La innovación yihadista: propaganda, ciberterrorismo, armas y tácticas

Carlos Echeverría Jesús

Análisis nº 7416 **23 de diciembre de 2009**

La red terrorista Al Qaida ha demostrado en su corta vida de dos décadas – fue fundada en agosto de 1988 – que ha sabido aprovecharse de las tecnologías de la información para expandir sus ambiciosos objetivos planetarios: a título de ejemplo, a fines de la década de los noventa sustituyó su periódico Nashrat Al Akhbar por su utilización de los medios audiovisuales con "La Voz del Califato", primero, y con la sofisticada agencia "As-Sahab" que hoy sirve para transmitir los vídeos propagandísticos después, y ello aparte de su página Web alneda.com que pasó a mejor vida tras el 11-S gracias a la labor de los servicios antiterroristas y de las agencias de inteligencia. Por otro lado, y en lo que al ciberterrorismo respecta, el ataque realizado en 1999 por 'hackers' contra los sistemas informáticos de la OTAN en protesta por el bombardeo de Kosovo es una buena referencia para terroristas cibernéticos de todo pelaje y no cayó en saco roto en lo que respecta a los terroristas yihadistas salafistas. En esa línea de referencias estudiadas, dos años después del ataque contra la Alianza Atlántica un experto en informática australiano indignado por no ser aceptada su solicitud de empleo por el empresa "Marrochy Shire" de Queensland provocó como venganza el caos en los servicios de aguas residuales de la ciudad. También en ese mismo año, en los EEUU, los macroatentados del 11 de septiembre llevaron a las autoridades a explorar fórmulas imaginativas de futuros ataques contra las sociedades abiertas y uno de los escenarios más inquietantes que identificaron fue precisamente el de los ataques cibernéticos.[1] Ya un año antes los terrores en torno a los posibles efec-

tos en las redes informáticas del cambio de siglo se habían centrado en el denominado "Efecto 2000" que finalmente fue resuelto sin problemas, pero ello daba acceso a una década que sí está marcada por temores emergentes a que terroristas u otro tipo de agresores dotados de conocimientos y con deseo de provocar daños puedan crear el caos en sociedades cada vez más dependientes de las nuevas tecnologías.

En los últimos años se ha detectado que la intrusiones o alteraciones cibernéticas en redes de ordenadores gubernamentales se han producido tanto de la mano de actores conocidos, en ocasiones, como de la de actores clandestinos, destacándose de forma creciente entre estos últimos terroristas de distintas extracciones.[2] Junto a estas vulnerabilidades tecnológicas están las ligadas a los nuevos métodos de ataque probados por los terroristas – el "Yihad urbano" ya ha sido analizado en estudios anteriores y no será por ello desarrollado aquí – así como al in-interrumpido interés por las armas de destrucción masiva.

El uso de las autopistas de la información por los terroristas yihadistas salafistas

Los canales de televisión por satélite, Internet y la sofisticada telefonía actual permiten a los terroristas globales por antonomasia que son los yihadistas salafistas hacer el mundo más pequeño y poder interactuar entre países y regiones muy lejanos entre sí. Si el terrorismo ha estado ligado históricamente a la publicidad, el actual en sus distintas latitudes vive en un auténtico paraíso operativo dado que sobran los medios y los instrumentos para hacer llegar hasta el más lejano rincón del mundo información, propaganda y/o instrucciones.

El terrorismo nacional de Hizbollah, el Partido de Dios libanés, cuenta con la cadena Al Manar para transmitir en Líbano pero también más allá de sus fronteras – se estima que esta cadena tiene unos 10 millones de televidentes diarios que siguen con afición sus contenidos profundamente antisemitas – tratando con ello de atraer partidarios para su causa por todo el mundo y no encontrando obstáculos salvo en algunos casos puntuales (Francia) dada la diversidad de opiniones existentes sobre el carácter de Hizbollah, grupo claramente terrorista para algunos pero partido político y socio de Gobierno en Beirut, tanto en el gabinete anterior como en el recientemente constituido.[3]

