Investigación, análisis e inteligencia antiterrorista

Estudios en investigación y análisis

Documento Nº: WP_02.08.2011

Difusión controlada.

Cualquier comentario relacionado con el material contenido en este documento puede ser enviados a: pubs@jmjdesigner.com

Índice

Introducción

La escalada terrorista internacional desarrollada a partir de la irrupción de Al-Qaeda y más concretamente desde la consecución exitosa de los atentados a gran escala en Nueva York, Madrid, Londres y recientemente Oslo, enfocan la atención de gobiernos y ciudadanos en los aparentes fallos de inteligencia atribuidos a las organizaciones responsables de su elaboración. Así pues los gobiernos occidentales desde hace tiempo están promoviendo cambios en la estructura y función de los servicios de inteligencia, mientras brilla por su ausencia la reflexión y los proyectos de cambio en los procedimientos y métodos usados en dichos servicios. Esto se debe sin duda al profundo desconocimiento de los políticos acerca del cuerpo doctrinal y metodológico de la disciplina de inteligencia y su función de utilidad real, y al mismo tiempo a la falta de innovación y dinamismo en la adecuación de los procedimientos y métodos a las nuevas realidades que presionan en forma de nuevas amenazas y demandas de inteligencia.

Centrándonos en el problema de la amenaza terrorista (a la que suelo describir como "transversal, combinatoria y contagiosa" en referencia a su complejo carácter), parece ser la caja de Pandora de donde salen a relucir todos los problemas, carencias y confusiones sobre las estrategias y los métodos a emplear en el ámbito de la inteligencia. En este punto cabe preguntarse si realmente estamos ante nuevos problemas que requieren nuevos métodos, o ante los mismos problemas de siempre que ocultos a la visión pública yacían bajo la "calma chicha" del mundo bipolar de la guerra fría, cubierto por el

manto de la disuasión nuclear y del papel terciario que los servicios de inteligencia de los países aliados de las dos superpotencias ejercían en esa época reciente. Como bien establece uno de los maestros, en este caso maestra de la llamada "Warning Intelligence" Cynthia Grabo, los problemas analíticos y los fallos de inteligencia actuales difieren muy poco de los viejos problemas de siempre, como ejemplo citemos algunos como la inadecuada percepción de amenazas emergentes, particularmente las de menor probabilidad y mayor peligro potencial, la consiguiente falta de una estrategia adecuada de obtención de información, la estructural falta de comunicación y enfoque cooperativo entre responsables de obtención de información, analistas y directivos y por último la ausencia total de referencias a modelos metodológicos que permitan sistematizar los procesos de producción de inteligencia e implementar métricas de desempeño en las distintas labores. A todo esto se suman nuevos vicios adquiridos, como el enfoque mecanicista del uso de las tecnologías de la información en los procesos de inteligencia y la permanente exigencia de más información y de más fuentes proveedoras de la misma, en este sentido es preocupante ver el enfoque que se está planteando respecto a la OSINT (fuentes abiertas) proveniente de Internet, dotándola de una importancia exagerada con respeto a su verdadero valor como fuente proveedora de evidencias o de alerta temprana.

Trabajos importantes como los de National Intelligence Council, Joint Military Intelligence College y en particular los del Kerr Group de la CIA establecen entre otras muchas consideraciones un aserto coincidente en todos, el cual establece que es en el análisis más que en la obtención donde se plantea la vía óptima para mejorar los procesos y los productos de inteligencia, pero al mismo tiempo es donde se registran las mayores carencias de planteamientos sólidos y mayor resistencia al cambio. En este punto puedo asegurar como humilde estudioso y contribuidor de la materia que existen modelos, métodos y procedimientos de validez contrastada y se está trabajando con bastante tino en el ajuste y creación de nuevos planteamientos por parte de la comunidad intelectual y profesional de la disciplina de inteligencia. Es importante reivindicar al analista de inteligencia como

pieza clave del sistema de producción, pero al mismo tiempo es necesario someter a una revisión amplia sus conocimientos doctrinales, su formación de base, su formación profesional continua, su papel y estatus en las organizaciones de inteligencia y sobre todo sus procedimientos de actuación.

Finalizando esta introducción que ha tenido por objetivo centrar al lector en la situación actual, a continuación voy a realizar una descripción básica de las líneas maestras que en procedimientos y métodos se está trabajando en inteligencia antiterrorista.

Estrategia, métodos y herramientas en la producción de inteligencia antiterrorista

Con un objetivo pedagógico para el lector no introducido empezaremos haciendo una distinción entre dos términos que reconocen casi todos los servicios de inteligencia aunque le den distintos significados, estos términos son contraterrorismo y antiterrorismo. Para el propósito que nos ocupa sin entrar en más consideraciones llamaremos inteligencia contraterrorista a la de soporte a operaciones activas que se toman contra operativos terroristas y sus actividades, por el contrario llamaremos inteligencia antiterrorista a las medidas defensivas encaminadas a prevenir y hacer más difícil la realización exitosa de un acto terrorista.

