteligencia y al mismo tiempo señalaremos los desajustes reales que se producen en su aplicación real. A continuación nos detendremos en los aspectos más destacados de cada **conjunto de tareas,** más que fases, pues en seguida veremos que no son del todo secuenciales.

El contraste entre el modelo puro del ciclo de inteligencia y la realidad

Según el modelo ideal, el proceso de inteligencia sigue cuatro etapas:

1. **Dirección**. Los destinatarios de la inteligencia (también llamados por la literatura *consumidores* o, incluso, *clientes*) plantean una serie de demandas a los responsables del servicio de inteligencia. Dependiendo del tipo de inteligencia esos destinatarios pueden ser decisores políticos, altos mandos militares, responsables policiales de alto nivel, etc. En lo concerniente a los servicios de inteligencia estratégica el destinatario por excelencia es el presidente del gobierno, sus asesores, determinados ministros, asesores de estos y altos cargos de sus respectivos ministerios. Las demandas generales de inteligencia son convertidas en

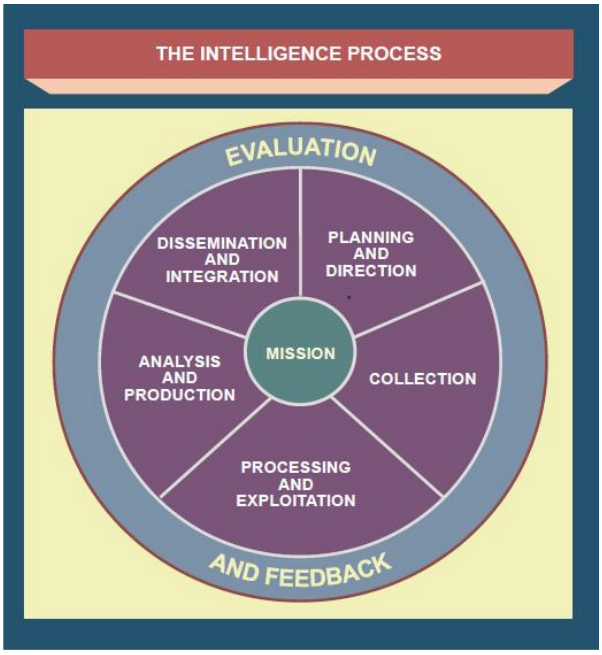
requerimientos específicos por los gestores de alto nivel del servicio, que a partir de ellas asignan tareas, distribuyen recursos y, cuando lo consideran necesario, reforman la estructura orgánica.

2. **Obtención**. Quienes trabajan en la fase de obtención buscan y recopilan información a través de diversos medios. Y, una vez procesada, esa información se entrega a los analistas.
3. **Elaboración**. Los analistas evalúan, analizan, integran e interpretan la información recibida. El conocimiento que se genera a partir de ella se plasma en diversos formatos de entrega de inteligencia.
4. **Difusión**. La inteligencia como producto es entregada a los destinatarios, que pueden pedir aclaraciones sobre la inteligencia recibida o solicitar nuevas demandas, activando de nuevo el ciclo.

Modelo de ciclo de inteligencia según el Centro Nacional de Inteligencia

En la comunidad de inteligencia norteamericana las fases del ciclo reciben otro nombre, y se distingue la fase de obtención de la de procesamiento, por lo que son cinco etapas:

Por su parte, la inteligencia militar norteamericana incluye dos fases más: el feedback de los protagonistas de cada fase y la evaluación del conjunto del proceso.



Fuente: Joint Publication 2-0 [2]

Hasta aquí el planteamiento teórico. Es sencillo, posee lógica interna y resulta fácil de comprender y recordar. También se corresponde en cierta medida con la organización interna de los servicios de inteligencia, que dividen sus funciones de manera acorde con las etapas del ciclo (Clark, 2013 [3]). De ahí su valor pedagógico como primera aproximación a la inteligencia como proceso, lo que explica que se siga estudiando a pesar de sus limitaciones.

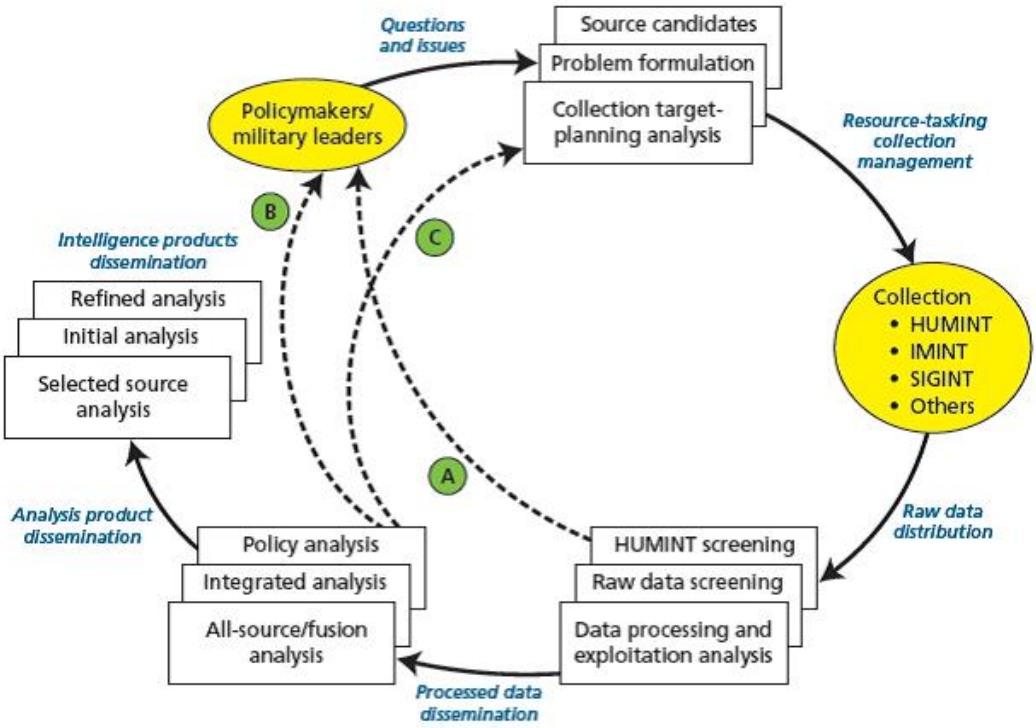
Ahora bien, desde hace años la literatura especializada viene llamando la atención sobre las **debilidades del ciclo** a la hora de explicar el **proceso real de producción de inteligencia**. Arthur S. Hulnick (2006) [4] ofrece una revisión sistemática de las incongruencias existentes entre el modelo puro y lo que sucede en la vida real, a partir de su experiencia en la comunidad de inteligencia norteamericana. Una opinión que según otras fuentes puede aplicarse al funcionamiento del sistema en otros países. Siguiendo los pasos del ciclo ideal el contraste sería el siguiente:

- **Dirección**. Por falta de tiempo, de interés o de saturación de su propia agenda, los decisores políticos no siempre señalan objetivos claros, específicos y continuos para que los responsables de los servicios de inteligencia continúen el ciclo. Con bastante frecuencia los *policy-makers* asumen que los servicios les avisarán de los problemas antes de que sucedan, o que éstos complementarán a través de sus propias fuentes y análisis las noticias que acaparan las portadas de los medios de comunicación. Por ello, son en realidad los responsables técnicos de los servicios (*intelligence managers*, en la literatura anglosajona), quienes a menudo impulsan el proceso, y lo hacen a partir de la vigilancia del entorno y de los vacíos en información que encuentran dentro de sus propias líneas de trabajo.
- **Obtención**. Como veremos un poco más adelante, el desarrollo de sistemas de obtención requiere espacios dilatados de tiempo. En consecuencia es arriesgado esperar a que lleguen indicaciones concretas por parte de los responsables políticos para ponerlos en marcha. En caso de recibir tales inputs los servicios sí que focalizarán su atención sobre aspectos más específicos pero lo más probable es que lo hagan sobre la base de lo que ya están trabajando.
- **Elaboración**. Los analistas no dependen en todos los casos de la información que les llega desde las unidades de obtención. Muchas veces pueden preparar un informe a partir de bases de datos alimentadas durante años. Cuando llega nueva información es puesta en perspectiva con información y análisis previos. Al mismo tiempo, en caso de surgir contradicciones o de

crearse nuevas necesidades informativas, los analistas pueden solicitar a los órganos de Obtención nuevas informaciones brutas sin necesidad de trasladar su análisis al decisor político para que éste a su vez planté una nueva demanda. Por tanto, más que dos etapas secuenciales, Obtención y Elaboración discurren de manera paralela e interactiva. Y de ambos procesos pueden producirse envíos a la fase de difusión.

