ieee.es
Instituto Español de Estudios Estratégicos

Documento
Opinión

49/2015 14 de mayo de 2015

*Juan Pablo Somiedo García**

LA SCA (SIGNAL-CONDITION-ACTION) COMO TÁCTICA TERRORISTA

LA SCA (SIGNAL-CONDITION-ACTION) COMO TÁCTICA TERRORISTA

Resumen:

La evolución del fenómeno terrorista para adaptarse a las nuevas circunstancias también se manifiesta en su modus operandi. Dentro del amplio campo de las TPP´s (Terrorist Tactics, Techniques, and Procedures), este artículo describe la táctica SCA (señal, condición, acción) como táctica empleada por los terroristas para atentar desde dentro del propio país.

Abstract:

The evolution of the terrorist phenomenon to adapt to new circumstances is also evident in its modus operandi. Within the broad field of TPP's (Terrorist Tactics, Techniques, and Procedures), this article describes the SCA tactics as a tactics used by terrorists to attack from within the country itself.

Palabras clave:

Tácticas terroristas, TPP´s, SCA (Señal, Condición, Acción), Kill Chain.

Keywords:

Terrorist tactics, TPP's, SCA (Signal, Condition, Action), Kill Chain.

INTRODUCCIÓN

El fenómeno del terrorismo no es ni mucho menos algo estático e invariable en el tiempo, sino que va adoptando diferentes formas y adaptándose a un entorno cambiante para lograr sortear a las fuerzas y cuerpos de seguridad del estado y lograr sus objetivos. Al mismo tiempo, las estrategias, tácticas y elementos operativos también van evolucionando, algunas son transformaciones de ideas antiguas desde un nuevo enfoque, otras resultan completamente novedosas. Además, la entrada en escena de las nuevas tecnologías de la información y comunicación posibilitan la implementación de nuevos métodos y tácticas y la transmisión indirecta de conocimiento de unos grupos terroristas a otros sobre ellas. No por casualidad, el actual director de la CIA, John O. Brennan aseguraba recientemente que la tecnología y los medios de comunicación social han amplificado la amenaza del terrorismo.
Las nuevas formas del terrorismo, considerado como una forma de guerra asimétrica, no enfatizan la búsqueda de una paridad de fuerzas, sino que el empleo de tácticas y medios no convencionales con una tendencia marcada a utilizar medios civiles (por ejemplo, los medios de transporte) como originales armas de guerra. (Aznar, 2011, p.3).

Como ya escribí en otra ocasión, los grupos terroristas son como los virus, en el sentido que se adaptan bastante bien al medio y las circunstancias. Pronto vieron que una estructura bien organizada en red era también más vulnerable. La existencia de un mando central o de una instrucción precisa ya no resultaban imperativas. De igual forma, la devaluación de la importancia del orden y la jerarquía es un subproducto propio de la globalización. Por eso comenzaron a operar en células independientes, pero, evidentemente, a estas células independientes les es más difícil comunicarse entre sí y planificar atentados simultáneos por el riesgo a ser descubiertas. Como contrapartida les resulta más fácil desafiar a estructuras jerárquicas tradicionales como son los sistemas de estado-nación, las policías y los ejércitos nacionales. Más tarde, el terrorismo polimórfico adoptó otra forma inesperada. Los denominados “lobos solitarios” saltaron a escena. Más difíciles de localizar y de calibrar en sus intenciones suponen un peligro grave pero, lógicamente, su capacidad de actuación está limitada a ataques secuenciales. (Somiedo, 2013, p. 12).

El papel de los TPP´s (Terrorist Tactics, Techniques, and Procedures) dentro del campo del análisis de inteligencia abarca el estudio de los patrones de comportamiento tanto de terroristas individuales como de organizaciones terroristas y el examen y categorización de las tácticas más generales y el tipo de armas utilizadas. Los TPP´s utilizados evolucionan y varían motivados por tres factores principales: circunstancias cambiantes, disponibilidad de recursos y cambio de ideología o de enfoque.

En este trabajo pretendemos estudiar en profundidad una de las tácticas terroristas cuyo uso se está extendiendo con aparente éxito dentro del grupo de las tácticas terroristas

empleadas para atentar desde dentro del propio país. Por evidentes razones, no plantearemos soluciones, aunque las hay y los diferentes organismos dedicados a la seguridad y la defensa las conocen, pero puede ser que el lector avezado descubra pequeñas migas de pan que señalan el camino a lo largo de la lectura del presente artículo. La SCA forma parte de ese vocabulario, a menudo complejo y abstracto que emplean los analistas para referirse a diferentes sucesos o eventos, bien sean de carácter político, social o, como en este caso, de índole terrorista. La complejidad llega hasta tal punto que apenas es necesario referirse por el nombre a los sucesos o personas involucradas sino que se utiliza toda una jerga conceptual para hacerlo, completamente ajena a profanos en la materia. La SCA es uno de esos conceptos.

La idea de no recibir órdenes ni indicaciones directas para llevar a cabo una acción no es ni mucho menos algo novedoso. Los agentes de los servicios de inteligencia conocen esta táctica de primera mano. Su uso se popularizó durante la guerra fría, cuando los agentes al otro lado del Muro de Berlín debían ser autosuficientes y tomar decisiones sobre la marcha sin esperar el visto bueno de sus superiores, pues toda posible comunicación entrañaba un riesgo difícil de calibrar.