A partir de los trabajos que se están realizando en la comunidad profesional de inteligencia, podemos clasificar la inteligencia antiterrorista en función del tipo de producto a entregar y los elementos informativos a obtener y valorar. Así, en lo referente a productos la clasificaremos en actual, investigativa, operacional, estimativa y de alerta, y en cuanto al contenido, en dos tipos: Inteligencia sobre el dominio del mundo real ocupado por las organizaciones terroristas e inteligencia sobre las actividades de las redes, grupos y organizaciones, orientadas a producir una crisis o ataque exitoso.

En lo relativo a la inteligencia sobre el dominio se hace imperativo tener una unidad bien organizada, encaminada a deducir los atributos y la

estructura de las organizaciones terroristas y su entorno, para ello es necesario crear y mantener un sistema analítico de información histórica (figura1) que, a partir de un modelo de referencia sometido a constante revisión, permita enfocar las tareas de obtención y análisis.

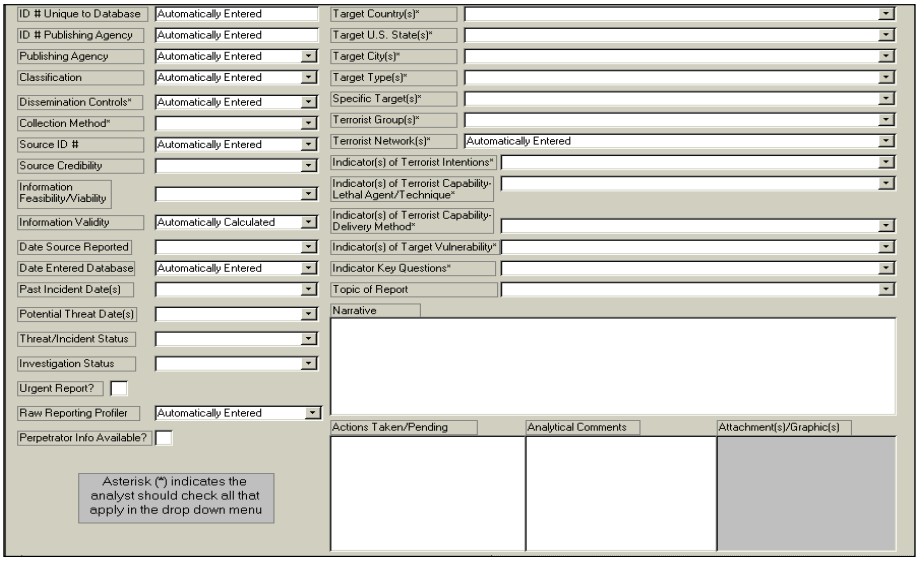

Figura 1. Base de información de inteligencia antiterrorista

Un ejemplo en este sentido sería el modelo de Wolf sobre terrorismo internacional adaptado a la situación actual. Dicho modelo introduce un sistema que permite establecer categorías a partir de las cuales crear, en un enfoque de revisión continua, el conjunto de atributos a monitorizar y analizar. Como ejemplo de dichas categorías tendríamos las siguientes:

Categoría de código 01: Información relativa a un acto simbólico internacional, nacional o interno ejecutado en un determinado lugar y en una fecha y hora concretas.

Categoría de código 02: Información que proporciona una base de asociación entre un acto terrorista y una fase de un proceso revolucionario: planificación, acción, consolidación.

Categoría de código 03: Información relativa a la organización perpetradora y sus miembros, sus asociaciones con delincuentes extranjeros o nacionales y, en especial, su aparato clandestino, que está construido para ayudar a los miembros a preparar y ejecutar

operaciones de acción directa y propagadora y para ampararlos cuando se cumplan las misiones.

Categoría de código 04: Información relativa a la ideología de individuos fervorosos y resueltos que están ineluctablemente comprometidos en una causa que creen justa.

Categoría de código 05: Información relativa a las técnicas utilizadas por un grupo terrorista para influir y combatir con efectividad, disponiendo de pocos recursos.

Categoría de código 06: Información relativa a tácticas fuera de las normales usadas por los terroristas (secuestros, colocación de bombas, asesinatos, etc.) y sus armas.

Categoría de código 07: Información relativa a objetivos atacados por los terroristas; específicamente todos los aspectos de la vulnerabilidad de estos objetivos, impacto adverso que tendrá sobre un grupo concreto la destrucción o inhabilitación del objetivo, o impacto positivo que tendrá la destrucción de un objetivo determinado sobre la imagen del grupo responsable de su asalto.

Categoría de código 08: Información pertinente al propósito propagandístico de un grupo terrorista.

Etc.

A partir de la información anteriormente descrita, podemos aplicar distintos modelos de análisis en correspondencia con los productos de inteligencia a obtener, un ejemplo podría ser la obtención de perfiles electrónicos extendidos de entidades relacionadas con el terrorismo, también llamados mapas de relaciones; este producto de inteligencia permite visualizar con ayuda del ordenador y de software específicos el conjunto de atributos que acompañan a una entidad determinada (terrorista, organización, etc.), los valores e informaciones de dichos atributos o la ausencia de ellos, así como la relación de la entidad con otras entidades del mundo real (figura 2).