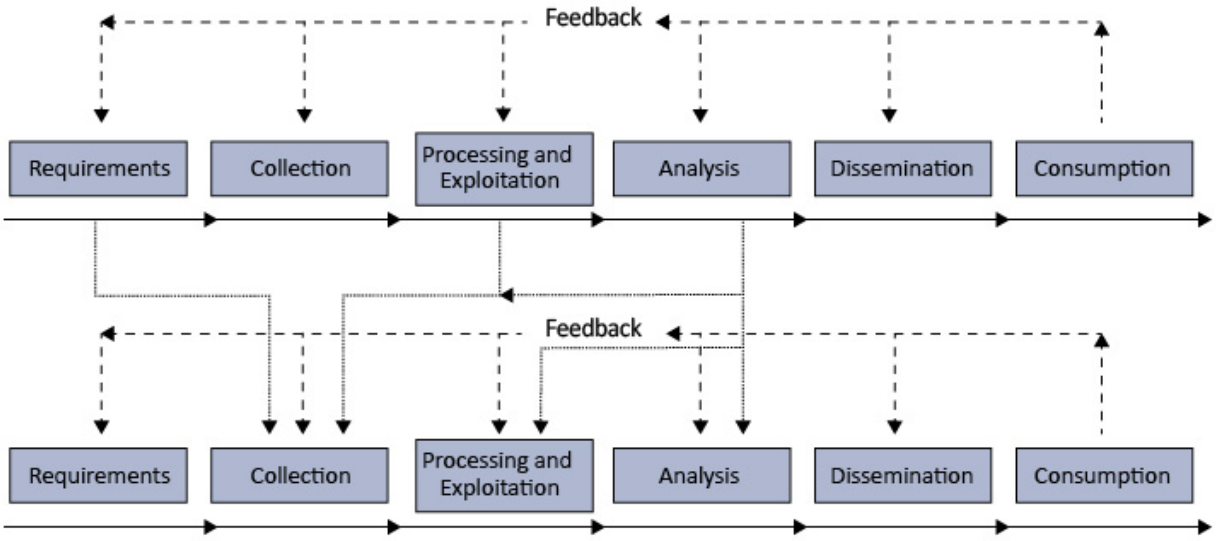
- **Difusión**. Es decir, además de los análisis que –según el ciclo ideal– se transmitirían al destinatario en la fase de Difusión, también la información bruta –especialmente en situaciones de crisis, como señalamos en el documento anterior [1]– puede abrirse camino directamente hasta llegar a las manos de los consumidores sin pasar antes por los analistas. Es una opción que plantea inconvenientes, por el déficit de evaluación e integración que supone, pero puede ser considerada oportuna por los altos responsables del servicio a tenor de las circunstancias, o demandada explícitamente por los decisores políticos. Por otra parte, no todos los análisis preparados en la fase de Elaboración llegan a los consumidores. En Estados Unidos, un indicador a la hora de valorar a un analista es el número de informes con inteligencia actual que son incluidos en el President Daily Brief. Decenas de ellos son relegados y pasan a formar parte de la base interna del servicio, sin mayor trascendencia. Lo mismo sucede con ciertos estudios en profundidad sobre cuestiones muy específicas. Cuando Robert M. Gates fue nombrado director de la CIA en 1991 ordenó que cada analista escribiera al menos dos análisis en profundidad al año como una forma de combatir la superficialidad a la que puede llevar el énfasis en la inteligencia actual. En efecto, se redactaron cinco mil informes de ese tipo en un año. Pero Hulnick (2006: 966) [4] se pregunta sarcásticamente cuántos de ellos fueron leídos por los destinatarios. Por último, aunque estrictamente no forma parte del ciclo, cabe esperar que la inteligencia una vez que llega al responsable político, sea tenida en cuenta en la toma de decisiones. La realidad, sin embargo, es que muchas veces el gobernante ya tiene clara cuál va a ser su decisión y, si la inteligencia que no la respalda corre el riesgo de ser simplemente soslayada (esta cuestión ya la tratamos en el documento anterior [1], en el epígrafe inteligencia y toma de decisiones).

En consecuencia, este gráfico de Gregory F. Treverton, y C. Bryan Gabbard (2008:4) [5] ofrecería una imagen más realista del ciclo:



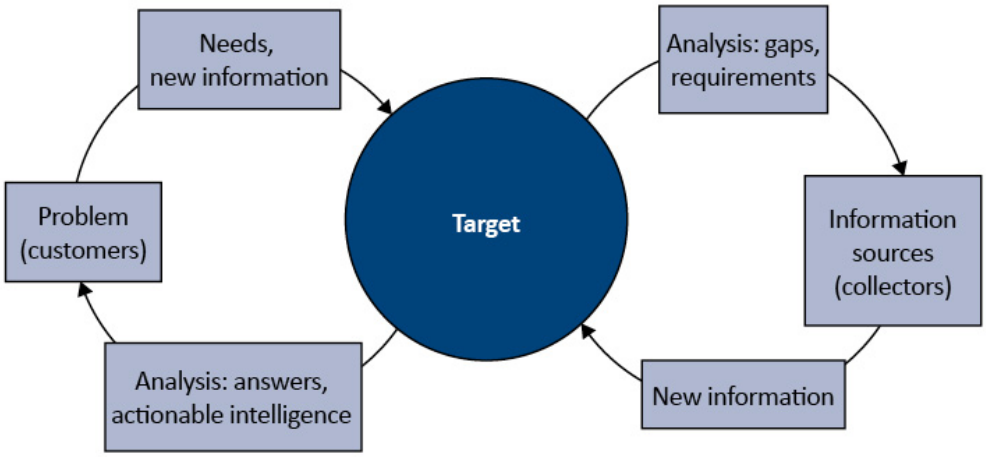
Las líneas con puntos del gráfico señalan la existencia de atajos entre una y otra fase: (A) el tránsito de informaciones no analizadas desde la fase de Obtención al decisor político (o militar en caso de que el ciclo describa el funcionamiento de ese tipo de inteligencia); (C) el de indicaciones de los analistas a la del Planeamiento previo a la Obtención; y (B) el que comunica la fase de Elaboración con los consumidores, sin pasar plenamente por selección y refinamiento de los análisis en la fase de Difusión.

Por su parte, Lowenthal (2012) [6] propone un modelo algo más complejo pero también ajustado a la realidad, pues como han advertido por ejemplo Michael McConnell (antiguo Director Nacional de Inteligencia en Estados Unidos) y el académico Michael Herman, el ciclo está compuesto por una suma de *feedbacks*. A lo largo del ciclo surgen incidencias (nuevas necesidades de obtención, ambigüedades en el procesamiento, resultados de análisis, cambios en los requerimientos) que ponen en marcha un nuevo proceso, e incluso un tercero, cuarto… De modo que los estratos que aparecen en la figura inferior podrían multiplicarse por varios.



Proceso multi-estratos de Mark Lowenthal

Finalmente, Robert M. Clark (2013) [3], ofrece una visión alternativa con su modelo de Target-Centric Intelligence (proceso de inteligencia centrado en el objetivo). Según él, la finalidad del proceso consiste en construir una imagen compartida del objetivo –del asunto de interés de la inteligencia. Una imagen de la que todos los participantes en el proceso puedan extraer elementos necesarios para su trabajo y a la que todos puedan contribuir con sus recursos y conocimientos con el fin de obtener un cuadro más ajustado de la realidad. No se trata de un proceso lineal ni cíclico, aunque contenga procesos de retroalimentación. Es más bien un trabajo en red, un proceso social, donde todos los participantes centran su atención en el objetivo.



Dichos participantes son, por un lado, los consumidores de inteligencia que al encontrarse con un problema se preguntan qué es lo que se conoce sobre el objetivo asociado a dicho problema (la imagen actual del objetivo) e identifican la información que necesitan. También participan en el proceso los analistas, que trabajando con los encargados de obtención que comparten su misma visión del objetivo, traducen sus necesidades en vacíos (*information gaps*) y requerimientos de información. Sin embargo, y a diferencia del ciclo clásico, este modelo no concede todo el protagonismo de la elaboración de la inteligencia a los analistas, sino que **introduce en el proceso de elaboración a los consumidores y a quienes proporcionan la información**. Ambos poseen sus propias intuiciones y valoraciones en lo que respecta al objetivo, y ambos tratan de incluirlas en la imagen final sobre él. Aun así, en este modelo los analistas también poseen una singular importancia pues se convierten en los principales gestores del proceso: son ellos quienes primero crean y mantienen la imagen del objetivo, quienes consultan y estimulan las necesidades de los consumidores y las traducen en requerimientos de información, quienes aceptan nuevas informaciones, las filtran y las incorporan a la imagen compartida, y quienes extraen inteligencia operativa de esa imagen del objetivo que pasan a los consumidores. A su vez, los consumidores y quienes obtienen la información observan la marcha del proceso y tienen por tanto oportunidad de intervenir en él.

La propuesta de Clark es interesante pero requiere dos matizaciones. En primer lugar, parece estar orientado fundamentalmente a la inteligencia operativa, donde los consumidores serían, por ejemplo, los mandos de una fuerza militar o policial. De hecho, los casos con los que ilustra su modelo responden a ese perfil, y, al mismo tiempo, la descripción del modelo guarda una estrecha relación con los cambios introducidos por el General McChrystal y su equipo en el Joint Special Operations Command [7] para enfrentarse con más eficacia a las insurgencias en Irak y Afganistán(enlace a revista Defensa). En segundo lugar, el modelo da la impresión de ser una propuesta a implementar para mejorar los procesos, antes que una descripción acertada de cómo son esos procesos en realidad. En ese sentido, una comparación de los modelos [8] de Clark y de Lowenthal aplicada a un caso histórico (la gestión norteamericana de la crisis de los misiles de Cuba) concede mayor valor descriptivo-explicativo al segundo de ellos.

Una vez advertidos de las limitaciones reales del ciclo de inteligencia, vamos examinar los aspectos más destacados de cada una de sus fases. Lo haremos siguiendo las cuatro etapas del modelo español.

Fase de Dirección

Hay tres cuestiones a resaltar en esta fase: los protagonistas, el contenido de los objetivos y las prioridades dentro de ellos.

En teoría los **protagonistas** de esta fase son los destinatarios de la inteligencia, de modo que lo lógico sería que las prioridades de inteligencia coincidan con las prioridades de los decisores políticos. La idea que subyace bajo este planteamiento es que dichos decisores han sopesado previamente cuáles son sus prioridades y actúan siguiendo un plan estratégico. Sin embargo, la realidad no siempre coincide con esa premisa. En la práctica:

- Los decisores políticos pueden carecer de una lista clara y real de prioridades (por ejemplo, en materia de acción exterior de su Estado). En tal caso, difícilmente podrán trasladarla al servicio de inteligencia. Ello puede deberse a falta de tiempo, urgencia de otras prioridades, falta de pensamiento estratégico, ausencia de interés, etc.
- En caso de haber establecido prioridades políticas que atañan potencialmente a la inteligencia, puede que no den suficiente importancia al rol que desempeñan los servicios a la hora de alcanzar tales objetivos y, en consecuencia, que no trasladen a éstos de manera explícita y formal sus requerimientos. Mark Lowenthal recoge la anécdota de un Secretario de Defensa al que preguntaron si en algún momento pensó en dar a los responsables de inteligencia del Pentágono instrucciones precisas sobre lo que trabajar. A lo que respondió: “No, asumí que sabían lo que yo estaba trabajando”.