Básicamente la teórica de la SCA dice que, en vez de utilizar la comunicación directa, se utilicen otras señales que adviertan al terrorista o terroristas en cuestión, la necesidad de actuar, bajo unas determinadas circunstancias previamente acordadas y estudiadas. La tipología de esas señales es muy variada y puede incluir desde sucesos o eventos, personas o incluso mensajes encriptados en prensa o en determinadas páginas web[1], como hace tiempo descubrió la inteligencia israelí. De la mera definición teórica se desprenden, al menos, dos dificultades: la posibilidad de que la confidencialidad de la señal en cuestión sea vulnerada y la segunda que las circunstancias no estén claras. Esto es, la incertidumbre y el riesgo siempre van a estar presente de una u otra forma.

De alguna forma, tácticas como la SCA vienen a terminar con el sueño de los servicios de inteligencia de controlar todo mediante la interceptación sistemática de las comunicaciones y el uso de la inteligencia de imágenes por satélite. Si no hay comunicación, no es posible interceptar nada. Alguien escribió que no hay nada más hermoso que el silencio. Para un servicio de inteligencia nada hay tan peligroso como el silencio.

[1] Un ejemplo de esta manera de proceder tiene que ver con el uso de coordenadas geográficas. Gracias a la posibilidad de consultar los mapas de Google, cualquiera puede obtener una localización si conoce las coordenadas. Éstas suelen ocultarse en sitios web como Ebay o Reddit, en páginas pornográficas o en los comentarios de diferentes videos de Youtube que previamente han sido seleccionados para esto por los individuos involucrados.

SIGNALS

Como en tantas otras ocasiones, la naturaleza se muestra como una hábil maestra cuando de adaptarse y sobrevivir se trata. Los seres humanos tratamos de replicar, a nuestra manera, muchos de los mecanismos utilizados por los animales. Uno de ellos está estrechamente relacionado con lo que estamos estudiando: la estigmergia.

La estigmergia[2], concepto introducido por el biólogo francés Pierre-Paul Grassé en 1959 para referirse al comportamiento de las termitas, hace referencia al hecho de que la coordinación de tareas no recae directamente sobre los agentes, sino sobre el entorno o medio físico. Hay unos mecanismos de coordinación y colaboración entre los agentes y actores del medio ambiente o entorno. La huella/acción dejada en el entorno o medio físico estimula la realización de una próxima acción/huella, tanto por el mismo como por otro agente diferente. En este esquema, las actividades de cada individuo no son controladas de forma directa, pero resulta necesario establecer un mecanismo de control indirecto. Es decir, desaparece el control centralizado para llegar a las acciones globales que repercuten positivamente en el sistema (Somiedo, 2014, p.9).

Sin embargo, hay una notable diferencia, pues mientras la inteligencia de enjambre es ciega debido a su escasez de holopticismo o visión de la totalidad completa y actualizada, esto no sucede así con los terroristas que sí tienen esa visión de conjunto que les permite calibrar de alguna forma el impacto de sus actuaciones dentro del conjunto global.

Así pues, los terroristas ya no necesitan comunicarse directamente con la cúpula de la organización a la que pertenecen, ni utilizar el teléfono móvil ni los correos electrónicos para saber exactamente lo que tienen que hacer, cuando y bajo qué circunstancias. Basta acordar previamente con el receptor el tipo de señales que se usarán, las condiciones y acotaciones de partida y las restricciones.

Pero, ¿Cuáles son los elementos definitorios de una señal?. En primer lugar una señal debe codificarse y descodificarse en un lenguaje común utilizado tanto por el emisor como por el receptor. En segundo lugar, la señal debe responder a una o varias de las tres W principales, esto es, Dónde (where), cuando (when) y Whom (A quién).

La tipología de señalas empleada es muy amplio, casi tanto como la imaginación de los propios terroristas pero, a grandes rasgos, pueden agruparse en tres grandes grupos:

[2] Etimológicamente el término deriva de las palabras griegas estigma στίγμα “marca, señal” y “trabajo”, laacción” ἔργον ergon.

- **Señales espaciales**: la identificación del lugar del acto terrorista es de suma importancia. Puede hacerse mediante el uso de coordenadas geográficas, como, por ejemplo, se especifica en la nota a pie de página número 1 de este trabajo. Es notable el grado de sofisticación que pueden alcanzar los terroristas, distribuyendo cuatro o cinco coordenadas de lugares diferentes para que luego el terrorista pueda calcular el centro de gravedad y, por tanto, las coordenadas del lugar exacto donde debe llevar a cabo su acción[3]. No obstante, esto último, aunque más difícil de descubrir por las fuerzas y cuerpos de seguridad del Estado (es más fácil descubrir unas coordenadas que cuatro o cinco), también es más arriesgado, pues un solo error en una de las coordenadas o un fallo a la hora de calcular el centro de gravedad puede arrojar un resultado final completamente diferente.

Si de coordenadas hablamos, también se han dado casos curiosos, como el del terrorista Abu Abdul-Rahman, también conocido como Mark Taylor, que publicó varios mensajes por medio de su cuenta en la red social Twitter, los cuales incluyeron coordenadas geográficas, facilitando así el rastreo de los puntos geográficos exactos donde había estado. Abu Abdul-Rahman se dio cuenta muy tarde del error, borrando 45 mensajes de la red social. En la actualidad su cuenta Twitter ya no existe[4].