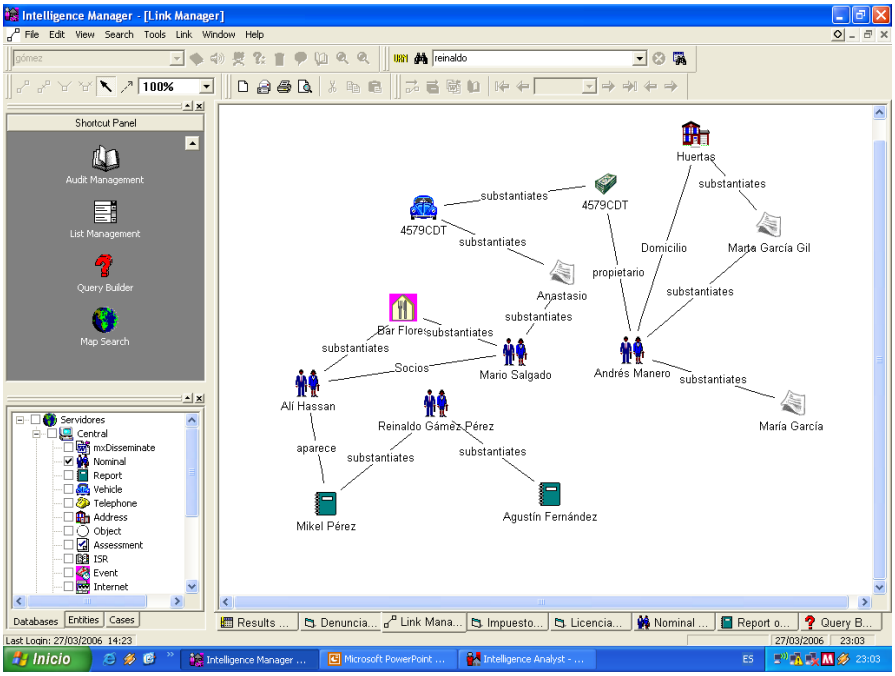

Figura 2. Mapa de relaciones de una entidad

Por otro lado, desde el punto de vista de las acciones terroristas es necesario adaptar modelos operacionales tales como el "Intelligence Led" a nuevas formas de actuación. De forma básica, en el desarrollo de una acción terrorista se pueden distinguir varias fases: planificación, preparación, crisis y consecuencias (figura 3).

PLANIFICACIÓN	PREPARACIÓN	CRISIS	CONSECUENCIAS
•Determinación del objetivo político •Selección del objetivo de la acción terrorista • Elección del "modus operandi" •Posible fijación de fechas de ejecución	• Reclutamiento de la red •Entrenamiento •Recaudación de fondos • R&D •Adquisición de materiales, herramientas e instrumentos •Recopilación de datos •Reconocimiento •Elaboración del plan de actuación	•Desplazamiento de la red y los materiales •Reunión •Montaje del operativo • Reconocimiento final •Ejecución •Extracción	• Exfiltración •Regeneración de los recursos •Determinación de las consecuencias •Análisis de la operación •Propaganda suplementaria al acto •Planificación de una nueva acción

Figura-3 Fases del desarrollo de una acción terrorista

En torno a estas fases es necesario obtener una cascada continua de información que permita realizar tareas que aborten el desarrollo de la acción y obtener información añadida, sobre todo teniendo en cuenta que las acciones terroristas en la actualidad estas caracterizadas por una

larga fase de planificación y preparación, una fase de crisis muy breve y un periodo de consecuencias bastante largo. Por tanto, es necesario aplicar modelos de inteligencia operacional ayudados por tecnologías de información con objeto de monitorizar, influir, regular y abortar el desarrollo de la acción terrorista. En el caso del modelo "Intelligence Led" la forma de operación desde un punto de vista de procesos puede describirse partiendo de ciclo iniciado por una **actividad** que tenga lugar, resultando en un **registro de información** relativa a dicha actividad, el **análisis** de dicha información registrada en combinación con otra información y la asignación de alguna **tarea** basada en la información hallada, que resultará en una nueva **actividad**.

El modelo de proceso Actividad – Registro – Análisis – Tarea – Actividad se ilustra de la siguiente manera en la figura 4.

