LA DEMOCRATIZACIÓN EN EL ACCESO A LA TECNOLOGÍA: INSURGENCIA, GUERRA ASIMÉTRICA Y EMPLEO DE TECNOLOGÍAS DE AMPLIA DIFUSIÓN.

FRANCISCO RAMÓN TRUJILLO FERNÁNDEZ
Licenciado en Comunicación Audiovisual (Univ. de Málaga)
Especialista Universitario en Seguridad Internacional (IUGM-UNED)
Experto Universitario en Criminología (UNED)

INTRODUCCIÓN

Resulta interesante analizar de manera sosegada el trasfondo de algunas noticias de prensa, que no por sensacionalistas (que también), no dejan de aportar indicios claros de cómo la Insurgencia islamista procura rentabilizar hasta el extremo las escasas herramientas de las que dispone, fundamentalmente para intentar doblegar maquinarias bélicas sin parangón en la Historia. Así, hace tiempo conocimos el siguiente titular:

*"**Insurgentes en Irak hackearon aviones no tripulados de EE.UU**"* (1)

Este encabezamiento, que perfectamente pasa desapercibido para el lector generalista o no especializado, encierra un verdadero elemento de disrupción en el acceso a la tecnología. Así, nos encontramos con que el concepto de David contra Goliat recupera una nueva dimensión interpretativa. Como veremos en este trabajo, no es tan sencillo acceder al empleo de alta tecnología por parte de la pléyade insurgente, pero sí que resulta asequible disponer de nuevas formas de comunicación como Internet y hacer uso de un mortífero artefacto explosivo improvisado. Así las cosas, el ejército más poderoso de EE.UU tiene verdaderos problemas en el enfrentamiento con guerrillas medievales, las cuales sin duda disponen de elementos tecnológicos de bajo perfil, pero que fundamentalmente cuentan con varios factores añadidos de acuerdo con el campo de batalla que se esté analizando, entre ellos, el elemento sorpresa y sobre todo, el extraordinario conocimiento del terreno (elemental en países como Afganistán, terriblemente montañoso y fuertemente hostil en el plano climático).

El objeto de este trabajo se cimenta en la necesidad de analizar cómo la insurgencia islamista en zonas de Yihad como Afganistán o Chechenia, dispone de interesantes accesos a la tecnología militar, que no radican tanto en la extrema sofisticación, como en el libre uso de tecnologías de amplia difusión. Resulta contradictorio que pequeños grupúsculos puedan hacer tanto daño a Unidades con alto nivel tecnológico, en el entendimiento de que la Insurgencia Islamista, interpretada según una mayoría de expertos como una forma de terrorismo, es una manifestación clara de la Cuarta Generación de las Guerras, y por consiguiente, cuenta con una dinámica diferente en cuanto al uso del elemento tecnológico, y sobre todo en cuanto a las *Reglas de Enfrentamiento.*

Resulta abrumadora la enorme cantidad de ocasiones en las que las tropas de la coalición en Afganistán se ven envueltas en ataques de la insurgencia, no solamente con fusiles de asalto, sino también por mediación de los llamados **IED`s**, acrónimo de "Improvised Explosive Device" o *"Artefacto Explosivo Improvisado".*

Estos artefactos explosivos han resultado verdaderamente letales para nuestras tropas, no sólo desde el punto de vista de las bajas, sino también como un factor de presión psicológica sobre los propios soldados. Su fabricación es relativamente barata y sin duda sus efectos logran infundir en el enemigo una percepción extrema de inseguridad. Progresivamente las tropas de la coalición han procurado aumentar los estándares de seguridad en sus movimientos así como el fortalecimiento de los blindajes de sus vehículos (2). Pero aún así la amenaza continúa estando latente. Un simple vistazo a la Historia bélica permite conocer claros ejemplos de cómo un enfrentamiento entre tropas regulares y guerrillas articuladas en estrategias de insurgencia, puede acabar siendo un auténtico suplicio parar batallones en principio mejor entrenados y con tecnología más avanzada, pero que no pueden hacer frente de forma eficaz a un "fantasma" que conoce a la perfección el terreno y que no duda en planear emboscadas imponiendo altas dosis de temeridad.

DIFICULTADES DE ACCESO A LA ALTA TECNOLOGÍA POR PARTE DE LA INSURGENCIA

El acceso a la tecnología ha permitido durante siglos materializar actividades que el ser humano por sí mismo no hubiera podido lograr. Uno de los principales problemas a los que nos enfrentamos radica a juicio de múltiples autores, en que esa tecnología efectivamente ha generado elementos de dependencia, con lo cual la propia sociedad moderna se ha vuelto mucho más expuesta y vulnerable a las actividades terroristas. El libre acceso a las tecnologías de la información no siempre congrega una política de buenas intenciones. También elementos terroristas de muy diverso calado (independentista, de corte religioso o revolucionario…) han hecho uso de los elementos tecnológicos, ya fuera para ocultar sus intenciones como para cifrar sus comunicaciones. Las Fuerzas de Seguridad y en el caso de los Conflictos Bélicos, los Ejércitos, se enfrentan a enemigos silenciosos que logran escabullirse con sigilos marcado en el abismo de las redes de información. En esta dimensión y tal y como plantea Brian Jackson en su *paper* sobre adquisición de tecnología por parte de Grupos Terroristas, lo cierto es que cada avance tecnológico tiene su contrapartida, dado que también de alguna forma nos volvemos mucho más vulnerables (3). Jackson apuesta por la idea de binomio, una especie de carrera armamentística, pero en este caso que no radica en la potencialidad balística, sino más bien en el matiz de cuál de los dos bandos -Estados de derecho y Grupos Terroristas- puede al final obtener el rédito tecnológico que más daño pueda hacer a su enemigo. Uno de los principales obstáculos a los que se enfrentan los Grupos Insurgentes y/o terroristas radica quizás en la necesidad de adquirir destrezas lo suficientemente significativas como para poder hacer uso de las herramientas de libre acceso que la actualidad Sociedad de la Información brinda a cualquier ciudadano.

De esta forma se entiende que el uso de herramientas como Internet en torno a los círculos insurgentes, requiera de destrezas eminentes como para poder establecer un aparato logístico sólido que permita obtener

financiación de diferentes fuentes globales, y que establezca rutas para la entrada de combatientes yihadistas en territorio bélico (Afganistán y en su momento Irak o incluso en el Cáucaso). Jackson incide en la necesidad que tienen estos grupos de publicitar su agenda con un incremento progresivo de sus capacidades tecnológicas. Es una presión constante a la que los Grupos Terroristas deben hacer frente para no caer defenestrados o incluso apartados por otros Grupos con superiores capacidades (4).

De otra parte, se confrontan dos conceptos diferentes muy bien planteados por el Autor Raymond F. Hain en su obra sobre usos y abusos de la tecnología (5). Rein ya consideraba a finales de los noventa la existencia por una parte de la Ciencia Militar, y por la otra del Arte Militar. A veces se circunscriben a un único concepto, pero en otras ocasiones parecen moverse en diferentes dimensiones. Lo cierto es que en los últimos años, la Insurgencia de corte Yihadista ha logrado fuertes dosis de lo que se entiende como Arte Militar. Raymond Hein entiende que el Arte Militar aglutina en un mismo compendio un estudio sistemático y la planificación creativa de las tácticas militares, lo cual sin duda requiere de altas dosis de audacia y en buena medida logra superar los obstáculos y las dificultades de una tecnología militar de última generación, ante la cual no pueden más que hacer frente con escasos medios y con más creatividad. En cualquier caso se produce cierto "*balance de poder*"(6) entre fuerzas terroristas y antiterroristas.