Otra de las formas utilizadas consiste en señalar el lugar físico exacto mediante el uso de simbología o calificativos camuflados en determinadas páginas web. Por ejemplo, puede ser que para un ciudadano cualquiera “la Casa” signifique exactamente eso, pero seguramente para un agente del CNI significa otra cosa completamente diferente. Frecuentemente este tipo de “dobles significados” o “significados simbólicos” de las palabras requieren, para su correcta traducción, el concurso no sólo de especialistas en la lengua sino también de la cultura propia de los emisores. El Mossad, por ejemplo, ha contratado especialistas en lengua y cultura árabe, urdu y pashto.

[3] Para los profanos en la materia señalamos que, aunque hay software disponible para calcular automáticamente los centros de gravedad, también se puede hacer a mano con unos sencillos cálculos de la media de las X y la media de las Y.
[4] Fuente información e imagen: http://www.larepublica.pe/02-01-2015/supuesto-soldado-del-estado-islamico-revela-su-localizacion-sin-darse-cuenta

- **Señales temporales**: las señales temporales revisten una complejidad más alta, pues pueden consistir en meras fechas y números, dentro de una franja horaria determinada, o en determinados eventos o sucesos que, incluso, pueden ser iterativos, esto es, uno no sucederá hasta que otro previamente haya sucedido. Es una forma de lograr una simultaneidad operacional retardada[5]. Este último aspecto reviste una clara acotación a la actuación del terrorista, que debe esperar a que el suceso acordado tenga lugar para actuar.

- **Targets**: aquí nos referiremos con esta palabra a los objetivos humanos, esto es, actuaciones o acciones de asesinato contra blancos humanos. Pueden ser individuales, grupos determinados o indiscriminados contra el conjunto de la población. Por grupos concretos, los que tienen más alta probabilidad (en términos de frecuencia) de ser atacados son empresarios y ejecutivos, los miembros del gobierno y los diplomáticos(ver gráfico de la p.11). Cabe notar, también, que los propios terroristas pueden ser objetivo de su propia organización o de otras por diferentes motivos. De hecho, las luchas internas por el poder y el control en una organización terrorista suelen ser igual de encarnizadas o más que en cualquier otro tipo de organización y más cuando los líderes o cabecillas de referencia son

[5] La simultaneidad operativa puede ser sincrónica (al mismo tiempo) o retardada (una acción justo después de la otra, logrando un efecto parecido a la primera).

eliminados o encarcelados. Los nuevos aspirantes a liderar la organización necesitan demostrar, de algún modo, su capacidad. Por este motivo los atentados suelen recrudecerse con la encarcelación o eliminación de un líder y suelen ser mucho más sanguinarios, si cabe. A este respecto, es interesante leer el trabajo de Aaron Mannes que figura en el apartado bibliográfico de este artículo.

Una de las formas más tradicionales de agrupar información de una manera disimulada es utilizar vectores y matrices. Por ejemplo, un vector con cuatro componentes (cuatro números) puede aportar información sobre donde (primer número), cuando (segundo número), a quién (tercer número) y cómo (cuarto número). Una manera muy sencilla de obtener mucha información de una forma sencilla si previamente se conoce el significado de cada uno de los números. Las matrices pueden almacenar mucha más información ordenada en n*m filas y columnas. Otra, más moderna, se basa en la estenografía básica y su capacidad para ocultar información en imágenes de una manera sencilla.

CONDITIONS

Mientras las señales dejan poco espacio para la interpretación del terrorista, no sucede lo mismo con las condiciones sobre todo si cuando son condiciones en negativo o restricciones. De hecho ésta es, con mucho, la parte más compleja del proceso. En ocasiones, aunque el terrorista conoce de sobra las condiciones de su actuación se ve imposibilitado materialmente para cumplirlas debido a las circunstancias o a su propia ineficacia. Aunque suene a chiste ya se han dado casos en los que el terrorista, sencillamente, se ve imposibilitado para llegar al objetivo o sospechosamente se queda dormido durante varias horas. Morfeo, casualmente, o no tanto, ha jugado a favor de los “buenos” en más de una ocasión. La condición o condiciones es una especie de “disparador de la acción”, esto es, una indicación clara de que debe o no debe actuarse.

Cabe distinguir dos tipos de condiciones: condiciones en positivo y condiciones en negativo, también conocidas como restricciones a la actuación.

- **Condiciones en positivo:** hacen referencia a las condiciones o circunstancias que el terrorista debe observar para actuar. Un ejemplo puede ser la espera por una determinada acción de otro terrorista para actuar justo después y lograr una simultaneidad operativa retardada que obligue a las fuerzas y cuerpos de seguridad del Estado a dividir sus efectivos. Tal fue el caso, por ejemplo, de los atentados en París donde Amedy Coulibaly esperó a la actuación de los hermanos Kouachi. Pero también puede serlo la celebración de un determinado evento o la visita de un

dignatario extranjero, entre otros. Estas condiciones frecuentemente no resultan problemáticas para el terrorista, pues conocidas de antemano solo tiene que tener la calma y paciencia suficientes para esperar. Pero cuando las condiciones de espera son difíciles debido a la necesidad de esconderse y pasar desapercibido, la inquietud y la ansiedad pueden hacer fácilmente en la psicología del terrorista.