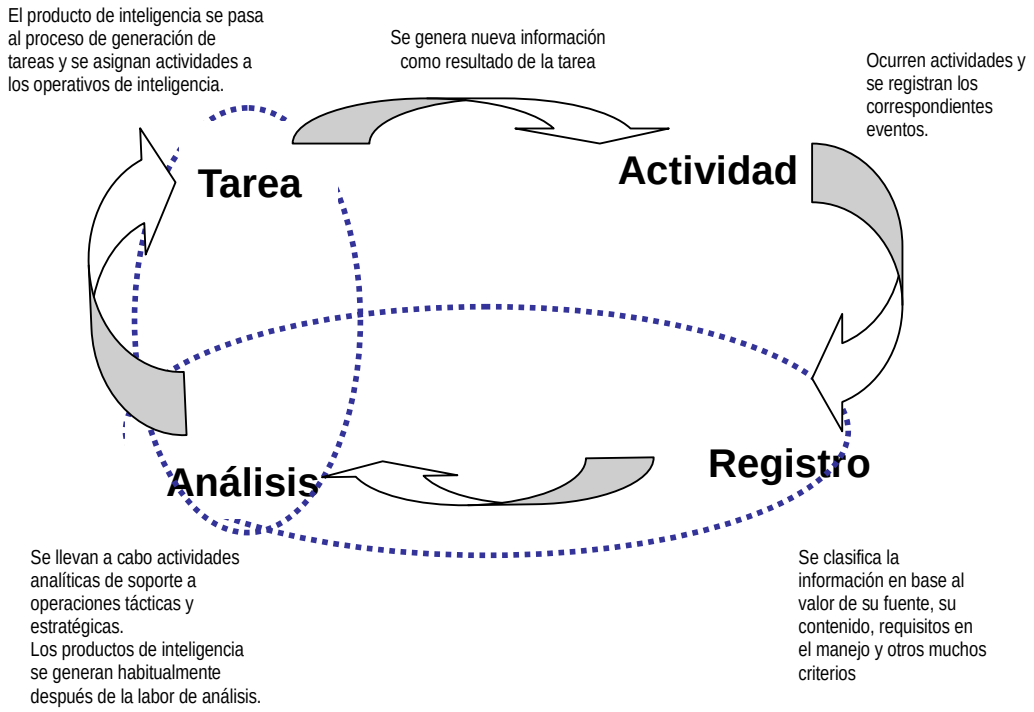

Figura 4. Ciclo de operaciones en el modelo "Intelligence-Led"

En base a nuestra experiencia en el área de inteligencia reconocemos los siguientes factores como preceptos fundamentales en una investigación basada en el modelo "Intelligence-Led":

- No puede predecirse lo que se investigará mañana.

- Toda información es potencialmente útil.
- Una vez recopilada, la información ha de estar disponible en tiempo real.
- La prioridad de las fuerzas de seguridad es prevenir y evitar los crímenes antes que reaccionar a ellos.

Al considerar el soporte y la automatización del proceso, existen una serie de factores críticos relativos a los sistemas de inteligencia a tener en cuenta:

- El principio de Pareto aplicado a la inteligencia define que el 80% de las necesidades de inteligencia será obtenida a partir del 20% de las fuentes de información potencialmente necesarias. Por ello se hace necesario introducir procedimientos de interpolación de fuentes primarias y secundarias, así como métodos de triangulación de contenidos a varios niveles que permitan reforzar su credibilidad y someter a la fuente de origen a un proceso de ponderación continua.
- Las actividades a monitorizar forman inevitablemente parte de largas cadenas de relaciones. A través del análisis de la información, las fuerzas de seguridad pueden identificar objetivos prominentes, asignar recursos en base a los mismos y potenciar la desestabilización de la actividad terrorista atacando los citados objetivos o las relaciones entre ellos.
- Los patrones en las actividades monitorizadas tenderán a repetirse dado que las acciones exitosas tenderán a reproducirse, por tanto es importante detectarlos y estudiarlos.
- Los investigadores y analistas deben aprovechar siempre que sea posible las lecciones aprendidas en casos previos mejorando sus procesos internos de trabajo y refinando los modelos de referencia de los mismos.

La información necesaria para la generación de productos de inteligencia sobre actividad terrorista puede provenir de fuentes tan diversas como:

- Informes de incidentes producidos en cualquier parte del mundo.

- Conversaciones con ciudadanos en la calle o durante controles específicos.
- Fuentes o informantes confidenciales.
- Investigaciones y vigilancia.
- Registros de facturas telefónicas, transacciones bancarias, etc.
- Pistas o consejos anónimos vía telefónica o e-mail.
- Páginas de Internet.
- Organizaciones religiosas, políticas radicales, etc.
- Boletines o difusiones de otras agencias de fuerzas de seguridad.
- Sistemas de gestión de registros.
- Cualquier otra fuente.

Estas fuentes conforman los cimientos para una base de información de actividades terroristas. Gracias a esta información, pueden identificarse actividades sospechosas así como sujetos ligados a la misma. La identificación de objetivos significativos facilita las decisiones de asignación de recursos a los responsables de las agencias de fuerzas de seguridad, siempre con el objetivo de combatir la actividad terrorista de forma **proactiva.**

Desde un plano más estratégico y aplicando al concepto la teoría del espectro que difumina las barreras entre lo estratégico, lo táctico y lo operacional, quiero manifestar la tremenda importancia de obtener y mantener una visión global a través de una concepción axiomática del riesgo y la amenaza terrorista (detectar cualquier problema en cualquier parte y a cualquier nivel). Para ello es necesario el desarrollo y la gestión de un sistema de alerta basado en indicadores resultantes de la ponderación de las conclusiones obtenidas en los informes de inteligencia, producidos a partir del conocimiento del dominio del mundo real de la organización terrorista y de la actividad criminal desarrollada o en preparación. A este respecto existen modelos interesantes que permiten obtener una evaluación permanente de las intenciones terroristas, su capacidad de acción y la vulnerabilidad de los objetivos a su alcance.