Por otro lado, y sin abandonar el extendidísimo y menos elitista mundo de la televisión si lo comparamos con el más sofisticado y por ello menos accesible de la informática y de Internet, una cadena no ligada como Al Manar a un grupo terrorista pero que ha sido y es aprovechada por los terroristas yihadistas salafistas para canalizar a través de ella su propaganda en la qatarí Al Jazira, fundada en Doha en 1996. Esta cadena de televisión por satélite ha venido siendo hasta la actualidad el soporte elegido por los terroristas yihadistas salafistas para

dar a conocer al mundo sus principales comunicados y vídeos propagandísticos incluyendo entre estos últimos las famosas arengas tanto de Osama Bin Laden como de Ayman Al Zawahiri. Surgida como decíamos anteriormente a mediados de los noventa ha sido capaz de romper con las tradicionales inercias anteriores que permitían el predominio de canales de noticias occidentales – piénsese en la BBC británica pero sobre todo en la CNN estadounidense – y ahora se presenta a sí misma no sólo como la voz de árabes y musulmanes sino, con frecuencia también, como la voz de marginados, de desposeídos, etc. Una buena comparación entre dos momentos históricos que no están muy distantes en el tiempo pero que sí marcan claramente los cambios producidos es la del seguimiento de la Segunda Guerra del Golfo, en los primeros meses de 1991 y lanzada para liberar Kuwait de las fuerzas invasoras iraquíes, y retransmitida prácticamente en exclusiva por la CNN, y la Tercera Guerra del Golfo, lanzada en marzo de 2003 y que mucha gente en el mundo pudo seguir a través de la aproximación ferozmente crítica de Al Jazira.

En cuanto a Internet los terroristas lo utilizan para coordinarse y planear acciones; para obtener y/o compartir información; para reclutar y movilizar a sus seguidores; para obtener fondos; para hacerse propaganda; y, tan importante como las anteriores, para llevar adelante su guerra psicológica. Cada vez con más frecuencia las páginas Web y los foros de Internet son utilizados por los terroristas para reivindicar atentados o secuestros, como acaba de hacer Al Qaida en las Tierras del Magreb Islámico (AQMI) para aparte de comunicar que tiene en su poder a tres cooperantes españoles y a un botánico francés obligarnos a ver vídeos de sus sangrientas emboscadas contra el Ejército argelino. Desde los tiempos en los que la tradicional dirección en Internet de la red Al Qaida fue cerrada gracias a las contramedidas gubernamentales producidas tras los macroatentados del 11 de septiembre de 2001, la historia del uso de Internet por los terroristas yihadistas salafistas es la de una continua competición entre terroristas y fuerzas del orden y servicios de inteligencia en la que las páginas se van cerrando y van cambiando de denominación sin cesar; los medios de pago para abonar los gastos que Internet genera se han hecho con frecuencia con tarjetas de crédito robadas que al dejar trazas también permitían a los investigadores policiales acabar neutralizándolas; y así se ha venido manteniendo una espiral imparable de actividad en la que, como vemos, se mezclan distintos tipos de delincuencia.[4]

Es útil destacar como otra de esas referencias que tan útiles y estimulantes son para los terroristas que en 2004 un grupo de "hackers" rumanos estuvieron a punto de poner en peligro las vidas de 58 investigadores que trabajaban en una misión científica en la Antártida; con este caso muchos vieron los enormes riesgos que hoy en día corremos todos ante las dependencias e inter-

acciones que la tecnología genera. Para cuando esto ocurría la red de Bin Laden ya llevaba a esas alturas y como hemos visto años de ingente trabajo en el ámbito de la explotación de Internet para sus fines terroristas y la detención tres años después, en 2007, del mayor experto del yihadismo salafista en materia informática hasta ahora identificado – el marroquí Younes Tsouli, más conocido por su alias de 'Irhabi007'[5] – ponía aún más en guardia a agencias de seguridad y a servicios de inteligencia de todo el mundo. Tsouli fue entre 2002 y 2007 el cerebro de Al Qaida en términos de distribución de vídeos terroristas, de diseño de otros instrumentos de propaganda, de perfeccionamiento de los métodos de reclutamiento, de transmisión de instrucciones, de preparación de los terroristas en técnicas violentas, etc. La red terrorista había maximizado sus beneficios en términos de adaptación tecnológica gracias a la utilización de un solo individuo, este joven estudiante hijo de un diplomático marroquí y residente en la capital británica a la que convirtió en la base desde la que puso durante un lustro en manos de Al Qaida sus conocimientos y su gran capacidad de innovación tecnológica.