Por ello, no es infrecuente que sean los propios servicios quienes tomen la iniciativa y pasen cuestionarios de requerimientos a los *policy-makers* o propongan un primer borrador con las líneas de trabajo a desarrollar.

Una vez establecida, la lista de requerimientos se traduce en un documento programático. En España se trata de la **Directiva Nacional de Inteligencia**. Es elaborada anualmente por la Comisión Delegada del Gobierno para Asuntos de Inteligencia, aprobada por el Presidente del Gobierno, y seguida y evaluada por dicha Comisión. Por su naturaleza la Directiva es de carácter secreto.

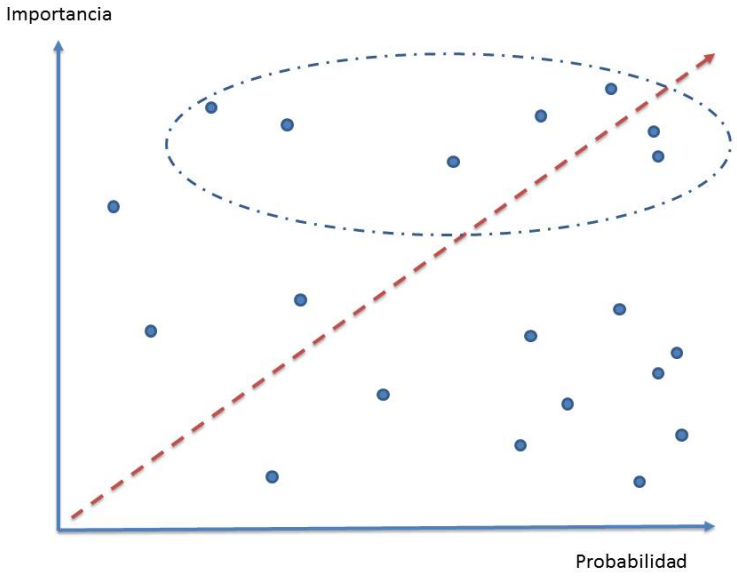
En Estados Unidos el Consejo de Seguridad Nacional es quien determina la política y los objetivos de inteligencia. Y compete al Director Nacional de Inteligencia asignar dentro de la comunidad los objetivos prioritarios para cada uno de los organismos de inteligencia que la componen. El documento que explicita dichos objetivos y prioridades, y que en cierto modo sería el equivalente de la Directiva Nacional de Inteligencia española, es el National Intelligence Priorities Framework (NIPF) [9]. Su contenido también es secreto y se renueva periódicamente (en principio, cada seis meses).

Los plazos de renovación de estos documentos (anualmente en el modelo español, dos veces al año en el norteamericano), pueden parecer los propios de una gran burocracia, pero lo cierto es que el dinamismo de las relaciones internacionales –y más en tiempos tan volátiles como los que estamos viviendo– pone en peligro la vigencia de las prioridades establecidas. Por ello Mark Lowenthal (2012) [6] recomienda un adecuado grado de flexibilidad en las actualizaciones de los objetivos y prioridades. Un exceso de alteraciones en cortos periodos de tiempo crearía serias disfunciones en el trabajo de los servicios, mientras que una actitud de resistencia al cambio desconectaría la inteligencia del proceso político.

En cuanto al **contenido de los objetivos**, ya señalamos en el documento previo [1] que los servicios de inteligencia asumen por lo general un enfoque integral de la seguridad, prestando atención a las dimensiones política, militar, económica, social, cibernética, etc. Más allá de esto cada país tiene sus

propias especificidades en lo relativo a intereses, riesgos, amenazas y oportunidades, condicionadas por su historia, geografía, poder relativo y mayor o menor presencia global. A partir de ellas se establecen los objetivos concretos. Estos no hacen referencia sólo a países hostiles. En la práctica también afectan a países amigos y aliados, pues aunque en una esfera exista cooperación (por ejemplo, en el seno de la OTAN), en otras –como la económica– esos mismos países son competidores. Al mismo tiempo, los Estados también desean conocer cuáles son las intenciones de política exterior de sus aliados en asuntos que afectan a intereses propios (por ejemplo, para Washington, la actitud de Francia frente a Rusia en el contexto de la crisis de Ucrania o tras los atentados de París). Por lo que las escuchas de la NSA norteamericana a la canciller Merkel [10] no resultan en el fondo tan sorprendentes… A pesar de ello, el Presidente Obama se comprometió tras el escándalo a reducir las escuchas de gobiernos amigos. Reducir, no abandonar por completo. Pues, Washington ha seguido manteniendo bajo vigilancia estrecha a ciertos aliados. En particular al gobierno israelí de Benjamin Netanyahu [11].

Por otro lado, la limitación de recursos obliga a **establecer prioridades entre los objetivos.** Esto supone que los últimos de la lista quedan menos cubiertos y que en ellos haya más 'sombras radar'. Mark Lowenthal [6] señala como como **criterios** la **importancia** y la **probabilidad** de que la amenaza o la oportunidad se presenten. El gráfico inferior representa los dos criterios con una tendencia creciente. Los puntos comprendidos en la elipse ocuparían los primeros puestos en el orden de objetivos.



Como puede observarse, el criterio de probabilidad no es tan relevante como el de importancia. Puede haber cuestiones altamente improbables –por ejemplo, un ataque militar a la integridad territorial de España– que por la severidad de sus consecuencias sean objeto de vigilancia permanente por parte de los servicios de inteligencia nacionales. Por el contrario, hay asuntos muy probables –choques fronterizos armados entre India y Pakistán en Cachemira– cuya importancia para España es sin embargo menor y por ello requiere menos prioridad en la lista de objetivos. Finalmente hay una serie de objetivos que por su importancia y probabilidad tienen asegurados los primeros puestos de la agenda. En el caso de nuestro país, es de suponer que el terrorismo yihadista, las amenazas a la ciberseguridad o las actividades de crimen organizado ocupen ese lugar.

La selección de objetivos y prioridades, y la asignación de recursos que de ello se deriva, conlleva riesgos inevitables. Los errores de visión y de cálculo en la fase de Dirección se traducen en vacíos de inteligencia sobre áreas de interés real pero no advertido, lo cual incrementa el riesgo de que se produzcan sorpresas estratégicas. También afecta a la capacidad de respuesta de los servicios una vez que se ha constatado la importancia de esos objetivos. Desarrollar capacidades de Obtención –especialmente de HUMINT– y de Análisis requiere periodos dilatados de tiempo, lo cual genera ventanas de vulnerabilidad en términos de inteligencia.

Finalmente, una vez que los consumidores de inteligencia establecen los requerimientos, la dirección de los servicios lleva a cabo cuatro acciones fundamentales que consisten en (Miguel Ángel Esteban y Andrea V. Carvalho (2012: 141) [12]:

- Fijar los objetivos generales y operacionales a partir de los requerimientos.
- Decidir qué información se ha de obtener y a través de qué sistemas.
- Organizar y destinar los recursos necesarios para obtener, procesar y analizar la información que se convertirá en inteligencia.
- Determinar las responsabilidades y procedimientos de dirección y acción orientados a la planificación, motivación, mando, control y coordinación dentro del servicio.

Fase de Obtención

Como ya hemos señalado, el modelo español incluye tanto la **obtención** propiamente dicha de datos e información bruta, como la sub-fase de **procesamiento y explotación**. Esta consiste en convertir los datos captados por los sistemas de obtención técnicos en información utilizable por los analistas. Dicho procesamiento y explotación también entraña una evaluación de la fiabilidad de la fuente y de la información, y un pre-análisis de la información obtenida, anterior a la siguiente fase de Elaboración.

Como ya se ha señalado, la fase de Obtención debe ir precedida del diseño de una **estrategia** basada en el objeto de interés y en los vacíos informativos que dificultan el análisis sobre él. Los protagonistas de la estrategia son en buena medida los analistas de inteligencia. Por ello el inicio de la fase de Obtención recibe inputs, además de la fase de Dirección, de la de Elaboración (de ahí las incongruencias en el ciclo de inteligencia canónico que advertimos al comienzo de este documento).

La fase de Obtención es también la más llamativa, la que ha dado lugar a un género propio de novelas y películas. Es donde se aplican los avances tecnológicos. Y –junto a las operaciones encubiertas– es quizás la más polémica, la que de cuando en cuando provoca incidentes diplomáticos y grandes escándalos políticos. Pero más allá de las controversias que genera, es una fase enormemente compleja. Veamos de manera esquemática cuáles son los desafíos a los que se enfrenta (Lowenthal, 2012 [6]):

- **Limitaciones presupuestarias**. La fase de Obtención es con diferencia la más costosa de todo el proceso de inteligencia. Y la limitación de recursos lleva a que ciertas capacidades (por ejemplo, satélites de observación terrestre o aviones no tripulados de largo alcance, tipo Global Hawk [13]) queden completamente fuera de la ecuación o, al menos severamente reducidos, para muchos países. Esto se aplica sobre todo a medios tecnológicos (IMINT, SIGINT, MASINT, etc), pero también afecta a los recursos humanos y a su despliegue internacional. El hecho de que la información sea cara de obtener es una de las principales razones por las que la fase de Dirección restringe y ordena la prioridad de los requerimientos de inteligencia.
- **Cuello de botella en el procesamiento**. El volumen de datos e informaciones captadas por los diversos sistemas de obtención es de tal magnitud que sólo una parte puede ser procesado y enviado a los analistas. Pensemos en los miles de millones de comunicaciones electrónicas que cada día intercepta la NSA. Aunque se utilicen diccionarios con palabras clave de búsqueda, posteriormente sus contenidos deben ser traducidos al idioma de los analistas. En otras ocasiones han de ser además descifrados. Igualmente, los miles de horas de grabación de los drones estratégicos y operacionales requieren cientos de analistas de imágenes, antes de que la información procedente de ellos pueda ser de utilidad para los analistas de inteligencia. Esto supone un coste económico añadido a los caros sistemas de obtención y limita comprensiblemente la disponibilidad real de este tipo de fuentes de información [14]. El filtro que

establece la sub-fase de procesamiento, obliga a plantearse la conveniencia de captar el máximo de información –especialmente a través de sistemas técnicos. Cuanta más información, más probabilidades de que entre lo captado haya piezas acertadas del puzle, pero también menos probabilidades de que entre lo procesado se encuentre la información correcta, a no ser que se focalicen de manera precisa los sistemas de obtención o que se dediquen ingentes cantidades de dinero al procesamiento y explotación. Por ello, la conclusión obvia es que **más cantidad de información no garantiza mayor calidad de inteligencia**.