Un sistema de alerta estratégica funcionaría sobre las siguientes premisas:

- Carece generalmente de redes de información propia.
- Se alimenta de información operativa previamente elaborada y produce generalmente productos de inteligencia estratégica.
- Prioriza indicadores y factores sobre escenarios y actores.
- Es un sistema orientado al conocimiento y a la previsión.
- Se basa en la obtención de superioridad informativa.

El sistema monitoriza un centenar de indicadores agrupados en los tres principales componentes de amenaza que generan "riesgo terrorista":

- Intenciones terroristas.
- Capacidad terrorista.
- Vulnerabilidad de objetivos.

Los perfiles de analistas necesarios serían tres:

- Evaluadores de informes (información e inteligencia de fuentes propias y de otras fuentes).
- Evaluadores de indicadores (crean, priorizan y actualizan).
- Evaluadores de alerta (niveles de alerta de intención, capacidad y vulnerabilidad).

Desde el punto de vista operativo una aproximación bastante exacta de los procesos a realizar por la unidad de alerta estratégica serían los siguientes:

FASE 1. Definir y validar los elementos esenciales de información usando indicadores:

- T1. Identificar y validar indicadores (tarea semestral o anual).
- T2. Priorizar indicadores (tarea semestral o anual).
- T3. Desarrollar y validar el conjunto de elementos clave de cada indicador (tarea semestral o anual).

- T4. Priorizar elementos dentro del conjunto de elementos clave de cada indicador (tarea semestral o anual).

FASE 2. Consolidación de información:

- T5. Recibir e integrar los informes de inteligencia de los distintos cuerpos y fuentes clave monitorizadas por el sistema (tarea diaria).

FASE 3. Ordenar la información usando juegos de hipótesis:

- T6. Categorizar la información mediante indicadores, elementos clave, objetivos, regiones, países, grupos terroristas, etc. (tarea diaria y continua).
- T7. Crear las Matrices de Hipótesis de objetivos potenciales a partir de la información consolidada agrupada por indicador (tarea diaria y continua).
- T8. Chequear las hipótesis y la validez de la información que las sustentan (tarea diaria y continua).

FASE 4. Desarrollar conclusiones (Inteligencia-producto) usando técnicas estructuradas y basadas en el conocimiento experto del analista:

- T9. Obtener los niveles de alerta de los indicadores combinando la prioridad del indicador y los niveles de actividad determinados en el mismo (tarea diaria).
- T10. Obtener los niveles de alerta de intención terrorista (tarea diaria).
- T11. Obtener los niveles de alerta de capacidad terrorista (tarea diaria).
- T13. Obtener los niveles de alerta de vulnerabilidad (tarea diaria).
- T14. Obtener los niveles de alerta de riesgo en objetivos terroristas (tarea diaria).
- T15. Obtener los niveles de alerta de riesgo en ciudades, regiones o países (tarea diaria).

- T16. Elaborar un análisis de tendencias de los indicadores de alerta (tarea mensual).
- T17. Elaborar un análisis de tendencias de los niveles de alerta de riesgo en objetivos (tarea mensual).

FASE 5. Desarrollar y refinar productos de inteligencia (tarea diaria, semanal o requerida).

- T18. Escribir un informe de análisis orientado a los proveedores de información operativa sobre lo que conocemos, lo que pensamos y lo que necesitamos conocer.
- T19. Escribir un sumario ejecutivo sobre lo que conocemos, lo que pensamos y lo que necesitamos conocer de los indicadores de alerta.
- T20. Escribir un sumario ejecutivo sobre lo que conocemos, lo que pensamos y lo que necesitamos conocer del riesgo en objetivos.
- T21. Escribir un sumario ejecutivo sobre lo que conocemos, lo que pensamos y lo que necesitamos conocer de las tendencias de escalada de los distintos grupos terroristas.

FASE 6. Difundir productos de inteligencia (cuando sea requerida):

- T22. Informar al consumidor de inteligencia vía web, informes escritos o cara a cara.
- T23. Enviar un informe complementario al consumidor de inteligencia cuando aparezcan nuevas evidencias, información significativa o por requerimiento explícito del mismo.

Desde el punto de vista funcional, un sistema como éste se conforma como un Portal Integrado de Inteligencia que se mantiene a partir de la implementación de un flujo operacional de producción de inteligencia de alerta estratégica basado en la obtención de evidencias e informes operativos. Estos se someten a un proceso normalizado de construcción de indicadores escalares que indiquen el grado de alerta. Una visión grafica de un sistema de este tipo puede verse en las figuras 5, 6, 7, 8.