Diferentes estudios han demostrado que el proceso de adquisición de Tecnología por parte de Grupos Terroristas y/o insurgentes es en ocasiones un proceso laborioso y complicado, que en muchos casos imposibilita la obtención. En este caso, es interesante constatar que la consolidación del empleo de una tecnología (por ejemplo la implementación de un artefacto explosivo) requiere sobre todo de tiempo y de experiencia, y esto entra de plano en un dilema, puesto que muchos grupos terroristas cuentan con una vida corta. Por otra parte, la adquisición de nuevas tecnologías requiere de importantes recursos económicos, ya que es cara, muy cara, y ello supone que los Grupos deban disponer de un sobresaliente aparato logístico que se encargue de recibir remesas del exterior, o que gestione el robo de un banco –por resultar gráficos-.

Otra de las dificultades la encontramos en lo que Brian Jackson denomina "*dinámicas internas de grupo*". En la práctica esto supone que la estructura (ya sea piramidal o en células independientes) determina el resultado final del acceso a la tecnología. Si el líder busca "acción inmediata", ello redundará sin duda en una falta de cualificación para el empleo del material tecnológico. Es evidente pensar que todo dependerá del grado de dificultad de la tecnología; esto es, que no será lo mismo gestionar un envío de armas que el aprendizaje de un dispositivo explosivo casero. El mejor ejemplo de cómo el acceso a la tecnología no siempre encuentra su contrapartida en su uso correcto o efectivo lo hallamos en el libre acceso a una misma tecnología por parte de las multinacionales. Observaremos que el resultado final no siempre es el más eficiente, ni tan siquiera el más eficaz. Es por tanto un verdadero reto para las Organizaciones Terroristas y en especial para los Grupos Insurgentes el hacer frente a un proceso de adquisición tecnológica que al final puede acabar por generar más fricciones en el seno de los mismos.

CONTRAMEDIDAS TECNOLÓGICAS

A pesar de sus grandes limitaciones, la Insurgencia Terrorista también dispone de determinadas herramientas para hacer frente a la capacidad tecnológica del enemigo. Así, varios autores, entre ellos Brian Jackson establecen una determinada taxonomía de las contramedidas efectuadas por estos Grupos. Jackson *et al* (7) se preguntan cómo es posible derribar el muro de la Fortaleza enemiga, y responden con algunas iniciativas:

a) Alterando las prácticas operacionales: Lo cual no afecta en exceso a los objetivos operativos de la Insurgencia. Al moverse en células reducidas –al igual que los Comandos de Operaciones Especiales-, no encuentran demasiados problemas para cambiar sus posiciones en el Teatro de Operaciones y converge de alguna manera en el concepto de factor sorpresa.

b) Modificando su propia tecnología: Ello significa que al modificar los procedimientos

tecnológicos, se dificulta la capacidad de las medidas contrainsurgentes. Es decir, infringiendo un duro golpe a las Fuentes de Inteligencia de los Aliados en su permanente búsqueda de datos a través de la interceptación de las comunicaciones. Pero también puede significar una alteración en la manera de implementar un Artefacto Explosivo Improvisado.

c) Evitando los lugares en los que se encuentra la tecnología defensiva: Un punto que perfectamente entronca con el apartado a), y que resulta una obviedad: si el enemigo se encuentra en un Valle, podemos alejarnos del mismo y realizar incursiones puntuales.

d) Atacando de forma directa la tecnología aliada: Quizás el punto más complicado.

Otra de las dificultades de los Grupos Insurgentes en cuanto al acceso a la tecnología la hallamos en el apartado de contramedidas tecnológicas, puesto que se advierte una necesidad acuciante de tiempo y de recursos económicos de los que no siempre se dispone para innovar y sorprender. Jackson *et al* insinúan la existencia de una ***ventana de tiempo*** en la que únicamente es posible emplear determinadas contramedidas, y ello sin duda es un riesgo y un obstáculo operacional (8).

Al final, debemos convenir que los grupos insurgentes han optado por usos más económicamente accesibles, apreciando ciertos matices que les benefician, en un mundo fuertemente globalizado que emplea las Tecnologías de la Información y la Comunicación como parte indisoluble de las relaciones sociales y humanas. Precisamente aquí radica el verdadero Talón de Aquiles de las Fuerzas Multinacionales y una cierta libertad de movimientos por parte de la Insurgencia: libertad de movimientos tanto en el apartado de búsqueda de fórmulas de financiación como en el libre uso de tecnologías de amplias difusión, asequibles, baratas y fáciles de obtener.

GUERRAS DE CUARTA GENERACIÓN

La victoria frente a los Talibanes suponía un verdadero soplo de ánimo patriótico para los americanos tras los duros acontecimientos del 11 de Septiembre de 2001. El planeta entraba de lleno en un nuevo período histórico en el que el concepto de Superpotencia perdía fortaleza ante un enemigo invisible, que había logrado penetrar sus fronteras e infligir un duro golpe a la moral, la política y la economía estadounidenses. Un *Casus Belli*, en el que por fortuna parecía poder identificarse, aunque sólo en parte al enemigo. En Octubre de 2001, una coalición englobada en torno a la Operación Libertad Duradera inició el 7 de Octubre de 2001 la invasión de Afganistán. La victoria sobre los talibanes se pretendía rápida y eficiente, aunque más pronto que tarde, los fantasmas del pasado volverían a hacerse un hueco en las mentes y en los corazones de muchos americanos. Afganistán ha vuelto a convertirse tras el paso de los años en un nuevo terreno de *Jihad*, esto es, en una zona sagrada para el Islam en la que la expulsión del invasor es elemento indisoluble para la estabilidad de la UMMA o Comunidad de Creyentes. Afganistán y Pakistán se han convertido con el devenir de los acontecimientos, en una auténtica fábrica de exportación de combatientes, reconvertidos en muchos de los casos en embajadores del terror en sus países de origen. Desafortunadamente y tras varios años de conflicto, Afganistán se ha convertido en un terreno controlado por delincuentes, señores de la Guerra, grupos terroristas y en conclusión, en suelo abonado para el conflicto asimétrico. De hecho, la baja tolerancia de la Coalición a las bajas no ha hecho más que empeorar los efectos psicológicos promovidos por el uso de IED`s, los cuales, como ya veremos en páginas posteriores, logran con un nivel tecnológico reducido un número de bajas exponencialmente alto.

Una de las claves del conflicto asimétrico que se está desarrollando en las zonas de Yihad (Somalia, Afganistán, Pakistán, el Cáucaso ruso…) la resuelven de manera certera David García Cantalapiedra y Gustavo Díaz Matey (9), al manifestar que los insurgentes disponen de cualidades especiales para ocultarse entre la población civil después de golpear al enemigo. El insurgente dispone de un ***equipo de comunicaciones básico*** y cuenta con la proactividad necesaria para marcar su propio campo de batalla o de acción. Estos autores defienden la tesis de que la tecnología aplicada a la información ha cambiado la naturaleza del conflicto en el siglo XXI. Y mientras tanto, nunca ha sido tan evidente que

la mejor manera de luchar contra los estados es a través de conflictos de baja intensidad.