- **Restricciones:** hacen referencia a una serie de condiciones o circunstancias bajo las cuales el terrorista tiene completamente prohibido actuar. Aunque últimamente no es el caso del terrorismo de carácter yihadista, como estamos hablando en general, podemos citar la restricción sobre asesinar población civil de la misma etnia, cultura o religión, la restricción impuesta por salvar a un informador, la restricción impuesta por un cese del fuego o una tregua concertada, las restricciones en cuanto a procedimientos (a veces el acto terrorista debe, obligatoriamente, llevarse a cabo de una determinada manera y no de otra por la carga simbólica, dificultando con ello la ejecución de la acción). Cabe señalar la autoinmolación o suicidio como uno de los procedimientos más extremos.

Resumiremos e ilustraremos la teoría expuesta con un caso real. Se trata del comunicado de Abu Muhamad al Adnani:

*"Si podéis matar a un infiel americano o europeo, especialmente a los vengativos y sucios **franceses**, o a un **australiano**, un **canadiense** o cualquier infiel de los que promueven la guerra infiel, incluidos los ciudadanos que han entrado en la coalición contra el Estado Islámico, confiad una vez más en Alá y matadles **de cualquier modo** o manera pero hacedlo"*
Es fácil identificar aquí la señal como el propio comunicado. Es una señal general pues no está codificada ni destinada a ningún receptor en concreto, sino a todos a la vez. Contiene dos condiciones: la primera de ellas está claramente compuesta por dos restricciones una dentro de otra: matar ciudadanos americanos o europeos, pero preferentemente francés, australiano o canadiense. La segunda en cambio es una condición no restrictiva que hace referencia a la forma de actuar: “de cualquier modo”.

Cuando la señal tiene lugar y una vez examinadas las condiciones y restricciones, el terrorista, por lo general, comienza una especie de protocolo que ha sido bien definido por Flaherty, basándose en el trabajo previo de Sullivan y otros, mediante el *modelo Kill Chain.*

El modelo *Kill Chain* es un patrón de actividad transaccional que describe una estructura de datos que conforman la actividad terrorista mediante una jerarquía de tareas y subtareas. Es decir, describe una secuencia de actividades desde la planificación y organización hasta la

puesta en escena de los recursos operativos. Podemos decir que el modelo *kill chain* describe, con carácter general, el modus operandi de los terroristas.

Los componentes del modelo son la preparación del ataque (que hace referencia sobre todo a la logística), el timeline de la ejecución, objetivos y planificación. Evidentemente algunos terroristas no siguen al pie de la letra estos procesos y podemos encontrarnos casos en los que se saltan una o varias etapas, pero el conocimiento de las excepciones no resta ni un ápice de importancia al esquema general a la hora de sistematizar los casos. Otra de las posibles lagunas, como explica Flaherty es que los terroristas planifiquen cosas grandilocuentes sin tener los medios técnicos para llevarlos a cabo. En estos casos, frecuentemente dan vueltas y vueltas en la planificación buscando la manera más eficaz de causar el mayor impacto, con lo que el resto de la cadena frecuentemente no llega a materializarse bien por discusiones entre los mismos terroristas o por la actuación de las fuerzas y cuerpos de seguridad (Flaherty, 2012, pp.63-64).

Como resultado de estos inconvenientes, según Flaherty debe reformularse el modelo configurando una cadena de actividades no lineal sino discontinua, algo que, dicho sea de paso, parece, a primera vista, más apropiado para encarar con seguridad un campo tan complejo y heterogéneo en medios, métodos y fines.

ACTIONS

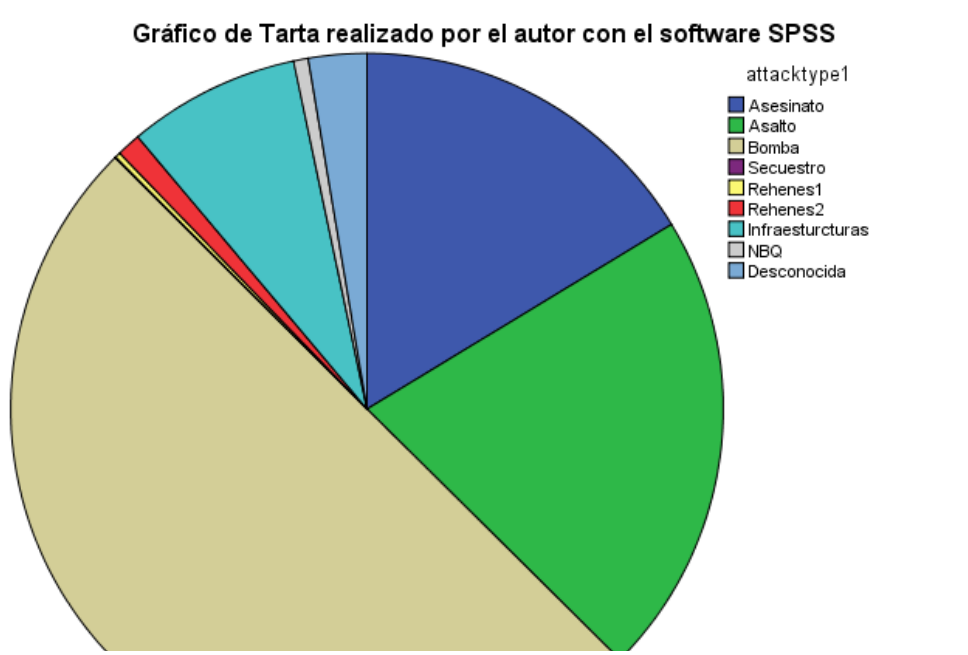
El catálogo de acciones terroristas es muy extenso. No es momento éste para describir todas y cada una de esas acciones, sino, más bien algunas tácticas que parecen importantes por su peligrosidad.