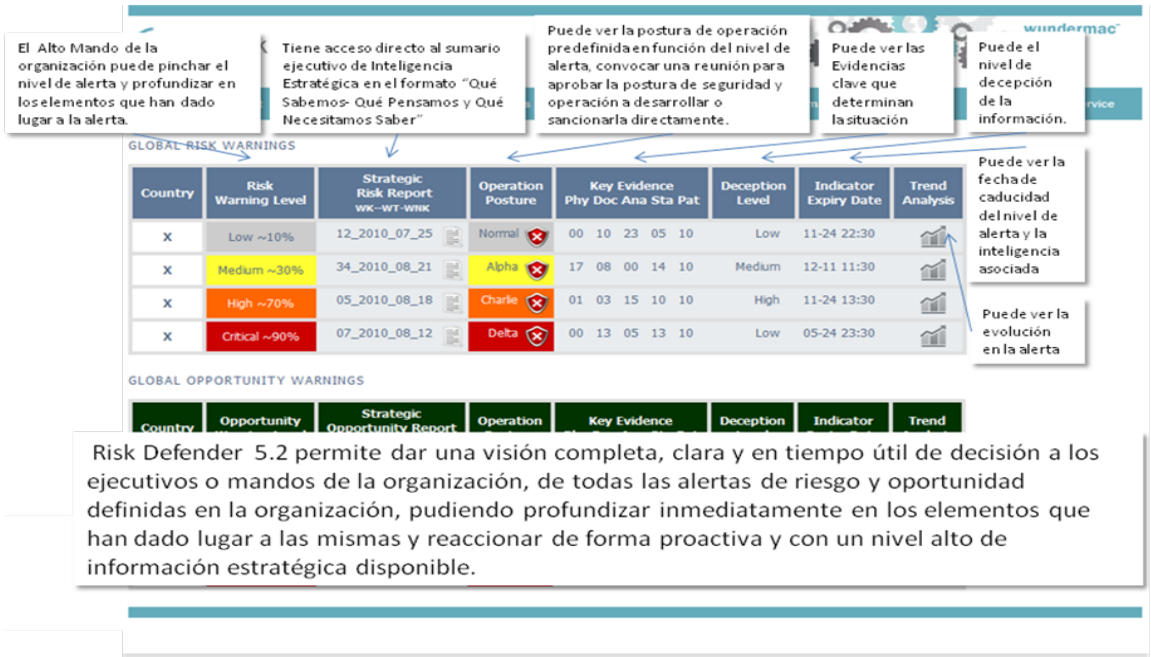

Figura 5. Niveles de alerta y seguridad por países, regiones, etc.

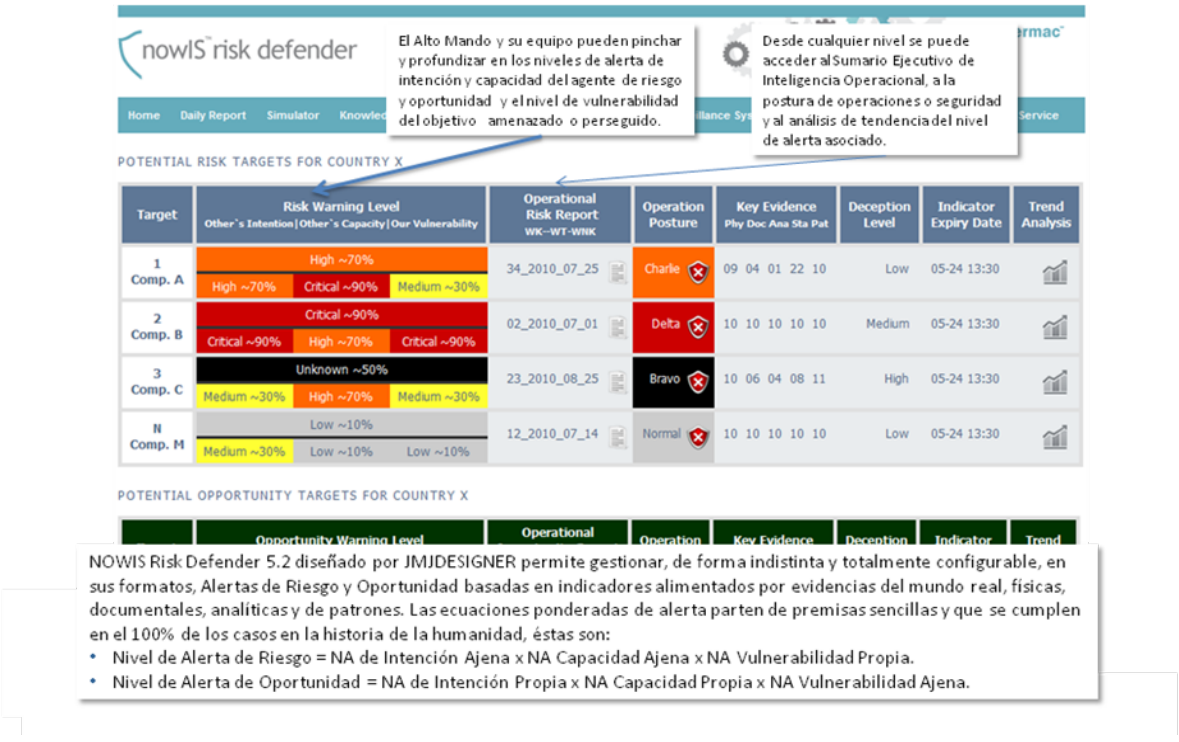

Figura 6. Indicadores de intención, capacidad y vulnerabilidad por país, objetivo y red terrorista.