- **Negación de acceso/Engaño**. El actor sobre el que se trata de obtener información (sea un Estado o una entidad no estatal) puede tratar de protegerse, bien negando el acceso (por ejemplo, cifrandolas comunicaciones) o bien proporcionando información falsa o engañosa. Uno de los ejemplos históricos más impresionantes fue la operación Fortitude [15], previa al desembarco de Normandía. A través de diversas acciones, que incluyeron la creación de un grupo de ejército ficticio mandado por el General George S. Patton y desplegado supuestamente en el sudeste de Inglaterra, los aliados consiguieron engañar a los alemanes sobre el auténtico lugar del desembarco. El peligro de negación o de engaño será mayor cuanto más conozca el objetivo de inteligencia los sistemas de obtención que se van a aplicar contra él (Clark, 2013 [3]).
- **Problemas de comunicación, coordinación y cooperación dentro de la propia comunidad de inteligencia**. Pueden obedecer a distintas razones: rivalidades corporativas, miedo a poner en peligro las fuentes o a comprometer –o a 'regalar' a otros el trabajo de– investigaciones en curso, arquitectura institucional que no facilite la colaboración, pérdidas y distorsiones de información inintencionadas resultado de pasar por varios canales institucionales (que Robert M. Clark [3] compara a la entropía de la termodinámica), etc. Se trata de deficiencias que pueden traducirse en sorpresas estratégicas, y lo más dramático: provocadas no por falta de información sino porque ésta se encontraba dispersa e inaccesible para los analistas que debían haberla interpretado correctamente.

Son numerosos los sistemas utilizados para la obtención de información, y su adecuación depende del objeto y el tipo de información al que se quiera acceder. Rara vez es suficiente con uno solo de ellos. Y en todos los casos es muy recomendable –por no decir sencillamente imprescindible– contrastar la información con varias fuentes. En Estados Unidos existen agencias especializadas en un sistema concreto de Obtención, pero hay tres en la comunidad (CIA, la DIA –inteligencia militar– y la INR –del Departamento de Estado) que son *all sources*. En España el CNI y el CIFAS también pertenecen a esta categoría.

A continuación ofrecemos una clasificación didáctica y, por tanto, simplificada, de los medios de obtención. Al mismo tiempo, exponemos también de manera esquemática los pros y contras de cada uno de ellos (Lowenthal, 2012 [6]):

Inteligencia de Imágenes (IMINT) y de Firmas (MASINT)

Incluye:

- Imágenes ópticas: obtenidas a través de aviones de reconocimiento tripulados y no tripulados (*Unmanned Aerial Vehicle*, UAV/*Remotte Control Vehicle*, RPV, o en el lenguaje coloquial, drones), satélites de observación terrestre a relativa baja altura (200-1.000 km), imágenes de costa o de otros buques obtenidas de manera discreta por submarinos, etc
- Imágenes infrarrojas (IR), que permiten la observación nocturna y la detección de fuentes de calor, como personas o motores.

- Captación de otro tipo de radiaciones (MASINT), algunas visibles y otras no, pero que permiten obtener información relevante. Un medio por ejemplo son los satélites radar, los sistemas de detección de explosiones nucleares o los sistemas de escucha submarina. Algunas clasificaciones también incluyen, justificadamente, las imágenes infrarrojas en el MASINT.
- Ambos tipos de fuentes (IMINT y MASINT, y en ocasiones también las otras 'ints'), más otras disciplinas como la topografía y la geodesia, nutren la inteligencia Geoespacial (GEOINT) dedicada a obtener, procesar y explotar información relacionada con la actividad humana sobre la Tierra.

Ventajas:

- Una gran cantidad de objetivos son observables a través de estos medios (campos de entrenamiento, ejercicios militares, bases, etc).
- Las imágenes tienen una gran fuerza sobre el decisor político y el público en general. Recuérdese la importancia que tuvieron las imágenes durante la crisis de los misiles en Cuba [16] y cómo contribuyeron a que Estados Unidos lograra el respaldo de aliados clave como Gran Bretaña y Francia.
- En la mayoría de las ocasiones pueden obtenerse a distancia, sin riesgo para los recursos humanos que desempeñan esa tarea. Una tendencia al alza por los avances en materia de drones [17].
- Cada vez más las imágenes se transmiten en tiempo real.
- Son de gran utilidad para algunos tipos de inteligencia (como, por ejemplo, asuntos militares) pero no tanto en otras áreas.
- En algunos casos (cuando se combinan con datos de elevación) las imágenes aéreas pueden ser utilizadas para crear simulaciones tridimensionales y ensayar operaciones militares o clandestinas sobre un escenario real. El propio Google Earth ofrece un rudimentario simulador de vuelo [18] que utiliza este tipo de información.

Imágenes satélite presentadas como prueba del incremento de la presencia militar rusa en Siria previa al inicio de los bombardeos a finales de ese mismo mes de septiembre de 2015. En este caso proceden además de fuentes abiertas (OSINT)

Limitaciones:

- Al igual que sucede con los otros tipos de fuentes, necesitan ser complementadas con otros sistemas de obtención. Por ejemplo, pueden ofrecer una imagen nítida de una fábrica pero desconocerse para qué se utiliza. Ese fue el gran fiasco de las imágenes presentadas por el

Secretario de Estado Colin Powell ante el Consejo de Seguridad de Naciones Unidas [19] en febrero de 2002. Existió cierto paralelismo entre aquella presentación, que trataba de demostrar la existencia de armas químicas en Irak, y la ofrecida en medio de la crisis de los misiles de Cuba en 1961. Con la salvedad de que la inteligencia de 2002 era gravemente imperfecta y que las imágenes no constituían una prueba evidente de la existencia de tales armas. El IMINT permite ver 'cosas' pero no siempre captar su 'significado'. Por eso algunos lo han comparado con la Arqueología.

- De este modo, la aparente fuerza de las evidencias obtenidas por IMINT constituye al mismo tiempo una debilidad. Puede darse demasiada verosimilitud a la inteligencia respaldada por IMINT, desechando –quizás de forma apresurada– informaciones que la contradigan y basando en ella decisiones mal informadas.
- Todavía no son útiles para identificar a personas individuales, aunque serán capaces de hacerlo [20] en pocos años.
- Las imágenes necesitan la interpretación de técnicos que ven detalles que escapan al personal no entrenado (recuérdese la pirámide informacional: las imágenes son datos). Esto obliga a que los analistas, los decisores políticos y, en casos excepcionales, la opinión pública, dependan de la opinión de esos expertos.
- Como ya se ha señalado antes, muchos de estos medios suponen un coste muy elevado de adquisición y mantenimiento. Por ejemplo, el sistema de satélites de observación terrestre Helios II, liderado por Francia y en el que participa España junto a otros países, asciende a 1.800 millones de euros, aunque la proporción del gasto español es sustancialmente menor.

Inteligencia de señales (SIGINT)

- Captación de comunicaciones emitidas a través de diversos medios: radio, teléfonos, fax, internet. Es también conocida como COMINT.
- Captación de señales electrónicas (ELINT), que no impliquen comunicación pero que sean relevantes para la inteligencia (por ejemplo emisiones de radar o sonar).
- Los medios de obtención de SIGINT son muy variados: satélites, aviones, buques, estaciones de tierra, etc. Y es habitual que haya plataformas que operen simultáneamente varios medios (IMINT y SIGINT).
- Aunque en las taxonomías clásicas no se incluye como SIGINT, la ciber-obtención (más conocido como ciber-espionaje) es un sistema en auge por motivos obvios. La dependencia cada vez mayor en los sistemas informáticos a la hora de almacenar, gestionar y trabajar con información; y las ventajas que ofrece esta posibilidad para un servicio: obtener grandes cantidades de información sensible –que impresas tendrían que ser transportadas en camiones– de manera discreta, a distancia y muchas veces instantánea. La brecha en la Oficina de Gestión de Personal de Estados Unidos [21], dada a conocer en 2015 y en la que se robó desde China información de millones de empleados del gobierno es una buena muestra de ello. La Agencia de Seguridad Nacional norteamericana ofrece carreras especializadas [22] en este sentido. Y los servicios chinos también se han labrado la reputación de ser muy agresivos [23] al respecto. Entre otras acciones se sospecha que su avión de combate de última generación J-31, debe mucho al ciber-robo de datos del F-35 norteamericano [24].

Ventajas:

- La interceptación de las comunicaciones personales permite conocer las ideas, planes, intenciones y características de los objetivos humanos.
- En el terreno militar, permite establecer el orden de batalla electrónico del adversario. Es decir, los medios de que dispone, su organización y localización. También advertir cambios en pautas establecidas que alerten por ejemplo de un incremento de su actividad.