En su último análisis publicado sobre las tendencias del terrorismo en suelo europeo la Oficina Europea de Policía (EUROPOL) advierte al analizar la situación en Europa en 2008 de que el uso de Internet por los terroristas sigue siendo muy preocupante pues direcciones en la red, weblogs y foros son utilizados para la propaganda y las comunicaciones de grupos y redes terroristas destacándose en particular el incremento en las direcciones de carácter islamista elaboradas en lenguas occidentales en un intento de ampliar lo más posible su espacio de actuación. También han detectado los servicios policiales europeos que algunos grupos terroristas, y en particular grupos islamistas, han comenzado a expandir sus esfuerzos propagandísticos entre audiencias muy concretas, definidas según criterios bien lingüísticos o bien étnicos, y ello aparte de sus esfuerzos tradicionales por llegar al gran público a los que nunca han renunciado.[6]

En términos de radicalización, el Informe de EUROPOL señala que imames radicales ubicados en algunas mezquitas, que antaño eran los principales vehículos de transmisión de los mensajes radicales, cada vez lo son menos, y ello gracias tanto a la creciente tendencia de muchos creyentes a mantenerse vigilantes para hacer frente a los transmisores del radicalismo, como a la importancia de Internet que es lo que aquí más nos interesa. Ello ha contribuido pues a dinamizar aún más el papel de la World Wide Web como instrumento imprescindible para alimentar la radicalización, intensificar el reclutamiento y expandir el adoctrinamiento aunque también señala el Informe que este método nunca podrá reemplazar del todo a la imprescindible relación personal entre reclutadores y los candidatos a ser reclutados, entre entrenador y entrenados, etc.[7] En cualquier caso el ejemplo del marroquí Tsouli es

especialmente ilustrativo sobre los peligros que conlleva canalizar de forma habilidosa el proselitismo terrorista en Internet. Otro ejemplo en la misma línea es el que brinda el denominado "Global Islamic Media Front" (GIMF): en 2008 dos individuos eran condenados por un tribunal vienés acusados de distribuir propaganda yihadista a través del susodicho GIMF, traducida al alemán y conteniendo un vídeo en el que se amenazaba a los Gobiernos de Austria y de Alemania si no retiraban sus fuerzas de Afganistán.[8]

Las medidas de respuesta a los desafíos cibernéticos

A la tradicional práctica de encriptado que dificulta el acceso a los contenidos de las redes utilizadas por los terroristas hemos de unir como dificultad añadida para quienes tratan de impedir el aprovechamiento del mundo cibernético por aquellos la ubicación de muchas de las páginas de los terroristas en servidores situados en países lejanos, haciendo con ello aún más difícil la identificación y la neutralización de los responsables de los mismos.

Todo ello ha ido obligando a los gobiernos a ir realizando esfuerzos que son ante todo y sobre todo nacionales pero que cada vez tienen que incorporar más a la colaboración internacional. Así, junto a medidas previas tomadas en los EEUU, que se consideran a sí mismos como el primer objetivo de ambiciosas y sofisticadas redes de delincuentes y de terroristas que operan en el ciberespacio, la superpotencia decidía poner en marcha un nuevo mando en el seno del Departamento de Defensa, el Mando Cibernético de los EEUU, USCYBERCOM en su acrónimo, que deberá estar plenamente operativo en octubre de 2010 desde su Cuartel General en Fort Meade, en el Estado de Maryland. Por otro lado, el marco jurídico más general en los EEUU en la materia aquí tratada es el delimitado por la denominada "Comprehensive National Cyber Security Initiative" (CNCI, en sus siglas en inglés) adoptada en enero de 2008 por la Administración Bush.

Obviamente y para todos los casos tratados, al ser esta una amenaza que se ha manifestado en tiempos recientes, la mayoría de los instrumentos tanto nacionales como multinacionales puestos en pie para hacerle frente son tan nuevos que aún es difícil hoy por hoy evaluar su eficacia. Junto a los esfuerzos de la superpotencia estadounidense y a los de los países europeos podemos destacar los de algunas potencias regionales que han asumido también la necesidad de blindarse lo más posible frente a esta amenaza. En el subcontinente indio los riesgos de una escalada en la tensión endémica entre India y Pakistán, o también el riesgo de que los enemigos de la aproximación entre Nueva Delhi e Islamabad puedan llegar a utilizar Internet para romper con tan endeble proceso, ha obligado a ambos a tomar medidas nacionales.[9] Por otro lado y sin salir de Asia, el continente donde el debate en torno en las tecnologías se está haciendo

más intenso, la sensibilización entre varios Estados llevaba a dinamizar una organización que agrupa a 26 países y que se denomina "Partenariado Internacional Multilateral Contra las Amenazas Cibernéticas" (IMPACT, en sus siglas en inglés), que tiene su sede en Malaisia y que está formalmente vinculada a la Unión Internacional de Telecomunicaciones (ITU, en sus siglas en inglés).