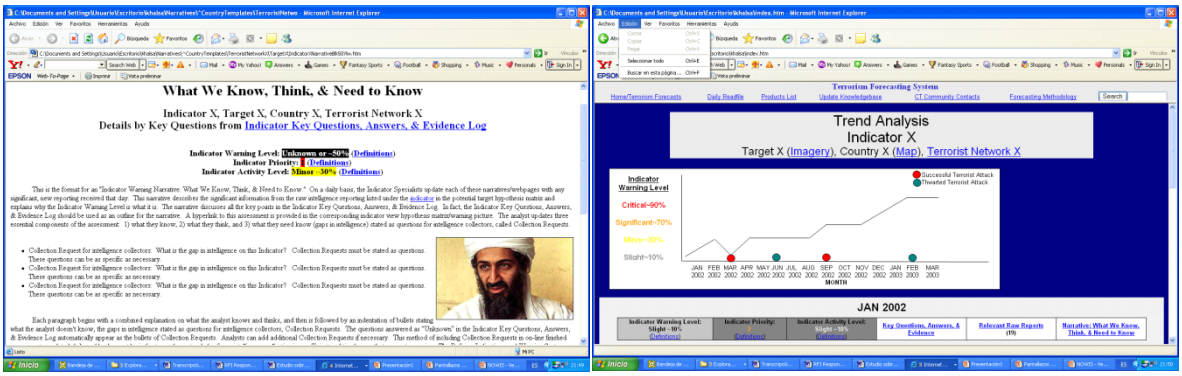

Figura 7. Indicadores de intención de ataque a un objetivo en un país e informes y evidencias asociadas que lo sustentan.

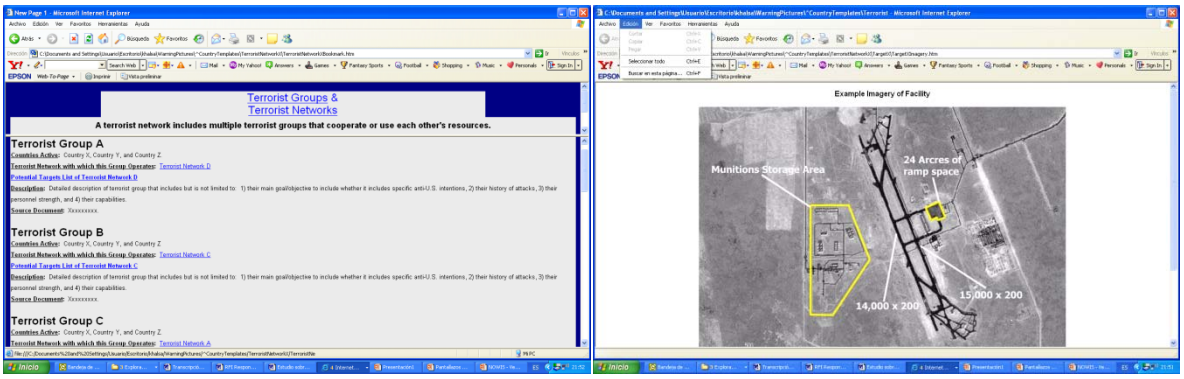

Figura 8. Informes de inteligencia que ofrecen hechos y evidencias y sustentan los valores de los indicadores respectivos: 1. Informe de evidencias y conclusiones sobre lo que sabemos, lo que pensamos y lo que necesitamos saber de la intención de un ataque terrorista en un país X y un objetivo Y. 2. Informe temporal de actividad. 3. Informes sobre las redes terroristas implicadas. 4. Informe de vulnerabilidad del objetivo.

Como antes mencionamos, es necesario establecer un flujo continuo de procesos de obtención, investigación y análisis que de soporte a un plan maestro de captación y producción de inteligencia (figura 9).