Los insurgentes cuentan con un extremado conocimiento del terreno, lo cual les permite buscar rutas de huida eficaces ante las embestidas de los soldados de la Coalición. Su dominio de las diferentes lenguas así como de la tradición local les ha permitido prolongar el conflicto hacia un estadio de presión psicológica sobre los invasores. A estas alturas de la campaña, la propia OTAN se manifiesta impotente ante las enormes necesidades de incrementar los presupuestos y el número de tropas destinadas a combatir la insurgencia afgana. En este contexto de dificultad, resulta a todas luces imprescindible considerar a las organizaciones insurgentes de corte terrorista como verdaderas precursoras de una nueva era de conflictos, planteamiento exhibido entre otros, por el Teniente Coronel David J. Kilcullen (10). Según este experto en contrainsurgencia, Al-Qaida ha conseguido adaptarse al nuevo entorno bélico con gran ligereza, aprovechando precisamente las lagunas de nuestras sociedades occidentales. Y precisamente esa facilidad de adaptación ha podido producirse en buena medida gracias a cierto cambio de actitud en el empleo de la tecnología. Así lo define el autor Antonio Giustozzi en su obra "*Coran, Kalashnikov and Laptop*".(11) Según Giustozzi (*apud Paula Hanasz*), los Talibanes han adoptado ciertos hábitos tecnológicos importados de los combatientes extranjeros/jihadistas procedentes de países occidentales.

El amplio espectro de uso de las tecnologías de la información de estos individuos ha posibilitado nuevos planteamientos metodológicos por parte de la Insurgencia: las cámaras de vídeo resultan un elemento muchas veces indispensable para distribuir por medio mundo y en pocas horas las hazañas de una célula insurgente frente a tropas de la ISAF puede ser difundida por medio mundo y comentada en los principales Foros Yihadistas. Como el propio Giustozzi indica, las motocicletas se han convertido en un medio rápido y eficiente de transporte por las zonas de combate, contando algunas de ellas con cargadores de teléfono móvil. En muchas ocasiones se ha priorizado el empleo de IED`s como elementos propagandísticos. Sólo así se entiende la enorme difusión que a través de Internet han tenido vídeos caseros de atentados terroristas contra convoyes que circulaban por carreteras de Irak o Afganistán.

En el siguiente apartado pasaremos a analizar algunos de estos dispositivos, elementos tecnológicos comunes para todos nosotros, de amplia difusión, sencillos de fabricar, baratos y de fácil acceso. Es la tecnología del siglo XXI adaptada al campo de batalla; por tanto, una nueva forma de entender la confrontación que busca sorprender al enemigo con dispositivos explosivos y que logra con efectividad mantener comunicaciones básicas en territorio hostil. Lo materializan con telefonía vía satélite, pero también con el empleo de Internet. Observaremos que la Web no es sólo una plataforma en la que se promuevan los ejercicios de Propaganda, sino que también clarifica determinados procesos de captación y reclutamiento de efectivos para el apoyo no solamente logístico (financiación), sino también operativo.

TECNOLOGÍAS DE AMPLIA DIFUSIÓN: UNA FÓRMULA "ASEQUIBLE".

I. IED`s (12): artefactos explosivos de fabricación barata

Los autores Fernando Mañas y Javier Jordán han logrado plasmar con precisión en su extraordinario paper sobre IED`s (13) la dureza de estos dispositivos en Irak y Afganistán. El objetivo de causar bajas en el enemigo sin mostrar visibilidad asegura un elemento más de disuasión como procedimiento de guerra asimétrica. España ha dado un paso adelante fundamental, con la creación de un centro especializado en desactivación de IED´s, en concreto el Primer Centro Internacional de referencia de la OTAN (14), todo un desafío, que se suma a la reciente renovación de blindados con los nuevos RG-31.

Los IED`s son dispositivos explosivos construidos manualmente que bien se camuflan en una carretera, como en el cuerpo de un terrorista suicida contra un blanco inmóvil. Es por tanto una definición generosa que agrupa un sinfín de usos y también cómo no una amplia

variedad de formas de activación a distancia. Desde teléfonos móviles a sencillos mandos remotos. Su sencillez la resume el Think Thank "*Global Security*" en la palabra "*home-made*" (15), es decir, hecho en casa. Según GS, los IED`s prácticamente pueden ser cualquier tipo de dispositivo con material explosivo y un iniciador. En este caso los autores Mañas y Jordán añaden un tercer elemento como es el revestimiento o contenedor (16). En cualquier caso, son muy difíciles de detectar, dado que por lo general se emplean en terrenos rocosos o arcillosos donde es posible ocultarlos con facilidad. Pueden emplearse para su fabricación explosivos militares o industriales, pero en el caso de la Insurgencia en el Cáucaso ruso, en el Valle del SWAT en Pakistán, o en el propio Afganistán, disponen de materia prima suficiente con las municiones de artillería de calibre medio o de minas anticarro (17).

En el caso de los ataques suicidas con dispositivos explosivos, se ha observado un significativo repunte desde el año 2002, multiplicándose de forma exponencial el número de víctimas mortales e incrementándose también la eficacia de los IED`s usados por los Talibanes. En esta línea se mueve Javier Jordán al considerar que el uso de estos dispositivos es una más de las iniciativas talibán (junto a la Propaganda y los ataques suicidas), que buscan igualar el escenario bélico de Irak y Afganistán, a fin de que las opiniones públicas de los países que participan en la Alianza encuentren similitudes, y por consiguiente exijan los mismos costes políticos . Es por tanto un impacto estratégico el que consiguen los IED, ya que además de los costes en vidas, también lleva asociado un remanente de negatividad en el seno de las opiniones públicas.

II. Uso de Internet, cámaras de vídeo y propaganda

La Red Global mantiene conectados a millones de internautas a lo largo de todo el mundo. Es quizás la representación más palpable de un mundo globalizado en el que las distancias se acortan, y donde cualquier cosa es posible. Las redes delincuenciales y los grupos insurgentes y terroristas no son ajenos a estas facilidades y buena muestra de ello lo encontramos en la constante y frenética búsqueda de iniciativas de recaudación y reclutamiento de combatientes.

Los periodistas del Washington Post Susan B. Glasser y Steve Coll publicaron una serie de artículos allá por el año 2005 en los que dieron buena cuenta de la transformación vivida por parte de los Grupos Terroristas e Insurgentes, sobre todo en los últimos años, en aras de la búsqueda de nuevas formas de comunicación que facilitaran ventajas en cuanto a la gestión de sus recursos y a la planificación de una estrategia operacional. Según estos autores, nunca antes en la historia una organización con estructura de guerrilla había logrado de manera tan efectiva aplicar de manera dual una Yihad electrónica adaptada al campo de batalla (19). Se trata en definitiva de la Insurgencia del futuro, que funciona con medios tecnológicamente básicos pero muy efectivos. La ventaja de Internet radica en la facilidad de distribuir un discurso asociado a los objetivos de la Yihad y de sostener con eficacia una comunicación permanente con Grupos Asociados que pueden mantener cierto apoyo logístico, económico o de reclutamiento de *mujahidines* en cualquier parte del mundo. Glasser y Coll sostienen que la grabación y distribución de imágenes cruentas de la actividad yihadista forma parte indisoluble de las nuevas estrategias de los insurgentes (20). Como veremos posteriormente, el empleo de la Propaganda logra infundir temor en las Opiniones Públicas occidentales y ayuda a avivar los objetivos insurgentes/yihadistas por medio mundo. Las Agencias de Seguridad occidentales han logrado identificar multitud de grupos terroristas que hacen uso de foros en web yihadistas en los que reciben un apoyo eminentemente logístico y operativo. Son iniciativas que parece que empezaron a cobrar una fuerza inusitada con el despegue del terrorista Abu Musab Al-Zarqawi, (eminente líder de Al-Qaeda hasta su muerte). La difusión de duros vídeos de degollamientos o ataques a convoyes de la ISAF logró aglutinar en torno a determinadas páginas a seguidores de medio mundo, pero también a combatientes que sobre el terreno hacían uso de escasos medios para distribuir sus hazañas. Algunas fuentes no contrastadas han considerado la posibilidad de que en