- Es una información que se obtiene la mayoría de veces a distancia, con escasos riesgos personales

Limitaciones:

- Para que funcione, el objetivo humano ha de comunicarse a través de sistemas electrónicos. Si renuncia a ellos, la obtención por SIGINT resulta estéril. Conviene recordar la escasa utilidad de este tipo de fuentes a la hora de localizar a Bin Laden y de confirmar que era el habitante desconocido de la casa de Abbottabad antes de lanzar la operación contra él. No obstante, evitar las comunicaciones electrónicas para protegerse de la SIGINT entraña un coste elevado a la hora de dirigir una organización global [25].
- En una línea similar, los objetivos de la inteligencia pueden seguir una férrea y exitosa práctica de control de emisiones (EMCON, en sus siglas inglesas) que dificulte seriamente su seguimiento. Puede ir desde el conocido silencio radio o de radar, hasta emplear líneas de comunicación terrestre, en lugar de radios tácticas, como por ejemplo hizo Hizbollah en la emboscada que dio lugar a la guerra de El Líbano en el verano de 2006.
- Como ya se ha señalado anteriormente, la SIGINT genera un volumen abrumador de información, prácticamente imposible de procesar en su totalidad y menos aún en tiempo preciso, a no ser que se focalice de manera muy detallada la búsqueda (por ejemplo, interceptando un determinado número de teléfono o una cuenta de correo concreta).
- En algunos casos las comunicaciones pueden estar fuertemente cifradas, lo cual obliga a recurrir a otro género propio de la inteligencia que consiste en obtener o descifrar los códigos del adversario. Uno de los ejemplos más conocidos a este respecto fue el desarrollo y explotación de Ultra durante la Segunda Guerra Mundial. Mucho es lo que se ha debatido [26] sobre su impacto real en la marcha de la guerra.
- Igualmente se puede sortear, o al menos poner dificultades serias dificultades, mediante otras técnicas: cambio frecuente de tarjetas de teléfono móvil prepago, empleo de cibercafés, comunicaciones a través de chats en foros inopinados (de contactos o de videojuegos) utilizando un código preestablecido, etc.
- Es frecuente que las comunicaciones deban ser traducidas al idioma de los analistas, lo cual requiere contar con traductores suficientes –y acreditados– para poder procesar las informaciones captadas. Esto puede plantear un problema serio cuando se trata de idiomas poco comunes.
- Vulnera el derecho a la privacidad de los ciudadanos, por lo que en los sistemas democráticos el empleo de estos medios dentro del propios país se encuentra sujeto a las lógicas limitaciones legales
- Al igual que sucede con el IMINT, los sistemas de SIGINT entrañan un coste muy elevado. Por ejemplo, durante años se ha comentado que el avión más caro del Ejército del Aire español era un Boeign 707 equipado y especializado en tareas SIGINT [27] (ya dado de baja).

Inteligencia humana (HUMINT)

Es la obtenida a través de diferentes tipos de personas:

- Funcionarios propios: diplomáticos, agregados militares, funcionarios de inteligencia en las embajadas (en Estados Unidos conocidos como *case officers*) o sin cobertura oficial.
- Infiltrados. Personas al servicio de una agencia de inteligencia que se introducen en un objetivo de interés: grupo terrorista, de narcotráfico, en la administración de un Estado extranjero, etc.
- Informantes. En este caso no hay un esfuerzo previo de infiltración, sino que se recluta a personas que ya tenían relación o forman parte del objetivo de la inteligencia.
- Agentes dobles que aparentemente trabajan para un servicio pero en realidad pasan información al rival.
- En ocasiones el reclutamiento del informador o del agente doble se produce a iniciativa del individuo en cuestión (los llamados ‘walk-ins’) que ofrece sus servicios por resentimiento,

ideología o dinero al servicio de inteligencia. Hay varios casos muy conocidos que pertenecen a esta categoría: los norteamericanos Aldrich Ames [28] y Robert Hanssem [29] al servicio de los soviéticos/rusos, Johathan Polard [30] también estadounidense al servicio de la inteligencia israelí, y Oleg Penkovsky [31] del lado soviético al servicio de los norteamericanos y británicos.

- Desertores.
- Refugiados o inmigrantes que han desarrollado trabajos de interés en sus lugares de origen y a los que se solicita información al respecto.
- Prisioneros de guerra
- Ciudadanos del propio país que residen en el país objetivo o que en viajes profesionales contactan con personas clave (científicos, empresarios, políticos, etc.)

Ventajas:

- Puede ofrecer informaciones de gran valor difícilmente obtenibles por otros medios. Sobre todo aquellas que hacen referencia a las verdaderas intenciones del otro.
- Además de proporcionar información puede ser utilizada como instrumento para influir o engañar al rival con informaciones falseadas
- Resulta de gran ayuda en las tareas de contrainteligencia, si se consigue penetrar otro servicio mediante HUMINT

Limitaciones:

- El desarrollo de HUMINT requiere periodos dilatados de tiempo. En el caso de los informantes hay que identificar a las personas que tienen acceso a información de interés, evaluarlas, reclutarlas y gestionarlas. Cuando se trata de infiltrados hay que fabricar además una cobertura y un perfil de interés para que la organización que se desea infiltrar los reclute y acepte.
- Requiere proximidad física, lo cual puede entrañar grave peligro tanto para la fuente humana como para su controlador dentro del servicio. La CIA sufrió uno de los atentados más duros de su historia en Afganistán en 2009 al reunir a varios de sus miembros con el agente triple Humam Al-Balawi [32].
- Por motivos de seguridad las comunicaciones entre el infiltrado y sus controladores no suelen producirse en tiempo real.
- En caso de ser descubierto, el espionaje humano puede dar lugar a un incidente diplomático, algo menos frecuente cuando se trata de otro tipo de sistemas de obtención.
- A veces supone trabajar con 'lo peor de cada casa' –traficantes de armas, criminales, terroristas, etc– pues por su posición en las *dark networks* les da acceso a información de gran valor. Esto plantea problemas éticos y legales.
- La información puede ser distorsionada voluntaria o involuntariamente por la fuente. Involuntariamente por prejuicios personales o su deseo de recibir más atención. Voluntariamente porque ha sido descubierto y doblado por el otro, convirtiéndose así en un instrumento de engaño. También puede inventarse la información para obtener beneficios a cambio. Este fue el caso de *Curveball*, el supuesto desertor que proporcionó información falsa [33] a la inteligencia alemana sobre el programa de armas biológicas de Sadam Hussein, y que fue una de las principales fuentes sobre la que se basó la inteligencia norteamericana para construir el caso que justificó la guerra de Irak de 2003. Por ese motivo, conviene escrutar con especial énfasis la información proveniente de desertores y refugiados, pues puede estar contaminada por las razones políticas o económicas que les forzaron a abandonar su país.
- Pero, al mismo tiempo, el temor a ser engañados puede llevar a que los servicios de inteligencia rechacen una fuente fidedigna. Mark Lowenthal compara la gestión de fuentes humanas a mantener el equilibro sobre una cuerda en el vacío.
- Los informes que los analistas reciben a través de este tipo de fuentes suelen estar enmascarados por motivos de seguridad, lo que dificulta que el analista tenga seguridad sobre la fiabilidad de la fuente (al margen de la evaluación que le adjunten sobre ella). Volviendo al caso de Curveball, esta limitación también afectó a la fiabilidad positiva que la CIA otorgó a las informaciones proporcionadas por esta fuente (llegaron a la CIA a través de la DIA y a estos de la pasaron los servicios de inteligencia alemanes).

Inteligencia de fuentes abiertas (OSINT)

Se refiere a:

- Medios de comunicación. Muchas veces los medios ofrecen información en tiempo real o análisis en profundidad sobre asuntos de interés para la inteligencia. En algunos casos también pueden ofrecer IMINT a través de fotos o tomas de televisión. Por ejemplo, la CIA utilizó durante años el Foreign Broadcast Information Service [34], FBIS, (que hizo un seguimiento de más de 3.500 medios de comunicación en 55 idiomas diferentes). Tras la reforma posterior al 11-S se creó el Open Sources Center [35], que asume las funciones del FBIS. Por su parte, las agencias de UK utilizan el BBC Monitoring Service [36]. Otro ejemplo de empresa que gestiona información de medios de comunicación es Factiva [37].

- Datos públicos. Informes de gobiernos o de organismos internacionales (FMI, OCDE, por ejemplo), bases estadísticas, debates legislativos, discursos, etc.
- Consulta directa a profesionales, académicos o miembros de think-tanks; asistencia a cursos o seminarios; o lectura de publicaciones académicas especializadas a través de suscripciones, consulta de fondos públicos o internet.

- Con respecto al apartado anterior, son reseñables los 'servicios de inteligencia privados'. Empresas que proporcionan no sólo información, sino también su propia inteligencia. Por ejemplo, Stratfor [38] y Jane's [39].

- También se incluyen en esta categoría las imágenes de satélites civiles. El propio Estados Unidos recurre a ellas, lo que le permite dedicar los satélites militares a misiones mucho más específicas o mostrar al público determinadas imágenes sin ofrecer detalles sobre la resolución de los satélites clasificados. Un ejemplo de empresa que presta este tipo de servicios es Digital Globe [40], que tiene entre sus clientes a la comunidad de inteligencia norteamericana, además de a Google Earth [41]. De hecho, esta compañía opera con satélites WorldWiev [42], que fueron desarrollados en conjunción con la National Geospatial Intelligence Agency [43], responsable de este tipo de inteligencia dentro de la comunidad.

- Igualmente forma parte de las fuentes abiertas, aunque cada vez más tiende a convertirse en un subgénero propio (SOCMINT), la información que las personas publican en sus perfiles personales de redes sociales (Facebook, Twitter, Linkedin, YouTube, etc.), las relaciones que mantienen, su geolocalización, etc (Omand, Bartlett & Miller, 2012 [44]). Este tipo de información ha sido útil, por ejemplo, para seguir el despliegue sobre el terreno de soldados rusos en Siria [45].