La obsesión de los yihadistas salafistas por las armas de destrucción masiva

Desde que Ayman Al Zawahiri, número dos de Al Qaida, hiciera referencia a la necesidad de utilizar armas de destrucción masiva en su famosa obra Los Caballeros bajo el Estandarte del Profeta, aludiendo a su constatación de que los occidentales sólo entienden el lenguaje de la sangre y la violencia y por ello hay que golpearles de la forma más letal posible, esta cuestión ha sido una constante tanto para los ideólogos y estrategas yihadistas – piénsese en el hispano-sirio Mustafá Setmarian Al Suri, por ejemplo – como para aquellos que se encargan de combatirles y que tratan de anticiparse a sus próximos pasos aplicando una estrategia antiterrorista proactiva y no reactiva. La posibilidad de que los terroristas utilicen alguna de estas armas se plantea hoy, y ello más como preocupación que como temor inmediato dado que las tecnologías que se hacen necesarias para utilizar dichos tipos de armas no estarían aún, suponemos, en manos de los terroristas.[10] Aunque con respecto a las armas químicas puede citarse el precedente del atentado sufrido por el metro de Tokio el 20 de marzo de 1995 a manos de miembros de la secta "Aum Shirinkyo" fundada en 1987 – y que provocó 12 muertos y miles de afectados – lo cierto es que no es fácil manipular dichos productos como tampoco lo es, de hecho es aún mucho más complicado, manipular productos biológicos susceptibles de ser utilizados como arma.[11] Productos como el gas sarín o el gas nervioso, entre los químicos, o el anthrax entre los biológicos, son sustancias que sólo pueden ser manipuladas por especialistas y contando con las circunstancias y las instalaciones adecuadas. Aquí también se podría argumentar que en lo que a las armas biológicas respecta también se cuenta con antecedentes en la ofensiva personal del Doctor Bruce Irvin quien llevó adelante en solitario la ofensiva en la que enviando anthrax a través del correo acabó en el otoño de 2001 con la vida de 5 personas y dejó en estado crítico a 17 provocando además una enorme alarma social a escala incluso planetaria. A pesar de todo lo dicho y teniendo en cuenta tanto la casuística aportada como las enormes ambiciones de los terroristas yihadistas salafistas, es importante reflexionar en clave de futuro sobre cualquier posibilidad de que en el medio plazo los terroristas comiencen a prestar atención de una manera distinta a estas cuestiones hoy por hoy aparentemente inabordables. Componentes químicos y biológicos – pudiéndose convertir el posible uso de los segundo en un escenario verdaderamente apocalíptico – y su

posible utilización, no sólo podrían provocar muchas víctimas si se utilizan con eficacia letal pero lo que es seguro que van a provocar de partida es ante todo y sobre todo pánico, algo que para la estrategia de los terroristas es crucial como sabemos.[12] Además, teniendo en cuenta el desprecio por sus propias vidas que los terroristas yihadistas salafistas tienen – el ataque contra el metro de Tokio en marzo de 1995 no fue más mortífero precisamente porque los autores, pertenecientes a la secta Shirinkyo, apreciaban sus vidas y evitaron verse contaminados -, ello plantea una dificultad añadida pues en nuestro caso tendríamos más posibilidades de utilización de este tipo de armas e incluso de las radiológicas o nucleares.

Ya para concluir y en lo que a las armas nucleares respecta, y a pesar de la actividad criminal que en este terreno se ha llegado a producir con casos como el del científico paquistaní Khan - que no lo olvidemos trabajó y negoció siempre con Estados-, lo cierto es aquí también que se requiere una tecnología que ningún grupo o red terrorista tendría a su disposición a día de hoy. Sí puede hablarse en cambio de potencial utilización terrorista de materiales nucleares en términos de bombas sucias y también de ataques a instalaciones de tipo nuclear, fueran estas militares o civiles.[13] No obstante también aquí debe de mantenerse la vigilancia atenta de las tendencias pues cabe recordar que en marzo de 2008 fue intervenido uranio empobrecido a miembros de las terroristas Fuerzas Armadas Revolucionarias de Colombia (FARC) y que la posibilidad de utilizar cualquier tipo de bomba sucia está ahí, incluyendo el impacto en términos también de pánico que el simple anuncio de su posible uso produciría. La ventaja que tendrían quienes combaten al terrorismo en lo que a esta casuística conlleva es que los componentes nucleares son relativamente fáciles de detectar si los comparamos con los biológicos y los químicos, y por ello más susceptibles de ser intervenidos en las fronteras interestatales y en controles internos. Pero a pesar de todo lo dicho en términos de plantear las dificultades técnicas – ya que las morales no las tienen como bien sabemos -, cada vez es mayor la preocupación en el mundo en torno a estos escenarios potenciales de actuación terrorista a través del uso de armas o de componentes consideradas como de destrucción masiva.[14]

Carlos Echeverría Jesús (Madrid, 26 de marzo de 1963) es Profesor de Relaciones Internacionales de la UNED y responsable de la Sección Observatorio del Islam de la revista mensual War Heat Internacional. Ha trabajado en diversas organizaciones internacionales (UEO, UE y OTAN) y entre 2003 y 2004 fue Coordinador en España del Proyecto "Undestanding Terrorism" financiado por el Departamento de Defensa de los EEUU a través del Institute for Defense Analysis (IDA). Como Analista del Grupo asume la dirección del área de Terrorismo Yihadista Salafista.