determinados emplazamientos pudiera hacerse uso de antenas parabólicas artesanales para así disponer de un acceso directo a la difusión vía satélite. Pero debemos considerar como válida la tesis de que el acceso a Internet se ha democratizado, incluso en las poblaciones más remotas.

En Internet es posible obtener información básica para la fabricación de un cinturón de explosivos artesanal y facilitar intercambios de información entre combatientes y aspirantes a serlo. En este sentido, resulta interesante la aportación realizada al estudio de los Foros yihadistas en Internet del especialista Evan Kohlmann, autor que identifica como un espaldarazo definitivo para la causa el apoyo recibido por los Administradores del Foro ***Ansar al-Muyahidin*** del Emirato Islámico de Afganistán (talibanes afganos). Estos últimos reivindicaron la importancia de las acciones de la Red en un comunicado distribuido en Octubre de 2009 (21) y reconocían la labor de ***Ansar*** como una de las más efectivas a la hora de distribuir los vídeos más recientes de las actividades operativas de los talibanes.

Otro de los foreros manifestaba su creciente aburrimiento con el "trabajo" en Internet y su deseo de unirse al campo de batalla "...*para luchar con mi arma, mi cámara y ordenador, así que le pido a Dios que nos conceda la gracia*..." (sic) (22). Observamos por tanto una clara conciencia pro-tecnológica, apoyada en parte en lo que Alfonso Merlos considera un "…marco de operaciones ideal para las organizaciones terroristas…" (sic). Su visión pasa por considerar a la Red como un compendio de ventajas en torno a la facilidad de acceso, escasa regulación y control gubernamental, anonimato, y sobre todo rapidez de intercambio de información . Una de las actividades que a juicio de Merlos más rentabilidad han proporcionado a las campañas yihadistas, se halla en la promoción de operaciones de guerra psicológica. En este caso se trata de una campaña sistemática de desinformación que incide tanto o más que un proyectil de mortero, esto es, afectando a la moral del enemigo, y facilitando una imagen "…*de vigor, fortaleza y pujanza*…" (24) (sic). Llegados a este punto, resulta interesante abordar la relevancia de las Nuevas Tecnologías en lo que Alfonso Merlos define como la planificación y coordinación táctica y estratégica de operaciones de destrucción en masa. O lo que es lo mismo, la gestión de una actividad terrorista. Es el caso del palestino Abu Zubayda, responsable de reclutamiento y logística de Al Qaida, el cual según las investigaciones en torno al 11 de Septiembre, utilizó la red para comunicarse con las células dirigidas por el suicida egipcio Mohamed Atta. Observamos por tanto cómo el mayor atentado de la historia podría no haberse gestado de igual manera sin la existencia de las Tecnologías de la Información. Y lo cierto es que Abu Zubayda no necesitó un Centro de Comunicaciones de última generación. Tan sólo un ordenador en un cibercafé de Pakistán con acceso a internet. Por otra parte, se ha demostrado que los coordinadores de la gestión de reclutamiento de mujahidines utilizan cuentas de correo electrónico, dado que perfectamente pueden combinar la inmediatez con la seguridad. Aprovechan la infinidad de programas de encriptación gratuitos disponibles en la Red para ocultar sus mensajes. Técnicas como la esteganografía (25) están al alcance de cualquiera.

CÁMARAS DE VÍDEO Y PROPAGANDA A TRAVÉS DE LA RED

El Profesor Dr. Torres Soriano en su Tesis Doctoral sobre Propaganda Yihadista (26), considera que el Movimiento Yihadista Global ha sabido agrupar los sabotajes de grupúsculos dispersos haciéndolos suyos mediante un mismo paraguas. Torres Soriano nos describe a la perfección la estructura básica de un elemento asimétrico fundamental; a saber, el abandono de un enfrentamiento abierto entre ejércitos y el desconcierto del "ejército ocupante".

Lo cierto es que en los últimos años, el empleo de la Propaganda por parte del aparato mediático de Al-Qaeda (27) ha obtenido importantes enteros en lo que respecta a la difusión de un terror global. Las siempre duras imágenes de degollamientos, los ataúdes envueltos en banderas y la promoción permanente de los logros de los insurgentes en el teatro de operaciones, enarbola una estrategia bien meditada, que hace uso de plataformas virtuales originadas ad hoc como ***Al Fajr***

Media Center y la ***Global Islamic Media Front*** (28), herramientas para verter toda una campaña de propaganda que tiene como objeto generar opiniones públicas enfrentadas y asociar los conceptos de injusticia social y opresión con la persistencia del enemigo. Encontramos asimismo como elemento accesorio, el enarbolamiento de una causa que en el fondo no es más que sectaria e intransigente.

Como ya se demostró en la Segunda Guerra Mundial, la Propaganda resulta esencial para el devenir de los conflictos. Afecta no sólo a la moral de los soldados, sino también a la motivación de toda una nación. Con estas herramientas, la Insurgencia yihadista en Irak y Afganistán ha logrado -probablemente sin pretenderlo de manera directa- un apoyo mediático sin precedentes, que aglutina la labor anónima e incansable de multitud de Administradores de foros yihadistas, verdaderos lobos solitarios cuya máxima premisa es la difusión global de elementos audiovisuales que ensalcen la labor insurgente. Se trata en suma, y siguiendo las tesis de Luis de la Corte y Javier Jordán, de uno de los "*..instrumentos esenciales y críticos del movimiento yihadista global*…" (29) (sic).

III. Telefonía móvil y teléfonos vía satélite

Uno de los elementos tecnológicos de amplia difusión que más popularidad y extensión han adquirido en los últimos años, es también el verdadero ejemplo de la democratización en el seno de una sociedad globalizada. Los teléfonos se caracterizan por ser un sistema de comunicación que aporta mayor inmediatez a la comunicación, y que como se ha puesto de manifiesto en el estudio de algunas redes de reclutamiento de *mujahidines*, una persona A entrega a una persona B un teléfono y una tarjeta de prepago, a fin de que en dicho terminal y con la tarjeta SIM recibida pueda coordinarse con el responsable logístico. Javier Jordán lo define muy bien al considerar que con este sistema de entrega de tarjetas SIM se minimiza la probabilidad de una infiltración de algún Servicio Occidental, y se reduce al máximo el círculo de personas que conocen dichos números (30). En esta misma línea el Evening Estándar informaba de la reciente preocupación del MI6 británico por el uso *in crescendo* de la versión móvil de Skype por parte de algunos insurgentes. El software en cuestión dispone de un sistema de cifrado tan potente que resulta verdaderamente complicada su interceptación por parte de sus aviones espía, los Nimrod (31). Es un ejemplo quizás sensacionalista, pero que evidencia la facilidad de acceso a entornos tecnológicos de amplia difusión por parte de la Insurgencia.