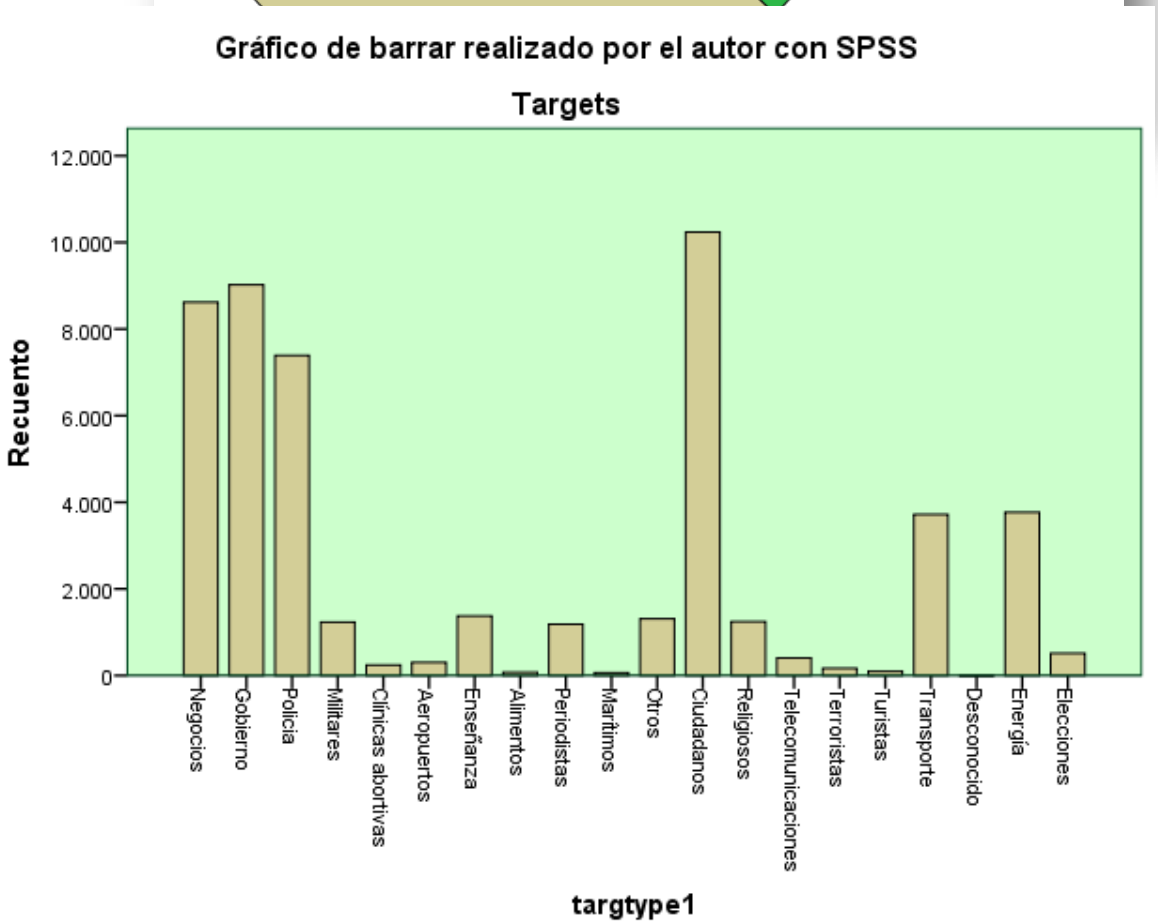
Una de las acciones más temidas por las fuerzas y cuerpos de seguridad del Estado, son los llamados “Embedded” o terroristas incrustados. Estos terroristas configuran una especie de acción retardada. Esperan a que se produzca el ataque principal y, si logran sobrevivir, ejecutan un nuevo ataque cuando las fuerzas de seguridad y los medios de rescate y socorro llegan al lugar, produciendo así nuevas bajas y sembrando el caos y el miedo (Flaherty, 2012, p.57).

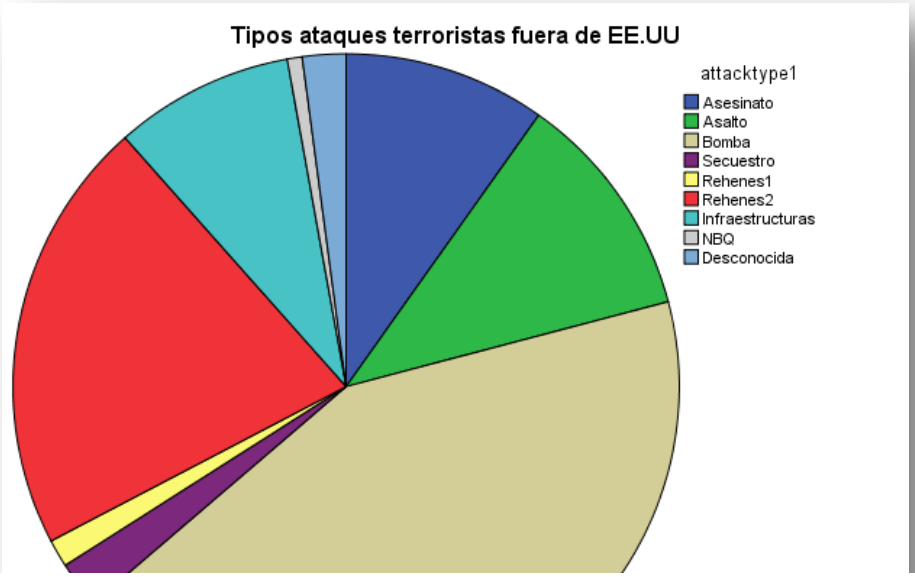
La simultaneidad sincrónica o retardada parece gozar también de un lugar de preferencia en la mente de los terroristas. Para su estudio en profundidad me permito remitir al lector a otro de mis artículos que figura en el apartado bibliográfico de este trabajo.