Drones de la CIA desplegados en una base de la fuerza aérea paquistaní descubiertos por OSINT de Google Earth

Esta imagen obtenida a través de una fuente abierta muestra a tres drones norteamericanos en la base de Shamsi, perteneciente a la fuerza aérea pakistaní. Pakistán tiene drones propios pero no contaba con aparatos como los Predator o Reaper que aparecen en la fotografía. Publicada en 2009, esta imagen prueba que algunos de los drones que protagonizan la campaña norteamericana contra Al Qaeda y los talibán en las Áreas Tribales Federalmente Administradas (oficialmente, una operación encubierta de la CIA) salían desde el propio territorio pakistaní, a pesar de las críticas vertidas por el gobierno de Islamabad contra dicha campaña.

Ventajas:

- Accesibilidad y validez para muchos de los asuntos de inteligencia
- Dada su diversidad es más difícil que sea manipulada por otros. Aunque parezca paradójico, en muchos casos es más fiable que las fuentes reservadas
- Muchas veces puede ser la primera etapa de un proceso de obtención: ¿Qué información pública existe ya sobre este asunto?

Limitaciones:

- Al igual que sucede con la SIGINT genera un enorme problema de volumen y en la mayor parte de los casos, los servicios no cuentan con un organismo especializado para la obtención y procesamiento de este tipo de información. Como consecuencia, es el mismo analista quien en principio debe hacer la búsqueda, discriminar y procesar este tipo de fuentes, y la carencia de tiempo no siempre lo permite.
- En la mayor parte de los casos debe ser complementada con información procedente de fuentes de carácter reservado, pues la opacidad de determinados temas de interés hace que queden fuera de la información abierta (por ejemplo proliferación de armas de destrucción masiva, composición real de un grupo terrorista, etc). Las fuentes abiertas sobre este tipo de cuestiones deben analizarse con extrema precaución antes de se consideren fiables.
- Por este último motivo, la OSINT despierta todavía recelos institucionales en algunas agencias de inteligencia (al menos, en las norteamericanas). Y a ello se añaden suspicacias corporativas, pues un énfasis excesivo en fuentes abiertas cuestiona la utilidad de las fuentes propias de los servicios.
- La OSINT no es tan caro como otros sistemas, pero tampoco es gratis ni económico. La suscripción corporativa anual a una revista académica especializada en Relaciones Internacionales o Estudios Estratégicos suele costar varios miles de euros. Si hablamos de decenas de revistas y del contrato de servicios de gestión de medios de comunicación la factura final puede acabar siendo elevada.

Cooperación con otros servicios de inteligencia

Supone otra fuente de información relevante sobre la base del *quid pro quo* o de un 'banco de favores'. Muchas veces los servicios extranjeros disponen de capacidades HUMINT en áreas específicas difícilmente adquiribles por los servicios propios. Otras veces pueden proporcionar informaciones obtenidas a través de IMINT o SIGINT con medios que exceden las capacidades nacionales.

- La cooperación se ve reforzada en la medida en que se comparten amenazas o intereses comunes. Este tipo de intercambios institucionales se remontan al siglo XIX (con los

movimientos revolucionarios y la aparición del terrorismo anarquista) y se vieron impulsados durante las dos Guerras Mundiales y la Guerra Fría.

- En la actualidad uno de los principales puntos de cooperación es el terrorismo internacional, pero no es el único. Ningún servicio puede ser hoy día autosuficiente. Todos necesitan este tipo de cooperación.
- El resultado son acuerdos bilaterales y multilaterales de diferente clase. En algunos casos puede haber incluso reparto explícito de tareas

No obstante, este tipo de cooperación también se encuentra con diversos problemas: protección de las fuentes, riesgo de fugas de información (que se incrementa con el número de miembros de un club de inteligencia), intereses nacionales irreconciliables en otras áreas de inteligencia, etc. El resultado es una mezcla de tendencias hacia la 'extroversión e introversión' en la interacción de unos servicios con otros

Fase de Elaboración

El primer paso en la fase de elaboración consiste en recopilar la información conseguida y procesada en la fase de Obtención y evaluarla. La recopilación no es un paso que se deba dar por descontado pues muchas veces supone discriminar de nuevo entre el trigo y la paja: algo que ya se ha hecho en la fase Obtención y en la subfase de procesamiento y explotación, pero que aun así no ha evitado que se genere un volumen gigantesco de información que acaba en la mesa de los analistas.

Al mismo tiempo, la recopilación exige consultar por un lado las bases de datos internas al servicio (el analista quedaría en evidencia si solicita a los encargados de Obtención una información ya existente). Y, por otro, las fuentes abiertas: también sería un error poner en marcha un proceso de obtención cuando la información ya está disponible en OSINT.

Existen diversos métodos para evaluar la fiabilidad. Uno genérico consiste en evaluar la credibilidad de la fuente (por ejemplo, en una escala A-E) y la consistencia interna y externa de la información recibida (en una escala de 1-5).

La puntuación puede realizarse siguiendo los criterios recogidos en la tabla:

Valoración de la Fuente:	
A	Fuente bien conocida y que lleva tiempo proporcionando información válida
B	Fuente bien conocida y con larga trayectoria pero que a veces ha proporcionado información que con el tiempo se ha demostrado errónea
C	La fuente parece fiable pero lleva poco tiempo informando
D	Fuente dudosa que lleva tiempo proporcionando informaciones de escasa fiabilidad y a la que pueden afectar intereses o sesgos ideológicos que –consciente o inconscientemente– le lleven alterar la percepción de la realidad
E	Fuente desconocida, sobre la que no existe experiencia previa

Valoración de la información:	
1	Información creíble, que coincide tendencias o hechos previos bien constatados
2	Información que se corresponde de manera general con tendencias constatadas o con hechos previos. Sin embargo, existen ciertas discordancias que conviene investigar
3	Información que contradice tendencias y hechos previos bien conocidos sin una explicación clara. La información puede ser incorrecta o puede ser necesario investigar para descubrir la causa de esa discordancia
4	Información inconsistente que choca con tendencias y hechos conocidos. Es altamente dudosa o simplemente incorrecta
5	Información que puede ser creíble, pero no hay modo de compararla con informaciones previas

Fuente: elaboración propia basada en (Quiggin, 2007: 171-172 [46])

A partir de estos criterios, la mejor sería una información valorada como A1, la peor como D4 y la E5 sería información quizás válida pero por el momento poco sólida.

Otros criterios para valorar la fuente serían el conocimiento del tema sobre el que informa (un técnico en radares puede ser competente al dar los detalles de la firma radar de un avión, pero poco fiable al informar sobre las especificidades aerodinámicas del avión); su acceso a la información (directo o indirecto); y la existencia de intereses particulares o de una carga ideológica fuerte que le lleve a distorsionar la realidad (Clark, 2013 [3]).

El siguiente paso es propiamente el análisis. Requiere un esfuerzo de examen sistemático de la información, de síntesis, integración, contextualización, identificación de variables clave, establecimiento de relaciones causales y, por tanto, de interpretación de la información con una orientación al futuro que convierta el conocimiento adquirido en una herramienta para la toma de decisiones.

En un documento anterior [47] hemos tratado de manera también introductoria las características del análisis de inteligencia, examinando las fuentes de error y algunas técnicas que contribuyen a mejorar su calidad. Del mismo modo, recomendamos el libro de Richards J. Heuer y Randolph H. Pherson (2011), *Structured Analytic Techniques for Intelligence Analysis* [48], (traducido al español [49] por la editorial Plaza y Valdés) donde se explican decenas de técnicas para mejorar el análisis de inteligencia: mapas mentales y conceptuales, mapas de proceso, matrices, análisis de redes, brainstorming estructurados presenciales y virtuales, matrices de impactos cruzados, análisis morfológico, análisis de escenarios, técnicas de generación y competición de hipótesis, mapas argumentales, role playing, análisis de equipos diferentes, análisis DAFO, matrices de decisiones, etc. En este análisis sobre el Daesh en Libia [50] puede encontrarse un ejemplo de su aplicación.

Además de esas recomendaciones bibliográficas, añadimos unos comentarios breves sobre tres aspectos relacionados con el análisis.

En primer lugar, la tendencia creciente a **favorecer la integración de la información** haciendo que la información circule entre los diversos departamentos del servicio y entre los distintos componentes de la comunidad de inteligencia (en Estados Unidos, por ejemplo, a través de los Fusion Centers [51]) con el fin de que llegue donde se necesita. Los atentados del 11-S, cuya prevención se habría beneficiado de una mayor colaboración e intercambio de información intra e inter-agencias, impulsaron un movimiento de reforma en ese sentido. Sin embargo, los escándalos ligados a las filtraciones del soldado Manning [52] y del caso Snowden han supuesto un retroceso. A pesar de ello, la tendencia a fomentar el trabajo en red y suavizar las restricciones internas para acceder a información sigue vigente y tiene grandes defensores, como es el caso –ya desde fuera de la comunidad de inteligencia– del General McChrystal [53], que como ya hemos comentado lideró la gran innovación del Joint Special Operations Command: un proceso de cambio que tuvo mucho que ver con la gestión e integración de información para producir inteligencia militar operativa.