LOS TELÉFONOS POR SATÉLITE THURAYA, CADA VEZ MÁS POPULARES.

Otro de los dispositivos de comunicación más efectivos lo encontramos en la telefonía vía satélite. En los últimos años, la Compañía ***Thuraya*** ha adquirido en la región de Oriente Próximo y sur de Asia una fuerza inusitada. Thuraya es una empresa regional dedicada al suministro de comunicaciones telefónicas por satélite cuya área de influencia abarca Afganistán, la mayor parte de Europa, África Central, África del Este y Australia. La compañía Thuraya, con sede en Emiratos Árabes, y cuyo servicio comercial se inició en el año 2001(32), opera con un satélite en órbita geoestacionaria que brinda cobertura a una tercera parte del mundo. Agencias de Comunicación, Contratistas y también elementos insurgentes en Irak y Afganistán hacen uso de sus servicios. Los teléfonos de mano de Thuraya combinan tres poderosas tecnologías: satélite, GSM y sistema GPS, con lo cual se aporta a los usuarios una gran flexibilidad de acuerdo con las coberturas de que puedan disponer (33).

Según algunas fuentes consultadas, aproximadamente un 40% de los afganos disponen o tienen acceso a la telefonía móvil, lo que supone una cifra verdaderamente significativa para uno de los países más pobres del mundo (34). Estas mismas fuentes afirman que los Talibanes consideran el uso y control de las comunicaciones uno de los vectores básicos de su estrategia. Si bien, las Fuerzas de la Coalición en ocasiones han sufrido en sus propias carnes el poderoso uso que una tecnología de amplia difusión puede generar en el campo de batalla. De hecho, recientemente,

fuerzas de Estados Unidos confiscaban a miembros del Nuevo Ejército Afgano varios teléfonos móviles y un teléfono por satélite de Thuraya, al sospechar que a través de estos medios algún infiltrado de la Insurgencia pudo haber informado de los puntos de paso de Fuerzas Especiales de los EE.UU (35). Se genera por tanto un temor a que en las propias filas amigas se haga uso de la tecnología de amplia difusión, pero en este caso para contactar con grupos de insurgentes que también disponen de teléfonos móviles, y que como ya hemos visto con anterioridad, muestran una voluntad inequívoca a favor de las Nuevas Tecnologías, curiosamente una perspectiva nunca vista antes de la Guerra iniciada allá por el año 2001.

Efectivamente, la corriente sunní *deobandí* de los talibanes, quizás una de las escuelas más extremas en la interpretación del Corán y la Sharia (36), parecía abandonar las tesis primigenias que giraban en torno al rechazo a todo aquello que pudiera estar asociado intrínsecamente a lo occidental. De alguna manera esto tenía que ver con sus propias creencias, vinculadas a una visión *salafista* del mundo, eminentemente maniqueista, que apuesta por una vuelta a la tradición y a la forma de vivir de los primeros compañeros del profeta. El cambio de visión venía asociado a las inmensas posibilidades que ofrecían las tecnologías occidentales en el desarrollo de las actividades de guerra de guerrillas. Pero los ataques a las redes de comunicación también han estado en la mente de los insurgentes durante cierto tiempo. Así, como comentan en medios especializados, en el pasado insurgentes afganos se marcaban como objetivo la destrucción de las torres de comunicación, incluso aunque para planificar sus ataques ellos mismos hicieran uso de los teléfonos móviles (37).

Los talibanes son conscientes de la importancia de neutralizar las redes de comunicación, pero también de controlarlas; en el año 2007 las Fuerzas de la Coalición ya advertían en informes de inteligencia de la vulnerabilidad asociada al empleo de teléfonos móviles civiles, tanto para los soldados que desde el frente realizaban llamadas telefónicas a las familias, como a personal diplomático o a miembros de los Cuarteles General. Según manifestaba el Diario británico *The Guardian*, los insurgentes habrían podido hacer uso de los datos facilitados por ***Roshan Network***, un suministrador de servicios telefónicos GSM, cuya infraestructura permite las comunicaciones entre las zonas fronterizas de Irán y Pakistán con el territorio afgano. A través de la tecnología GSM es posible establecer el track y la ruta telefónica seguida por las llamadas, y al parecer la insurgencia dispondría de HUMINT (38) en el seno de ***Roshan*** (39).

LIMITACIONES DE LAS TECNOLOGÍAS DE AMPLIA DIFUSIÓN

En el Islam el concepto de tiempo se encuentra a miles de años de distancia del que disponemos en Occidente. El paso del tiempo se antoja en ocasiones lento pero en un continuo discurrir, y puede quizás para algunos que ése sea el motivo por el que la Insurgencia Islamista en las zonas de Yihad no tiene prisa en hacer las cosas. En ocasiones el objetivo final no se encuentra en la victoria, sino más bien en el mantenimiento de una situación desesperada para las tropas de la coalición. Efectivamente, las tecnologías de amplia difusión, no son determinantes para ganar una guerra, pero sí que favorecen una situación de continua desafección a la inestabilidad por parte de los *infieles cruzados*. En este sentido, el concepto de Contrainsurgencia aplicada sobre el campo de batalla parece haber tenido efectos positivos en el Teatro de Operaciones iraquí -recordemos la Estrategia The Surge, que permitió reducir el número de bajas de la Coalición en Irak-, y precisamente, el análisis exhaustivo de las a veces precarias técnicas operativas de los Grupos Talibanes, ha permitido conocer que efectivamente la Insurgencia utiliza Internet, se comunica por teléfonos móviles y al fin, dispone de ciertos puntos débiles.

En primer lugar, se puede decir que las Tropas de la Coalición han hecho los deberes, al menos en lo que respecta a la estricta observación de las medidas de seguridad en los desplazamientos de sus convoyes (40). Unidades específicamente dedicadas a la desactivación de IED`s barren día tras día con vehículos especiales las vías principales de comunicación, a lo que se suma la constante

inversión en I+D, que ha permitido reducir de manera significativa el número de bajas. El reforzamiento de los vehículos blindados procura proteger a los soldados de los efectos de los Dispositivos Improvisados (41), y sin duda, como ya comentamos en páginas anteriores, la presión de la opinión pública ha condicionado un aceleramiento de las inversiones en seguridad.

Los IED`s disponen de limitaciones dependiendo de sus modalidades. Así los dispositivos activados a distancia -según la OTAN, los más utilizados en la zona de operaciones (42) - podrían verse afectados por elementos como la climatología, la dificultad técnica en su construcción, las contramedidas electrónicas o incluso las interferencias producidas por terceros (43). En ocasiones se necesitará una observación directa por parte del insurgente, con lo que ello tiene de riesgo para su propia seguridad, sobre todo en caso de que el dispositivo fallara. Por su parte, el uso de Internet efectivamente facilita las comunicaciones entre la Insurgencia y participa de alguna manera en ciertas labores logísticas, pero debemos recordar que EE.UU es líder en tecnologías de la información, y que por consiguiente, dispone de herramientas que permiten rastrear IP`s, localizar servidores, y a la postre rastrear los emplazamientos desde los que habitualmente chatean o navegan.