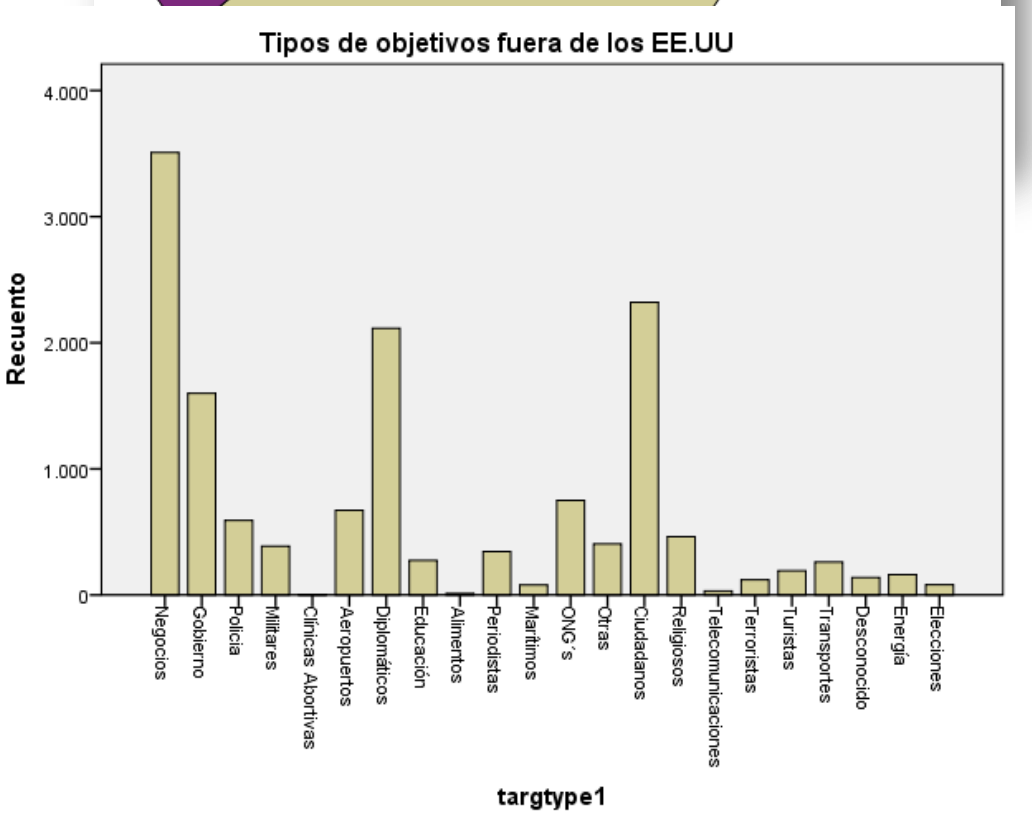
A continuación exponemos, de modo ilustrativo, la frecuencia de diferentes tipos de ataques y objetivos terroristas. Para su realización me he utilizado la base de datos de la Global Terrorism Database (GTD), disponible en http://www.start.umd.edu/gtd/. Para la

realización del análisis estadístico se han importado los datos (que originalmente estaban en formato Excel) en el SPSS y después se han limpiado. Los dos primeros gráficos hacen referencia a ataques producidos en EE.UU durante el periodo 1970-2010. Los dos siguientes se refieren a terrorismo global fuera de EE.UU en el mismo periodo.