Notas

[1] Para una aproximación general al objeto de estudio véase ROLLINS,John y WILSON, Clay: Terrorist Capabilities for Cyberattack: Overview and Policy Issues Washington DC, Congressional Research Service CRS Report for Congress, actualizado el 22 de enero de 2007, en www.fas.org/sgp/crs/terror/RL33123.pdf.

[2] También los actores gubernamentales intervienen cada vez más en el mundo cibernético pudiendo contar en tiemos recientes con diversos ejemplos, desde la Junta Militar birmana para ahogar las protestas de monjes budistas o el Kremlin para inutilizar la resistencia georgiana en su breve guerra, ambos en 2008, hasta la utilización por el Gobierno chino en julio de 2009 como parte de su estrategia global contra los disturbios en la región musulmana china de Xinjiang inmediatamente antes del comienzo de los Juegos Olímpicos.

[3] ECHEVERRÍA JESÚS, C.: "Today's Islamist Radicalization in Spain" Análisis GEES nº 273, 30 abril 2008, en www.eng.gees.org.

[4] Este procedimiento es explicado detalladamente por Manuel R. Torres Soriano en su artículo "Maintaining the Message: How Jihadists Have Adapted to Web Disruptions" CTC Sentinel Vol. 2, nº 11, noviembre 2009, en www.ctc.usma.edu/sentinel/.

[5] Conocido por este nombre en la red Irhabi quiere decir terrorista en árabe y el número 007 recordaba de forma desafiante al famoso personaje creado por Ian Fleming y llevado con éxito al cine de forma ininterrumpida desde hace cinco décadas.

[6] En su estudio que es global y engloba a todos los grupos terroristas inventariables Europol destaca que junto al uso masivo por parte de los yihadistas Internet era usado en 2008 por los terroristas separatistas para reivindicar sus ataques mientras que los de derechas suelen utilizarla para anunciar manifestaciones y consignas. Véase el apartado 10 titulado Trends en TESAT: EU Terrorism Situation and Trend Report 2009de p. 40.

[7] Ibidem p. 20.

[8] Ibidem p. 20.

[9] La Ley paquistaní denominada de Prevención de Delitos Electrónicos y la india sobre Tecnologías de la Información son ambas de 2008.

[10] Véase el estudio en profundidad de esta cuestión en VELARDE, Guillermo y CARPINTERO SANTAMARÍA, Natividad: Terrorismo nuclear, químico y biológico Madrid, Fundación Cultural de la Milicia Universitaria (FUNDAMU), 6 mayo 2008.

[11] La secta Aum Shirinkyo contaba con instalaciones y con una tradición de investigación y desarrollo en la materia. De hecho realizaron algunos ataques anteriores al del metro de Tokio con diversos objetivos entre 1990 y 1995, incluyendo alguna base militar estadounidense en Japón, aunque no llegó a producir bajas.

[12] Llegados a este punto es útil recordar con los autores VELARDE y CARPINTERO SANTAMARÍA que el caso del asesinato de Alexandr Litvinenko llevó a investigar trazas encontradas de material radioactivo en el restaurante de Londres donde había comido, en un hotel de la ciudad, en dos aviones e incluso en la ciudad de Hamburgo. El fallecimiento de Litvinenko no hizo sino incrementar las alarmas: fallecido el 23 de noviembre de 2006, tres días después cientos de personas habían contactado con la Agencia Británica de Protección de la Salud y a la altura del 4 de diciembre se habían recibido ya 3.000 llamadas de ciudadanos alarmados. Véase VELARDE, G y CARPINTERO SANTAMARÍA, N.: op cit p. 25.

[13] Véase ECHEVERRÍA JESÚS, C.: "La vitalidad de la Iniciativa para Combatir el Terrorismo Nuclear permite presagiar que la amenaza aumenta" Apunte del GEES nº 68, 26 mayo 2008,

[14] Véase TOUAHRI, Sarah: "Morocco hosts seminar on countering nuclear terrorism" Maghrebia 8 febrero 2008.