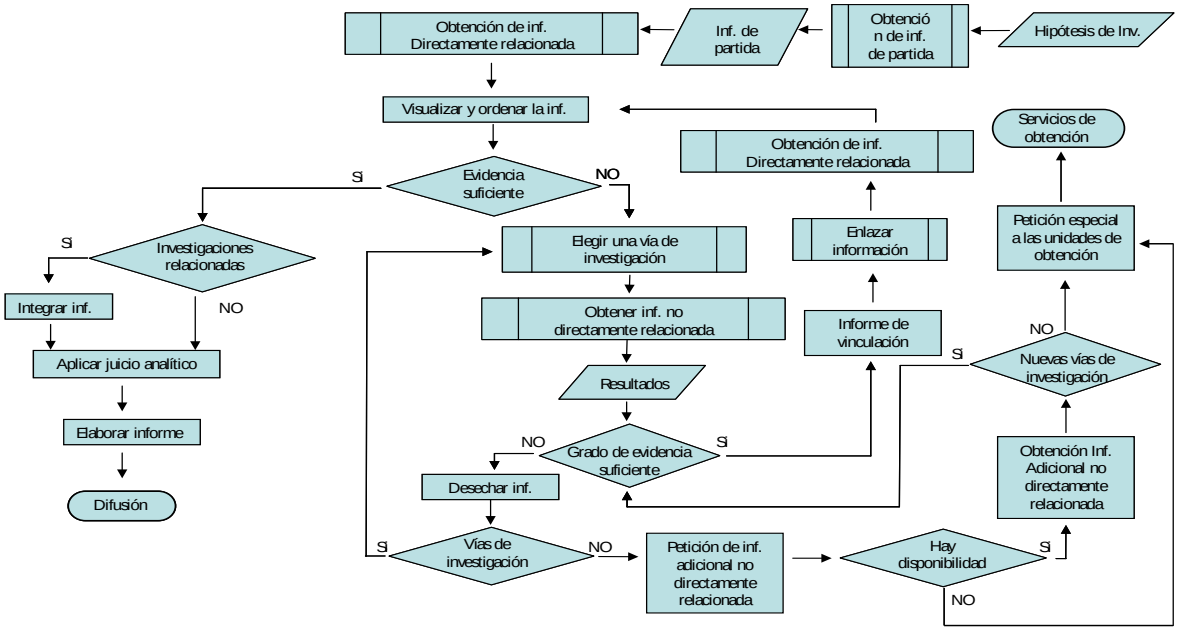

Figura. 9. Flujo de producción de inteligencia basada en evidencias. Metodología EELD 2.2.1.

Finalmente, no querría pasar por alto algunos temas tales como la necesidad de crear unidades de inteligencia especiales dedicadas a evitar a toda costa la tenencia y el uso de armas de destrucción masiva por parte de grupos terroristas. En este sentido, modelos como el de Mengel y otros aplicados sobre los enfoques anteriormente citados, pueden ser relevantes y urgentes de implementar. Sobre este tema trataré en un próximo trabajo denominado "Pensando en lo impensable en el siglo XXI", donde desarrollo un estudio comparativo con el trabajo realizado por Hermann Kahn en el Hudson Institute; en dicho trabajo Kahn introduce la escalera de escalada como una metáfora útil para la previsión de una crisis nuclear. Asimismo me gustaría dejar constancia de la necesidad de utilizar modelos prospectivos como el MACTOR de Godet que permite fijar la estrategia de los actores y simular su comportamiento en función de escenarios y objetivos; los modelos conductuales de Crelinsten que permiten realizar análisis

coste-beneficio; los sistemas de negociación y compensación de Bobrow y los juegos de predicción que tienen por objetivo superar la inventiva terrorista y anticiparse a nuevas formas de actuación. Todos estos enfoques serán tratados de forma amplia en próximos trabajos.

Conclusiones

Sin querer extenderme mucho en las conclusiones de lo expuesto, ya que considero que en una disciplina tan compleja como la inteligencia no hay verdades absolutas ni debe haber planteamientos dogmáticos o reaccionarios, me gustaría fijar algunas ideas generales que por su importancia quiero reseñar:

- Actualmente los gobiernos y las organizaciones de inteligencia están priorizando cambios estructurales sobre cambios metodológicos que a mi juicio impactan poco o nada sobre la función de utilidad de los servicios de inteligencia en el ámbito antiterrorista.
- Lo anteriormente expuesto se agrava y acentúa con el uso poco estratégico, bastante endogámico e instrumental de las nuevas tecnologías en la comunidad de inteligencia.
- No estamos ante nuevos problemas de inteligencia derivados de nuevas amenazas sino ante viejos problemas evidenciados por estas nuevas amenazas.
- Es en el análisis más que en la obtención de información en donde debemos poner el énfasis para mejorar los procesos de inteligencia.
- El modelo de trabajo intuitivo y poco estructurado basado en que "cada maestrillo tiene su librillo", es la norma habitual de trabajo en la comunidad de inteligencia y ha demostrado plenamente su ineficacia.
- Existen modelos de referencia probados y maduros que permiten establecer un marco razonablemente normalizado de

procedimientos de actuación y métricas de evaluación del desempeño de los mismos.

- Finalmente, para abordar con eficacia las amenazas terroristas que se ciernen en torno a los ciudadanos de los distintos países, se debe exigir cambios notables en la formación del personal encargado de la producción de inteligencia, en el conocimiento de la función de utilidad de los servicios de inteligencia por parte de los políticos y en la transferencia y asimilación de estrategias, métodos y nuevas herramientas por parte de las organizaciones de inteligencia.

JMJDESIGNER 2011