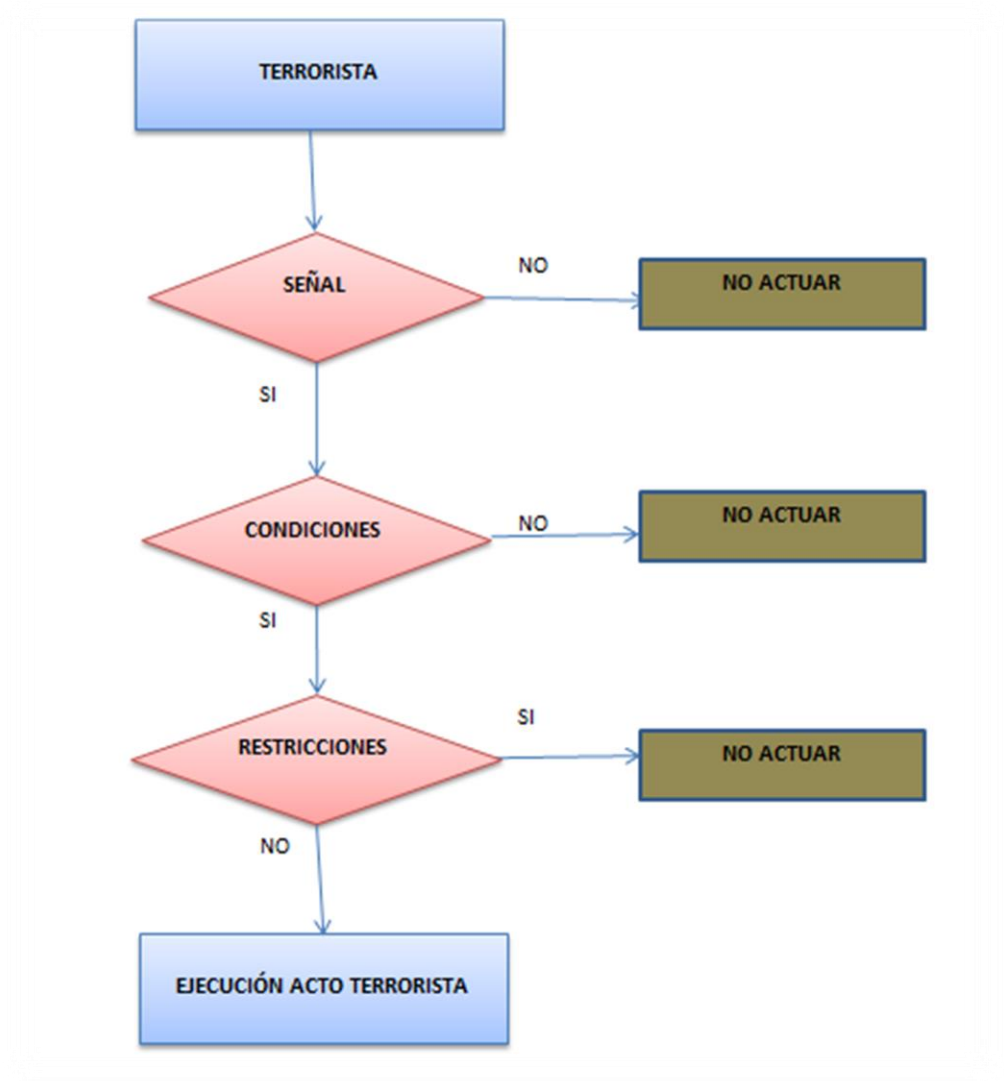


A partir de esta información (en este caso escogemos los ataques realizados fuera de EE.UU), utilizando la información sobre las frecuencias de cada evento y creando una sencilla tabla de contingencia, podemos establecer las probabilidades de varios eventos. En particular, si sabemos de antemano que el target u objetivo es un diplomático porque hemos logrado captar y descodificar las señales, podemos establecer las probabilidades "a priori" de que el tipo de ataque escogido por los terroristas sea una bomba.

		Negocios	Gobierno	Policia	Militares	Clínicas Abortivas	Aeropuertos	Diplomáticos	Educación	Alimentos
Asesinato	Recuento	199	215	51	48	1	5	280	17	0
	% dentro de targtype1	5,7%	13,4%	8,6%	12,4%	33,3%	0,7%	13,2%	6,2%	0,0%
Asalto	Recuento	175	104	136	71	0	22	224	17	0
	% dentro de targtype1	5,0%	6,5%	23,0%	18,3%	0,0%	3,3%	10,6%	6,2%	0,0%
Bomba	Recuento	1686	612	247	189	1	328	1090	86	0
	% dentro de targtype1	48,0%	38,3%	41,8%	48,8%	33,3%	48,8%	51,5%	31,4%	0,0%
Secuestro	Recuento	17	4	0	0	0	225	4	4	1
	% dentro de targtype1	0,5%	0,3%	0,0%	0,0%	0,0%	33,5%	0,2%	1,5%	7,7%
Rehenes1	Recuento	18	14	3	2	0	8	48	3	1
	% dentro de targtype1	0,5%	0,9%	0,5%	0,5%	0,0%	1,2%	2,3%	1,1%	7,7%
Rehenes2	Recuento	851	556	94	45	0	7	143	106	1
	% dentro de targtype1	24,3%	34,8%	15,9%	11,6%	0,0%	1,0%	6,8%	38,7%	7,7%
Infraestructuras	Recuento	485	70	44	23	1	54	237	36	6
	% dentro de targtype1	13,8%	4,4%	7,4%	5,9%	33,3%	8,0%	11,2%	13,1%	46,2%
NBQ	Recuento	12	13	6	8	0	6	13	2	0
	% dentro de targtype1	0,3%	0,8%	1,0%	2,1%	0,0%	0,9%	0,6%	0,7%	0,0%
Desconocido	Recuento	66	12	10	1	0	17	76	3	4
	% dentro de targtype1	1,9%	0,8%	1,7%	0,3%	0,0%	2,5%	3,6%	1,1%	30,8%
	Recuento	3509	1600	591	387	3	672	2115	274	13
	% dentro de targtype1	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%

Observando la tabla, sabemos que la probabilidad, a priori (basándose en frecuencias) de que si el objetivo es un diplomático, la forma de ataque sea el uso de explosivos es de un 51.5%. Un riesgo elevado. De igual forma, si el objetivo es un empresario o un hombre de negocios, hay un 24.3% de probabilidades de que la intención sea capturarlo como rehén. El analista puede así calcular otras probabilidades similares. Lógicamente estas probabilidades nunca serán estáticas e irán modificándose conforme se introduce nueva información.