En segundo lugar, las **competencias básicas que debe tener cualquier buen analista** (Lowenthal, 2012 [6]):

- *Capacidad intelectual* para retener informaciones previas y para plantear preguntas y respuestas interesantes. A ello se une la *actitud ante el conocimiento y el aprendizaje*. Deben ser personas con una gran curiosidad y deseo de aprender, capaces de trabajar duro y ser tenaces a la hora de desarrollar una investigación detallada. También imaginativas y con capacidad para reconocer lo importante. No es necesario que sean superdotadas, aunque al igual que sucede con otras profesiones hay individuos que de manera innata resultan especialmente aptos en este sentido: sintetizan y analizan de manera rápida e intuitiva, y saben leer entre líneas, haciéndose una idea acertada de lo que se esconde detrás de determinados hechos o informaciones. Los analistas de inteligencia no proceden de una titulación universitaria específica. Los hay de las carreras más variadas (Ciencia Política, Derecho, Economía,

Historia, Ciencias de la Comunicación, Ingenierías, Ciencias Exactas, etc.), además de aquellos que provienen de Fuerzas Armadas o Fuerzas y Cuerpos de Seguridad del Estado.
- Un *notable conocimiento del campo de especialización* sobre el que realiza su trabajo (un país o área geográfica, un determinado grupo terrorista o de crimen organizado, etc). Resulta fundamental para integrar y poner en contexto las nuevas informaciones recibidas.
- Habilidades para la *exposición oral*, de modo que sea clara y sintética, demostrando seguridad y ganándose la empatía de quienes le escuchan.
- Correcta *exposición escrita*, de manera también clara y concisa.

Y, en tercer lugar, varios **principios básicos sobre la gestión de los analistas** que atañen a los directivos, a quienes supervisan la organización, trabajo y trayectoria profesional de los analistas (Gentry, 2014 [54]):

- Un dilema que suele presentarse es la *rotación de los analistas*. Trabajar sobre un mismo tema durante muchos años favorece la especialización y rentabiliza la inversión realizada en esa persona. Pero un exceso de permanencia puede dar lugar al anquilosamiento analítico (que hace vulnerable a las sorpresas estratégicas) o a que el analista acabe cansado del tema. De manera general, la solución sería un equilibrio en las rotaciones, cuya duración dependa de la intensidad del trabajo, de las características y de las preferencias personales del analista y de las demandas de producción sobre determinados temas.
- Equilibrio entre *inteligencia actual y otros tipos de inteligencia*. Una cuestión que ya comentamos en un documento anterior al hablar de la inteligencia estratégica.
- *Evitar la politización*. Tema que también tratamos en el documento anterior y en el que los directivos desempeñan un papel esencial pues muchas veces son la correa de transmisión entre los analistas y los decisores políticos que reciben la inteligencia.
- *No cerrar el servicio sobre sí mismo*. Fomentar el intercambio de opiniones con analistas de otras agencias de la comunidad de inteligencia y con expertos de la comunidad de inteligencia extendida. La apertura y el contacto con otros expertos contribuye a que se revisen los marcos de análisis, a conocer nuevas fuentes OSINT y reducir el peligro de 'group-thinking'. La comunidad de inteligencia norteamericana utiliza herramientas informáticas para favorecer el análisis colaborativo como A-Space, una red social protegida y pensada para que participen en ella analistas de diversas agencias. No obstante, para que ese tipo de herramientas sean útiles debe haber también contactos cara a cara y una actitud positiva por parte de los directivos de cada uno de los servicios.

Fase de Difusión

Es una fase tan importante y compleja como las tres anteriores. En ella convergen dos de los tres afanes que Sherman Kent atribuye a todo analista de inteligencia: el afán de saber, el de *ser creído* y el de *influir para bien*.

Según Miguel Ángel Esteban y Andrea V. Carvalho (2012: 155 [12]), hay seis condiciones que deben cumplirse para que esta fase sea eficaz:

- Que el mensaje llegue a tiempo, ya que la inteligencia está orientada a la toma de decisiones
- Que sea pertinente y adecuado a la necesidad de información que intenta satisfacer.
- Que su contenido sea claro y fácilmente comprensible.
- Que posea un formato adecuado para el receptor y adecuado para el canal de comunicación empleado.

- Que se efectúe por canales seguros y que mantenga un carácter reservado o, cuando menos, confidencial.

Para asegurar en la medida de lo posible todas estas condiciones, la fase de Difusión es la más estandarizada de todas, al menos en la Comunidad de Inteligencia norteamericana que es la que ofrece mayor cantidad de información pública al respecto. La inteligencia llega a los destinatarios en una gama variada de formatos: informes breves con inteligencia actual, como el ya mencionado PDB (algunos históricos ya han sido desclasificados [55]), monografías con inteligencia estratégica, estudios estimativos como el National Intelligence Estimate, inclusión de nueva inteligencia básica en bases de datos ya existentes, *briefings*, etc.

Cada institución establece sus propios requisitos formales a la hora de redactar, presentar o difundir los productos de inteligencia, pero hay una serie de guías maestras que pueden ayudar:

- *Brevedad*. Uno de los bienes más preciados por los decisores políticos es el tiempo. Su agenda se encuentra sobrecargada y sus prioridades personales o profesionales no coinciden con muchos de los temas abordados por un servicio de inteligencia estratégico. Salvando las distancias, lo mismo puede aplicarse en niveles intermedios del gobierno y de la administración, por lo que una de las características fundamentales del análisis de inteligencia es su concisión. Lo cual también resulta válido para los documentos monográficos que por su temática requieran una extensión más amplia. En esos casos se ha expresar en decenas de páginas lo que en otro contexto se podría exponer en centenares.
- *Relevancia.* Un buen análisis incluye sólo aquellas cuestiones que puedan ser de interés para el consumidor de inteligencia. Hay que preguntarse por tanto qué es lo que querríamos saber sobre un determinado asunto si estuviésemos en su lugar. Según Frank Watanabe (1996: 46) [56], no se trata de que el analista demuestre lo mucho que sabe, sino de que transmita los hechos y las explicaciones verdaderamente relevantes. Los detalles superfluos pueden oscurecer los aspectos que merecen ser destacados.
- *Claridad expositiva.* Se consigue redactando el análisis en base a preguntas bien definidas que hagan comprensible una situación o realidad compleja. También contribuye a este objetivo el empleo de construcciones gramaticales sencillas, así como la inclusión de gráficos, fotografías y mapas fáciles de entender.
- *Precisión.* Aunque la incertidumbre sea una constante de las relaciones internacionales y en la conducta de otros actores, los análisis de inteligencia deben evitar el lenguaje ambiguo. Es aconsejable que las palabras ‘quizás’, ‘probablemente’, ‘podría’, etc, así como otras también genéricas como ‘beneficia’, ‘limita’ o ‘sugiere’ vayan acompañadas de explicaciones (por ejemplo, utilizando ‘porque’) que aporten un significado más definido. A veces las inconsistencias internas de un texto se encuentran relacionadas con un lenguaje impreciso (Petersen, 2011: 17 [57]). Al mismo tiempo, Lowenthal (2012) [6] previene de un exceso de seguridad en el lenguaje (empleo de porcentajes a la hora de hablar probabilidades). Se corre el riesgo de transmitir una precisión de la que se carece. Por ello en los NIEs se habla de confianza alta, media o baja en el análisis, fundamentada en la fiabilidad de la información y la solidez de los juicios que se pueden realizar a partir de ella. Lowenthal recomienda otro tipo de expresiones –diferentes a los números– al estimar probabilidad futuras o de exactitud del análisis: remota, improbable, con alguna probabilidad, probable, altamente probable, y prácticamente seguro. Parte de la precisión consiste también en hacer explícito lo que se sabe y lo que se desconoce. Ambos pueden ser igual de relevantes para el destinatario de la inteligencia y pueden orientar futuras demandas de Obtención. Según Lowenthal, Colin Powell,

en su etapa de Secretario de Estado, pedía lo siguiente: “dime lo que sabes, lo que no sabes y lo que piensas”.

Una vez que se dispone de la inteligencia en el formato debido, el siguiente gran reto consiste en que llegue a los consumidores que la necesitan para que puedan hacer el mejor uso de ella. Existen diversos sistemas de difusión en cada comunidad. Además de las listas de distribución asociadas a determinados productos de inteligencia actual –como el CIA World Intelligence Review (WIRe) [58] que, además de a decisores políticos, llega a un amplio abanico de funcionarios civiles y militares–, se encuentran las bases de datos de acceso múltiple como el proyecto de la Library of National Intelligence impulsado por la Oficina del Director de Inteligencia Nacional norteamericano.

Es conveniente atraer la atención sobre la inteligencia. En cierto modo, *saber venderla*. Según Robert M. Clark (2013) [3], la inteligencia debería ser como el alimento –algo demandado y fácil de colocar a los consumidores. Sin embargo, la inteligencia es similar a los seguros, se ha de llamar la atención del cliente sobre su importancia.

Y el último reto consiste en que una vez que la inteligencia llega a los destinatarios y logra atraer su atención, éstos sepan apreciarla y, si es el caso, la tengan en cuenta en sus decisiones. En buena medida esto escapa al control de los funcionarios de inteligencia. Al mismo tiempo un exceso en el deseo de ser escuchados aumenta el peligro de politizar la inteligencia, de generar *intelligence to please*; es decir, de adaptar el producto a las preferencias políticas del decisor con el fin de que sea aceptado.

En efecto, la inteligencia tiene mayores probabilidades de ser rechazada por el destinatario cuanto más contradiga la opinión de éste sobre una determinada cuestión. Más aún si no se trata sólo de una valoración previa sino de una política en marcha (hace cinco siglos Maquiavelo ya advertía que *“los hombres no contemplarán las cosas como realmente son, sino como les gustaría que fueran”*). Uno de los ejemplos históricos más señalados fue la negativa de Stalin a aceptar los informes que alertaban de un ataque alemán inminente a comienzos del verano de 1941 [59]. Décadas más tarde la Administración Johnson no aceptó las valoraciones de la CIA que entre 1963 y 1965 advirtieron repetidamente que un incremento de las fuerzas militares en Vietnam no resolvería un conflicto que requería una salida política, no militar. En 1983 la Administración Reagan tampoco escuchó a la Agencia cuando ésta afirmó que no habría un modo razonable de forzar la retirada del ejército sirio de El Líbano. El resultado de esa desconexión entre inteligencia y política exterior fue el despliegue militar norteamericano en el país y su abrupto abandono tras sufrir un atentado en el que murieron 241 Marines (Clark, 2013 [3]).