Las Fuerzas de Seguridad disponen de herramientas judiciales de intervención de las comunicaciones que facilitan la detección de células logísticas de reclutamiento y captación de combatientes, tal y como se puso de manifiesto a finales del pasado mes de Agosto en Alicante. Allí fue detenido el súbdito marroquí Faical Errai, en la actualidad en prisión provisional, acusado de ser según el Auto de la Audiencia Nacional "…*Administrador general del aparato mediático, coordinador de envío de voluntarios a zonas de conflicto, facilitador de rutas para el tránsito de voluntarios, dinamizador en funciones de recaudación de dinero para el envío de voluntarios y para la propia autofinanciación de la actividad propagandística del grupo*…" (44) (sic).

Otra de las herramientas de amplia difusión más extendidas son los teléfonos móviles, sobre todo por vía satélite, y nuevamente, disponen de grandes limitaciones. En primer lugar en cuanto a la cobertura. En el caso de Afganistán la montañosa orografía dificulta enormemente la obtención de señal, a lo que se le suman los obstáculos a una comunicación directa con el satélite como las edificaciones o las interferencias eléctricas. La disponibilidad de recursos de la Inteligencia estadounidense permite intervenir las comunicaciones móviles y vía satélite con enorme facilidad, lo cual hace enormemente difícil evitar filtraciones de información a la Coalición. De alguna manera, el espacio radioeléctrico está intervenido, y a la postre esta intervención ha permitido a las fuerzas de la Coalición anticiparse a la jugada en actividades ofensivas. El rastreo de la señal tanto vía satélite como a través de GSM es posible técnicamente y de hecho se materializa para la detección de la Insurgencia. La inteligencia de señales o SIGINT es una más de las herramientas utilizadas por la ISAF que incluso puede acoplarse a los *Predator*, últimamente muy utilizados en Pakistán y Afganistán.

CONCLUSIONES

En estos momentos es esencial comprender que nos abocamos a nuevos desafíos que no se circunscriben de manera exclusiva al propio desarrollo tecnológico, sino más bien a la eficacia de ese empleo. El siglo XXI ha acabado por comprender que no siempre el ejército más poderoso es el que obtiene las mayores victorias; por el contrario, se ha demostrado que una inteligente estrategia asociada al Arte militar puede resultar mucho más contraproducente para los planteamientos exclusivamente científicos, al menos en lo que respecta a la implementación de una tecnología de última generación aplicada al campo de batalla. Los talibanes, y en definitiva todo el elenco de grupos insurgentes –asociados a grupos yihadistas con proyección exterior- han actuado de manera resolutiva en los últimos cinco años, fundamentalmente en lo que respecta al empleo de tecnologías de amplia difusión, que no de última generación.

En buena medida, podríamos apreciar un elemento cultural como intrínsecamente asociado al despliegue talibán en entornos diametralmente opuestos a los elementos tecnológi-

cos occidentales como Internet. Ese elemento cultural estaría asociado a la llegada a zonas de conflicto de jóvenes occidentales, reclutados por redes de captación vinculadas a grupos como Al Qaeda que han nacido y crecido en sus suburbios de origen (Londres, Madrid, París…) con elementos tecnológicos económicamente asequibles que brindan sus propias sociedades de acogida. Hablamos de Internet, pero también del uso de teléfonos móviles y de tecnologías como el VoIP. Así, la complementación entre esos usos y las técnicas de guerrilla ha promovido un cóctel explosivo desde el punto de vista del enfrentamiento, aunque sobre todo en cuanto a la logística. Las comunicaciones por GSM y por satélite, más accesibles recientemente gracias a la creación de grandes consorcios de telecomunicaciones en la zona, permiten sin duda la generación de nuevas sinergias de creación de células o comandos. Los talibanes lo saben, y por ello han acabado por ceder ante la facilidad de uso de la tecnología de amplia difusión. No debemos hacer caso de titulares sensacionalistas, dado que al final se demuestra que el acceso a la alta tecnología no es tan sencillo. Se ha demostrado que a través de Internet, los grupos insurgentes no sólo establecen comunicaciones básicas vinculadas al teatro de operaciones, sino que también obtienen financiación y conocimientos para la implementación de IED`s u otros métodos de emboscada. Los foros yihadistas han empezado a adquirir dimensiones preocupantes, por cuanto que sus Administradores, en la mayoría de los casos ***"Lone wolves"*** o lobos solitarios, han entendido que sus objetivos en la vida pasan por la defensa de los territorios de yihad, lo cual se hace extensible al actual conflicto bélico que ocupa a las tropas de la ISAF. A ello se le ha unido una estructurada estrategia propagandística que ha hecho uso de software tipo ***streaming*** para publicitar sus hazañas bélicas". La democratización de programas como ***Youtube*** ha brindado la posibilidad de difundir prácticamente en tiempo real vídeos caseros realizados por los propios insurgentes, o incluso por foreros con ansias de protagonismo, muchas veces incitados por los propios aparatos mediáticos de Al Qaeda. Así las cosas, el miedo es sin duda uno de los elementos que más valor añadido aporta a la estrategia de cuarta generación que promueven los insurgentes. Frente a estos posicionamientos, las tropas de la ISAF han demostrado fuerte vulnerabilidad, fundamentalmente en lo que atañe a la rigurosidad con que sus opiniones públicas valoran la temperatura del conflicto. Y ello es sin duda de gran ayuda para el enemigo.

Otro de los elementos más interesantes abordados en el presente trabajo lo hemos identificado como IED o dispositivo explosivo improvisado. Su crudeza en el campo de batalla, y sobre todo la facilidad con que la Insurgencia lo ha promovido en los últimos nueve años, ofrece buena cuenta de los cambios habidos en los últimos años en las fuerzas de la coalición. Tecnologías de fácil desarrollo que han tenido una respuesta en el fortalecimiento de los blindajes de los vehículos y en la creación de unidades especializadas en detección y desactivación de explosivos. La Insurgencia actual ha adoptado un rol que se asocia más a una perspectiva ***"open-mind"*** o apertura de miras que procura luchar contra Occidente empleando sus propias armas. Es aquí donde radica el verdadero desafío: cómo evitar que las herramientas que utilizamos en nuestra vida diaria puedan ser empleadas para fines terroristas.

NOTAS

(1) [http://www.elmundo.es/elmundo/2009/12/18/navegante/12611298-70.html]

(2) Las víctimas producidas en las filas españolas en Afganistán por el uso de minas terrestres planteó la necesidad de incrementar los blindajes de los vehículos de los soldados. Así, los blindados RG-31 han hecho acto de presencia en sustitución de los obsoletos BMR. Más información en el siguiente enlace: [http://www.abc.es/20100327/nacional-nacional/chacon-supervisa-torrejon-envio-201003271502.html].

(3) JACKSON, Brian. *"Technology Acquisition by Terrorist Groups*: *Threat Assessment Informed by Lessons from Private Sector Technology Adoption"*. RAND CORPORATION. Paper disponible en el siguiente enlace: [http://www.rand.org/pubs/reprints/2007/RAND_RP1248.pdf]

(4) Ibid. Pag. 5

(5) HAIN, F. Raymond. "*The Use and Abuse of Technology In Insurgent Warfare"*. Artículo disponible en el siguiente enlace: [http://www.airpower.maxwell.af.mil/airchronicles/cc/Hain.html]

(6) JACKSON, Brian. Op Cit. Pag. 5.