ARBOL DE DECISIÓN DE UN SCA



Muchas veces es suficiente con lograr descubrir y entender la señal para dar al traste con los planes de los terroristas. Pero obligatoriamente esto trae consigo seguir dos caminos paralelos, uno para interceptar la señal y otro para descubrir lo que significa. Para éste último se hace casi imprescindible la inteligencia humana, también conocida por sus siglas en inglés, HUMINT, que minusvalorada durante un tiempo por su riesgo y por la aparición de los modernos medios de interceptación de comunicaciones y visualización de imágenes mediante satélite, cada vez está tomando un mayor peso específico.

Pero los problemas para un servicio de inteligencia no terminan ahí, pues, muy a menudo se desconoce la identidad del terrorista en cuestión que va actuar. Y mucho más ahora, cuando el incremento del número de posibles terroristas en algunos países europeos hace

prácticamente imposible su control[6], con lo que hay que establecer prioridades y, claro está, se puede fallar a la hora de calibrar las intenciones de determinados individuos. Por otro lado, asociar señal e individuo es una cuestión complicada cuando el número de posibles combinaciones aumenta y éstas no pueden ser descartadas.

Una vez descubierta la señal, si se desconoce la identidad del individuo en concreto, caben, al menos, dos posibles actuaciones, ambas arriesgadas. La primera de ellas es preparar un plan de actuación con la información aportada por la señal e intentar eliminar al terrorismo cuando éste intente actuar. La segunda opción es mucho más arriesgada que la primera, pero a cambio aporta mejores réditos. Consiste en impedir de algún modo que el terrorista lleve a cabo sus intenciones pero sin eliminarlo. Después de haber fracasado en su intento, tanto el terrorista como los líderes de la organización se sentirán inclinados a descubrir qué ha sucedido. Además hay una mayor probabilidad de que el terrorista cometa el error de contactar con elementos de la organización en su misma área espacial o en otras. Esto hace que, una vez monotorizado, el terrorista, aún sin saberlo, esté aportando un flujo de información constante a los servicios de inteligencia.

Pero, frecuentemente, la organización sospecha de los terroristas que fallan en sus intentos, pues la desconfianza siempre está presente. Y aunque el terrorista siga convencido de que no ha podido actuar por “casualidades” o “impedimentos de última hora”, cabe la posibilidad de que los líderes de la organización o incluso sus propios compañeros sospechen que algo va mal y lo dejen a un lado de los planes de la organización aunque insista en colaborar. Si esto sucede, la baza se esfuma.

Sea como fuere, en la SCA tanto los terroristas como los servicios de inteligencia tienen que lidiar con la incertidumbre. Es una táctica igual de compleja para unos y para otros pero con una diferencia: los terroristas sólo tienen que tener suerte una vez y las fuerzas y cuerpos de seguridad del Estado la tienen que tener siempre.

i

*Juan Pablo Somiedo García**
Analista y Profesor Ciclo Superior Análisis en Inteligencia, UAM

[6] Tradicionalmente para hacer una vigilancia total de un individuo durante 24 horas varios dias se necesitan no menos de 20 hombres (interceptación de comunicaciones incluida). Otra opción son los sondeos, que consisten en interceptación de comunicaciones y vigilancia esporádica para calibrar los riesgos o amenazas que representan ciertos individuos.

BIBLIOGRAFÍA

- AZNAR, F. (2011). *Terrorismo y estrategia asimétrica*. Documento de Opinión, Instituto Español de Estudios Estratégicos (IEEE). Madrid. Disponible en: http://www.ieee.es/Galerias/fichero/docs_opinion/2011/DIEEEO09_2011TerrorismoEstrategiaAsimetrica.pdf
- FLAHERTY, C. (2012). *Dangerous Minds: A Monograph on the relationship between Beliefs-Behaviours-Tactics*. OODA LOOP. Disponible en: http://files.ooda.org/DangerousMinds.pdf
- MANNES, Aaron (2008) *The snake head Strategy: Does killing or Capturing its leaders*
- *reduce a terrorist group´s activity*, Journal of International Policy, vol. 9, pp. 40-49.
- SOMIEDO, J.P. (2013). *Simultaneidad operativa y su aplicación a operaciones no lineales de amplio espectro y a la lucha contraterrorista.* Documento de Opinión. Instituto Español de Estudios Estratégicos (IEEE). Madrid. Disponible en: http://www.ieee.es/Galerias/fichero/docs_opinion/2013/DIEEEO85-2013_OperacionesAntiterroristas_JPSomiedo.pdf
- SOMIEDO, J.P. (2014). *El análisis de información en entornos colaborativos*, Universidad Nacional de Educación a Distancia (UNED). Madrid. Disponible en: http://e-spacio.uned.es/fez/eserv/bibliuned:masterFilosofiaFilosofiaPractica-Jpsomiedo/Documento.pdf
- SULLIVAN, J.P. y BAUER, A. (Editores) (2008*). Terrorism Early Warning: 10 years of achievement in fighting terrorism and crime.* Los Angeles County Sheriff's Department. Los Angeles, California. Disponible en: http://shq.lasdnews.net/Content/uoa/SHB/publications/TerrorismEarlyWarning.pdf

Páginas web consultadas:

- Terrorism Database (GTD): http://www.start.umd.edu/gtd/