Finalmente, y de manera ideal, los destinatarios deberían ofrecer *feedback* a los servicios sobre la utilidad de la inteligencia recibida, matices a tener en cuenta, nuevos requerimientos, cuestiones a ampliar, etc. Sin embargo, los mismos problemas que reducen el protagonismo del consumidor de inteligencia al inicio del ciclo (como ya hemos señalado, falta real de tiempo, tiranía de la agenda y de la urgencia de los asuntos, y en ocasiones falta de pensamiento estratégico, escaso interés, etc) pueden afectar negativamente al proceso de retroalimentación.

Javier Jordán es Profesor Titular de Ciencia Política y miembro del Grupo de Estudios en Seguridad Internacional (GESI) de la Universidad de Granada.

Bibliografía

Clark, Robert (2012), *Intelligence Analysis: A Target-Centric Approach*, Washington, DC: CQ Press.

Esteban, Miguel Ángel (Coord.) (2009), *Glosario de Inteligencia*, Madrid: Ministerio de Defensa.

Esteban, Miguel Ángel y Carvalho, Andrea V. (2012), “Etapas y actividades del proceso de producción y transferencia”, González Cussac, José Luis (Coord.), *Inteligencia*, Valencia: Tirant lo Blanch, pp. 130-160.

Esteban, Miguel Ángel y Carvalho, Andrea V. (2012), “La inteligencia y los activos informacionales, González Cussac, José Luis (Coord.), *Inteligencia*, Valencia: Tirant lo Blanch, pp. 19-26.

Hulnick, Arthur S. (2006), “What's wrong with the Intelligence Cycle”, *Intelligence and National Security*, Volume 21, Issue 6, pp. 959-979.

Lowenthal, Mark M. (2012), *Intelligence: From Secrets to Policy*, Washington, DC: CQ Press.

McChrystal, Collins, Stanley, Silverman, David, Fussell, Chris (2015), *Team of Teams: New Rules of Engagement for a Complex World*, New York: Penguin Group.

McDowell, Don (2009), *Strategic Intelligence. A Handbook for Practitioners, Managers, and Users*, Lanham: Scarecrow Press.

Treverton, Gregory F. & Gabbard, C. Bryan (2008), *Assessing the Tradecraft of Intelligence Analysis*, Santa Monica: RAND Corporation.

Treverton, Gregory F. & Ghez, Jeremy J. (2012), *Making Strategic Analysis Matter*, Santa Monica: RAND Corporation.

Varios Autores (2013), *Diccionario LID Inteligencia y seguridad*, Madrid: LID.

Warner, Michael (2002) “Wanted: A Definition of "Intelligence"”, *Studies in Intelligence*, Vol. 46, No 3.

[60]

Editado por: Grupo de Estudios en Seguridad Internacional (GESI). Lugar de edición: Granada (España). ISSN: 2340-8421.

[61]

Inteligencia [62]
Documentos didácticos [63]

URL de origen: http://www.seguridadinternacional.es/?q=es/content/una-revisi%C3%B3n-del-ciclo-de-inteligencia

Enlaces:
[1] http://www.seguridadinternacional.es/?q=es/content/introducci%C3%B3n-la-inteligencia-en-el-%C3%A1mbito-de-seguridad-y-defensa
[2] http://www.dtic.mil/doctrine/new_pubs/jp2_0.pdf
[3] http://www.amazon.es/Intelligence-Analysis-A-Target-Centric-Approach/dp/1452206120
[4] http://www.tandfonline.com/doi/full/10.1080/02684520601046291
[5] http://www.rand.org/content/dam/rand/pubs/technical_reports/2008/RAND_TR293.pdf
[6] http://www.amazon.com/Intelligence-From-Secrets-Policy-Edition/dp/1608716759
[7] http://www.ugr.es/~jjordan/JSOC-Defensa.pdf
[8] http://www.isn.ethz.ch/Digital-Library/Articles/Detail/?lng=en&id=186901
[9] http://www.fas.org/irp/dni/icd/icd-204.pdf
[10] http://www.theguardian.com/us-news/2015/jul/08/nsa-tapped-german-chancellery-decades-wikileaks-claims-merkel
[11] http://www.wsj.com/articles/u-s-spy-net-on-israel-snares-congress-1451425210
[12] http://www.tirant.com/editorial/libro/inteligencia-miguel-angel-esteban-navarro-9788490045626
[13] http://www.bga-aeroweb.com/Defense/RQ-4-Global-Hawk.html
[14] http://www.thedailybeast.com/articles/2015/01/04/exclusive-u-s-drone-fleet-at-breaking-point-air-force-says.html
[15] http://www2.warwick.ac.uk/fac/soc/pais/people/aldrich/vigilant/tavares_fortitude.pdf
[16] http://digitalcommons.unf.edu/cgi/viewcontent.cgi?article=1077&context=ojii_volumes
[17] http://www.seguridadinternacional.es/blog.mosaico/?q=es/content/drones-militares-impulso-la-innovaci%C3%B3n-tecnol%C3%B3gica-y-civil
[18] https://support.google.com/earth/answer/148092?hl=es
[19] https://www.youtube.com/watch?v=ErlDSJHRVMA
[20] http://www.biometricupdate.com/201505/public-drones-equipped-with-facial-recognition-software-raise-privacy-concerns
[21] http://www.theatlantic.com/technology/archive/2015/09/opm-hack-fingerprints/406900/
[22] https://www.nsa.gov/careers/cyber/
[23] http://journal.georgetown.edu/u-s-military-defense-systems-the-anatomy-of-cyber-espionage-by-chinese-hackers/
[24] http://www.defenseone.com/threats/2015/09/more-questions-f-35-after-new-specs-chinas-copycat/121859/
[25] https://www.ctc.usma.edu/posts/the-abbottabad-documents-bin-ladins-security-measures
[26] http://www.airpower.maxwell.af.mil/airchronicles/aureview/1984/jul-aug/murray.html
[27] http://www.infodefensa.com/es/2009/09/08/noticia-indra-se-adjudica-el-mantenimiento-del-sistema-de-guerra-electronica-scapa-por-48-

millones-de-euros.html
[28] https://www.fbi.gov/about-us/history/famous-cases/aldrich-hazen-ames
[29] https://www.fbi.gov/about-us/history/famous-cases/robert-hanssen
[30] http://topics.nytimes.com/top/reference/timestopics/people/p/jonathan_j_pollard/index.html
[31] https://www.cia.gov/news-information/featured-story-archive/2010-featured-story-archive/colonel-penkovsky.html
[32] http://www.seguridadinternacional.es/blog.mosaico/?q=es/content/humam-al-balawi-el-agente-triple
[33] http://www.spiegel.de/international/world/the-real-story-of-curveball-how-german-intelligence-helped-justify-the-us-invasion-of-iraq-a-542840.html
[34] https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/foreign-broadcast-information-service/
[35] https://www.opensource.gov/
[36] http://www.monitor.bbc.co.uk/
[37] http://www.factiva.com/
[38] http://www.stratfor.com/
[39] http://www.janes.com/
[40] https://www.digitalglobe.com/
[41] https://www.google.es/intl/es/earth/index.html
[42] http://www.satimagingcorp.com/satellite-sensors/worldview-3/
[43] https://www.nga.mil/Pages/Default.aspx
[44] http://www.tandfonline.com/doi/abs/10.1080/02684527.2012.716965#.Vfho-NKvGUk
[45] http://www.elconfidencial.com/mundo/2015-11-12/selfies-de-rusos-con-metralleta-para-mostrar-que-putin-juega-sucio-en-siria_1091096/
[46] http://www.amazon.com/Seeing-Invisible-National-Intelligence-Uncertain/dp/9812704825
[47] http://www.seguridadinternacional.es/?q=es/content/introducci%C3%B3n-al-an%C3%A1lisis-de-inteligencia
[48] http://www.amazon.es/Structured-Analytic-Techniques-Intelligence-Analysis/dp/1608710181/ref=pd_sim_14_1?ie=UTF8&refRID=0H6EDP442H9JPRGX8EFG&dpID=51JYuPBW2WL&dpSrc=sims&preST=_AC_UL160_SR100%2C160_
[49] http://www.plazayvaldes.es/libro/tecnicas-analiticas-estructuradas-para-el-analisis-de-inteligencia/1493/
[50] http://www.seguridadinternacional.es/?q=es/content/an%C3%A1lisis-estrat%C3%A9gico-del-daesh-en-libia
[51] http://www.cfr.org/intelligence/fusion-centers/p12689
[52] http://www.theguardian.com/world/2013/aug/21/bradley-manning-35-years-prison-wikileaks-sentence
[53] http://www.amazon.com/Team-Teams-Rules-Engagement-Complex/dp/1591847486
[54] http://www.tandfonline.com/doi/abs/10.1080/02684527.2014.961244
[55] https://www.cia.gov/library/publications/intelligence-history/presidents-daily-brief/index.html
[56] https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/97unclass/axioms.html
[57] https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol.-55-no.-1/what-i-learned-in-40-years-of-doing-intelligence-analysis-for-us-foreign-policymakers.html
[58] https://www.cia.gov/offices-of-cia/intelligence-analysis/products.html
[59] https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol50no1/9_BK_What_Stalin_Knew.htm
[60] http://www.ugr.es/~gesi/analisis/2-2016.pdf
[61] http://creativecommons.org/licenses/by-nc-nd/3.0/deed.es_CO
[62] http://www.seguridadinternacional.es/?q=es/tags/inteligencia
[63] http://www.seguridadinternacional.es/?q=es/tags/documentos-did%C3%A1cticos