(7) JACKSON, Brian, CHALK, Peter, *et al*. "*Breaching the Fortress Wall: Understanding terrorist efforts to overcome defensive technologies"*. RAND CORPORATION. Paper disponible en el siguiente enlace: [http://www.rand.org/pubs/monographs/2007/RAND_MG481.pdf]

(8) Ibid. Pag. 121.

(9) GARCÍA CANTALAPIEDRA, David y DÍAZ MATEY, Gustavo. *"EE.UU, el uso de la inteligencia y la doctrina de contrainsurgencia norteamericana: lecciones para Afganistán"*. Real Instituto Elcano. Documento de Trabajo Nº54/2008, 22 Diciembre 2008. Working Paper disponible en: [www.realinstitutoelcano.org].

(10) KILCULLEN, David J. *"Paradigmas nuevos en los conflictos del siglo XXI"*. Web del Departamento de Estado de los EE.UU. - en español-. 15 Septiembre 2008. Artículo disponible en: [http://www.america.gov/st/peacesecspanish/2008/September/20080915151816pii0.0073511.html]

(11) Podemos acceder a una interesante reseña de esta obra en la Revista de la OTAN:[http://www.nato.int/docu/review/2008/04/AP_BOOK/ES/index.htm]

(12) Acrónimo de "Improvised Explosive Devices"

(13) MAÑAS, Fernando M. y JORDÁN J. "*Los artefactos explosivos improvisados (IED`s)*". Athena Assessment. No 6/07. 17 Octubre 2007. Paper disponible en el siguiente enlace: [http://policialocal.tv/files/ieds.pdf] P. 12.

(14) NIEVES, Gema. *"España, en la lucha contra los artefactos explosivos improvisados"*, en Revista Atenea. 02/07/10. Artículo disponible en el siguiente enlace: [http://www.revistatenea.es/RevistaAtenea/REVISTA/articulos/GestionNoticias_2429_ESP.asp]

(15) Información accesible en el siguiente enlace web perteneciente a Global Security: [http://www.globalsecurity.org/military/intro/ied.htm]

(16) MAÑAS, Fernando M. y JORDÁN J. *Op Cit*. Pag. 110

(17) Ibid. Pag. 110.

(18) JORDÁN, Javier. *"La Insurgencia Yihadista en Afganistán y Pakistán: implicaciones para la seguridad española"*. Athena Assessment. No. 3/08. 21/04/08. Paper disponible en el siguiente enlace web: [http://infodefensa.com/documentos/docs/insurgenciapakistan[1].pdf]

(19) GLASSER, B. Susan y COLL, Steve. *"The Web as Weapon"*. The Washington Post. 09/08/05. Artículo en tres partes disponible en el siguiente enlace web: [http://www.washingtonpost.com/wp-dyn/content/article/2005/08/08/AR2005080801018.html]

(20) Ibid.

(21) KOHLMANN, Evan. "A Beacon for Extremists: The Ansar al-Mujahideen Web Forum". Combating Terrorism Center At West Point (CTC). February 2010. Vol. 3. Issue 2. Paper disponible en el siguiente enlace: [http://www.ctc.usma.edu/sentinel/CTCSentinel-Vol3Iss2.pdf]

(22) Ibid. Pag. 3.

(23) MERLOS GARCÍA, Alfonso. *"Internet como instrumento para la Yihad"*. Araucaria. Revista Iberoamericana de Filosofía, Política y Humanidades. Año 8, Nº16. Segundo Semestre de 2006. Documento accesible en el siguiente enlace:

[http://www-en.us.es/araucaria/nro16/ideas16_5.htm]

(24) Ibid.

(25) Ocultamiento de mensajes en objetos portadores, como pudiera ser el caso de fotografías.

(26) TORRES SORIANO, Manuel R. *"La dimensión propagandística del Terrorismo Yihadista Global"*. Tesis Doctoral. Departamento de Ciencia Política y de la Administración. Universidad de Granada. 2007, p. 121.

(27) As-Sahab

(28) TORRES SORIANO, Manuel R. *"Terrorismo yihadista y nuevos usos de Internet: la distribución de propaganda"*. ARI Nº110/2009 de fecha 09/07/09 Real Instituto Elcano. Documento disponible en el siguiente enlace:

[http://www.realinstitutoel-cano.org/wps/wcm/connect/a4f7d300-4f0199b4a174e53170baead1/ARI110-2009_Torres_terrorismo_yihadista_internet.pdf?MOD=AJPERES&CACHEID=a4f7d3004f0199b4a174e53170baead1]

(29) DE LA CORTE, Luis y JORDÁN, Javier. "*La Yihad Terrorista*". Madrid. Edit. Síntesis, 2007. Pag. 218.

(30) JORDÁN, Javier. "*Estructura organizativa del terrorismo de inspiración yihadista en Europa: retos para los Servicios de Inteligencia"*, en Instituto Español de Estudios Estratégicos y Centro Nacional de Inteligencia: La inteligencia, factor clave frente al terrorismo internacional. (Madrid: Ministerio de Defensa, 2009. Pag. 71-108. Artículo disponible en el siguiente enlace web: [http://www.ugr.es/~jjordan/publicaciones/organizacionyihadista.pdf]

(31)[http://www.thisislondon.co.uk/news/article-23555425-taliban-using-skype-phones-to-dodge-mi6.do]

(32) [www.space.com/news/satellite_phones_011113.html]

(33) [www.ts2.pl/en/Thuraya/Afghanistan]

(34)[http://www1.voanews.com/english/news/science-technology/Mobile-Phones-and-Modern-War-92963214.html]

(35) BROWN, Drew. *"Insurgents knew of Kunar Operation"*. Artículo publicado en "Stars and Stripes" y disponible en el siguiente enlace web: [http://www.stripes.com/news/u-s-insurgents-knew-of-kunar-operation-1.79181]

(36) Ley Islámica.

(37) MADDUX, Catherine. "*Mobile Phones and Modern War*". Mayo 2010. Artículo disponible en el siguiente enlace web: [http://www1.voanews.com/english/news/science-tehnology/Mobile-Phones-and-Modern-War-92963214.html]

(38)Fuentes de inteligencia humanas.

(39)TISDALL, Simon. "*Afghanistan war logs: Nato feared Taliban could tap its mobile phones"*. Diario The Guardian. 25/07/2010. Artículo disponible en el siguiente enlace web: [http://www.guar-dian.co.uk/world/2010/jul/25taliban-tapped-mobile-phones-afghanistan]

(40)Las Fuerzas Armadas españolas desplegadas en Afganistán han empezado a utilizar un rodillo antiminas instalado en los RG-31. Más información en el siguiente enlace web: [http://www.revistatenea.es/Revista-Atenea/REVISTA/articulos/GestionNoticias_2724_ESP.asp]

(41)Ya comentamos en páginas anteriores cómo el Ministerio de Defensa español optó por blindados más robustos y protegidos como los RG-31, en sustitución de los anticuados BMR.

(42)Un 38% de incidencia según datos de 2009.

(43) VV.AA. *"La seguridad frente a artefactos explosivos"*. Documentos de Seguridad y Defensa. N.28. (CESEDEN). Septiembre 2009. Documento disponible en el siguiente enlace web: [http://www.ceseden.es/centro_documentacion/documentos/28.pdf]

(44) Información de prensa accesible en el siguiente enlace web: [http://www.europapress.es/nacional/noticia-prision-presunto-islamista-detenido-alicante-20100831181816.html]

BIBLIOGRAFÍA

-BROWN, Drew. *"Insurgents knew of Kunar Operation"*. Artículo publicado en "Stars and Stripes" y disponible en el siguiente enlace web: [http://www.stripes.com/news/u-s-insurgents-knew-of-kunar-operation-1.79181]

-DE LA CORTE, Luis y JORDÁN, Javier. *"La Yihad Terrorista"*. Madrid. Edit. Síntesis, 2007. Pag. 218.

-GARCÍA CANTALAPIEDRA, David y DÍAZ MATEY, Gustavo. "*EE.UU, el uso de la inteligencia y la doctrina de contrainsurgencia norteamericana: lecciones para Afganistán"*. Real Instituto Elcano. Documento de Trabajo Nº54/2008, 22 Diciembre 2008. Working Paper disponible en: [www.realinstitutoelcano.org].

-GLASSER, B. Susan y COLL, Steve. "*The Web as Weapon"*. The Washington Post. 09/08/05. Artículo en tres partes disponible en el siguiente enlace web:

[http://www.washingtonpost.com/wp-dyn/content/article/2005/08/08/AR2005080801018.html]

-HAIN, F. Raymond. *"The Use and Abuse of Technology In Insurgent Warfare"*. Artículo disponible en el siguiente enlace: [http://www.airpower.maxwell.af.mil/airchronicles/cc/Hain.html]

-JACKSON, Brian. *"Technology Acquisition by Terrorist Groups*: *Threat Assessment Informed by Lessons from Private Sector Technology Adoption"*. RAND CORPORATION. Paper disponible en el siguiente enlace: [http://www.rand.org/pubs/reprints/2007/RAND_RP1248.pdf]

-JACKSON, Brian, CHALK, Peter, *et al*. *"Breaching the Fortress Wall: Understanding terrorist efforts to overcome defensive technologies"*. RAND CORPORATION. Paper disponible en el siguiente enlace: [http://www.rand.org/pubs/monographs/2007/RAND_MG481.pdf]

-JORDÁN, Javier. *"La Insurgencia Yihadista en Afganistán y Pakistán: implicaciones para la seguridad española"*. Athena Assessment. No. 3/08. 21/04/08. Paper disponible en el siguiente enlace web: [http://infodefensa.com/documentos/docs/insurgenciapakistan[1].pdf]

-JORDÁN, Javier. "*Estructura organizativa del terrorismo de inspiración yihadista en Europa: retos para los Servicios de Inteligencia"*, en Instituto Español de Estudios Estratégicos y Centro Nacional de Inteligencia: La inteligencia, factor clave frente al terrorismo internacional. (Madrid: Ministerio de Defensa, 2009. Pag. 71-108. Artículo disponible en el siguiente enlace web: [http://www.ugr.es/~jjordan/publicaciones/organizacionyihadista.pdf]

-KILCULLEN, David J. "*Paradigmas nuevos en los conflictos del siglo XXI"*. Web del Departamento de Estado de los EE.UU. - en español-. 15 Septiembre 2008. Artículo disponible en: [http://www.ame-rica.gov/st/peacesecspanish/2008/September/20080915151816pii0.0073511.html]

-KOHLMANN, Evan. "*A Beacon for Extremists: The Ansar al-Mujahideen Web Forum"*. Combating Terrorism Center At West Point (CTC). February 2010. Vol. 3. Issue 2. Paper disponible en el siguiente enlace: [http://www.ctc.usma.edu/sentinel/CTCSentinel-Vol3Iss2.pdf]

-MADDUX, Catherine. *"Mobile Phones and Modern War"*. Mayo 2010. Artículo disponible en el siguiente enlace web: [http://www1.voanews.com/english/news/science-tehnology/Mobile-Phones-and-Modern-War-92963214.html]

-MAÑAS, Fernando M. y JORDÁN J. *"Los artefactos explosivos improvisados (IED`s)"*. Athena Assessment. No 6/07. 17 Octubre 2007. Paper disponible en el siguiente enlace: [http://policialocal.tv/files/ieds.pdf]

-MERLOS GARCÍA, Alfonso. *"Internet como instrumento para la Yihad"*. Araucaria. Revista Iberoamericana de Filosofía, Política y Humanidades. Año 8, Nº16. Segundo Semestre de 2006. Documento accesible en el siguiente enlace:

[http://www-en.us.es/araucaria/nro16/ideas16_5.htm]

-NIEVES, Gema. *"España, en la lucha contra los artefactos explosivos improvisados"*, en Revista Atenea. 02/07/10. Artículo disponible en el siguiente enlace: [http://www.revistatenea.es/RevistaAtenea/REVISTA/articulos/Ges-tionNoticias_2429_ESP.asp]

-TISDALL, Simon. *"Afghanistan war logs: Nato feared Taliban could tap its mobile phones"*. Diario The Guardian. 25/07/2010. Artículo disponible en el siguiente enlace web: [http://www.guardian.co.uk/world/20-10/jul/25ta-liban-tapped-mobile-phones-afghanistan]

-TORRES SORIANO, Manuel R. *"La dimensión propagandística del Terrorismo Yihadista Global"*. Tesis Doctoral. Departamento de Ciencia Política y de la Administración. Universidad de Granada. 2007, p. 121.

-TORRES SORIANO, Manuel R. *"Terrorismo yihadista y nuevos usos de Internet: la distribución de propaganda"*. ARI Nº110/2009 de fecha 09/07/09 Real Instituto Elcano. Documento disponible en el siguiente enlace: [http://www.realinstitutoelcano.org/wps/wcm/connect/a4f7d3004-f0199b4a174e53170baead1/ARI110-2009_Torres_terro-rismo_yihadista_internet.pdf?MOD=AJPERES&CACHEID=a4f7d3004f0199b4a174e53170baead1]

-VV.AA. *"La seguridad frente a artefactos explosivos"*. Documentos de Seguridad y Defensa. N.28. (CESEDEN). Septiembre 2009. Documento disponible en el siguiente enlace web: [http://www.ceseden.es/centro_documentacion/documentos/28.pdf]

OTRAS WEB´S CITADAS

-http://www.thisislondon.co.uk/news/article-23555425-taliban-using-skype-phones-to-dodge-mi6.do

-www.space.com/news/satellite_phones_011113.html

www.ts2.pl/en/Thuraya/Afghanistan

-http://www1.voanews.com/english/news/science-technology/Mobile-Phones-and-Modern-War-92963214.html

-http://www.globalsecurity.org/military/intro/ied.htm

-http://www.elmundo.es/elmundo/2009/12/18/navegante/1261-129870.html

-http://www.abc.es/20100327/nacional-nacional/chacon-supervisa-torre-jon-envio-201003271502.html

-http://www.nato.int/docu/review/2008/04/AP_BOOK/ES/index.htm

-http://www.revistatenea.es/ RevistaAtenea/REVISTA/articulos/Gestion-Noticias_2724_ESP.asp

-http://www.europapress.es/nacional/noticia-prision-presunto-islamista-detenido-alicante-20100831181816.html