

# El terrorismo en la sociedad de la información. El caso de Al Qaida

Por **Javier Jordán**

**Resumen:** El objeto de este artículo es analizar cómo una organización terrorista como Al Qaida ha utilizado en su favor las oportunidades que le ofrece el contexto tecnológico e informativo de las economías avanzadas. Y, en consecuencia, indagar sobre el tipo de medidas que deberán adoptarse en el marco de esas sociedades del conocimiento para ganar la batalla a esta nueva forma de terrorismo. En el artículo se describe la forma en que las nuevas tecnologías refuerzan a los actores no estatales, especialmente cuando estos adoptan una estructura de red. Se estudia la importancia de la gestión del conocimiento en el caso de la guerra internacional contra el terrorismo y se finaliza con algunas recomendaciones en materia de lucha contraterrorista.

**Palabras clave:** Terrorismo, Seguridad, Globalización, Sociedad de la información, Tecnología de la información, Gestión del conocimiento, Redes de información, Opinión pública.



Javier Jordán, investigador del Depto. de Ciencia Política y de la Administración de la Univ. de Granada. Es miembro del Centro de Estudios y Análisis de Seguridad de la misma universidad y colaborador del Centro de Estudios de la Defensa Nacional (Ceseden) en Madrid. Junto con Carlos de Cueto es coeditor del libro "Introducción a los estudios de seguridad y defensa".

**Title:** Terrorism in the information society: the case of Al Qaida

**Abstract:** The objective of this article is to analyse how a terrorist organisation such as Al Qaida has successfully taken advantage of the technological and information infrastructure offered by advanced economies and, to this end, the article explores the types of measures needed to be taken by "knowledge societies" in order to win the battle against this new form of terrorism. A description is provided of the ways in which new technologies reinforce non-governmental actors, especially when these adopt a network structure. The importance of knowledge management in the international war against terrorism is also discussed, and the article concludes with recommendations for counter-terrorism policies.

**Keywords:** Terrorism, Security, Globalisation, Information society, Information technology, Knowledge management, Information networks, Public opinion.

**EL TÉRMINO TERRORISMO se acuñó poco después de la revolución francesa para referirse al régimen de terror instaurado por los jacobinos. El concepto se aplicó después a los grupos anarquistas y revolucionarios que proliferaron durante la segunda mitad del siglo XIX.**

Sin embargo, entendido como violencia sistemática cuyos efectos psicológicos exceden la materialidad del acto violento tiene un origen remoto en la historia. Evidentemente, a lo largo del tiempo sus características han variado en función de las circunstancias externas. Al igual que sucede con la guerra, el paso de una generación a otra en el modo de desarrollarse el terrorismo se encuentra en gran medida determinado por los cambios políticos, sociales, culturales y económicos de las sociedades que lo padecen. La emergencia de las socie-

dades basadas en el conocimiento y la revolución en las tecnologías de la información constituyen dos importantes motores de cambio en la forma de plantearse los conflictos.

**«Al Qaida, en árabe 'La Base', fue designada así por Bin Laden, pero no como base física, sino como base de datos»**

El objeto de este artículo consiste en analizar el modo en que la organización terrorista Al Qaida ha utilizado a su favor las oportunidades que le ofrece el contexto tecnológico e informativo de las economías avanzadas. Y, en consecuencia, indagar sobre el tipo de medidas que deberán adoptarse en el marco de esas sociedades del conocimiento para ganar la batalla a es-

ta nueva forma de terrorismo. El enfrentamiento que inició esta organización hace más de una década contra los países occidentales también constituye un caso especial porque en él, la diferencia entre terrorismo y conflicto bélico no resulta fácil de delimitar.

¿Es la lucha entre Al Qaida y la coalición internacional una guerra? Tradicionalmente los grupos terroristas han utilizado la violencia como una forma de presión para obtener determinadas concesiones políticas. Por ello, es habitual que a un atentado le siga una reivindicación por parte del grupo responsable. Sin embargo, la lucha que ha emprendido la red a la que pertenece Bin Laden persigue un objetivo diferente, que en último término consiste en la derrota del mundo occidental. La magnitud de los atentados, la letalidad de los mismos y la no reivindicación son

pruebas de ello. El presidente **Bush** afirmó poco después del 11 de septiembre que aquello no había sido un ataque terrorista sino un acto de guerra. La naturaleza de los atentados, la motivación que los originó así como la respuesta internacional que han provocado hacen pensar que efectivamente es así.

En realidad, el empleo del terrorismo por parte de *Al Qaida* parece tener un carácter meramente instrumental (de arma de guerra), ya que dada la supremacía militar de EUA y la *Otan* en el terreno de las fuerzas convencionales, el enfrentamiento sólo tiene posibilidades de resultar favorable si se libra con tácticas asimétricas. Por tanto, el terrorismo se convierte en este caso en un instrumento de destrucción que no sólo busca llamar la atención sino también eliminar físicamente al enemigo. Mantiene, al mismo tiempo, la carga psicológica provocando un estado de inseguridad y de alarma social desproporcionado. Y se suma a la batalla por la percepción, en la que el discurso político, el papel de los medios de comunicación y las acciones simbólicas adquieren una importancia mayor que en los conflictos tradicionales.

Las tecnologías de la información:  
multiplicadores de fuerza de los nuevos actores en materia de seguridad

La revolución tecnológica y la globalización de las comunicaciones potencian el papel que pueden desempeñar actores relevantes desde el punto de vista de la seguridad, especialmente de los de carácter no estatal. Hasta no hace mucho la guerra había sido patrimonio casi exclusivo de los estados, pues era necesario contar con los enormes recursos de una nación para sostener el esfuerzo bélico. Pero en el nuevo entorno de los países con economías avanzadas, la tecnolo-

gía y la capacidad de influir sobre la opinión pública —y de este modo ejercer presión indirecta sobre las decisiones de los gobernantes— ponen en manos de grupos terroristas, señores de la guerra, grupos violentos antisistema o sujetos aislados, las herramientas para enfrentarse a estados o, incluso, a una coalición internacional a pesar de que éstos cuenten con importantes fuerzas armadas. En la sociedad de la información el poder se transfiere a entidades no estatales.

### «Los terroristas también se benefician de los programas de encriptación que hay disponibles en la Red»

Esto tiene sus aspectos positivos en cuanto que refuerza el papel de la sociedad civil, pero también su lado oscuro al beneficiar a sectores perversos de la humanidad. Al mismo tiempo, la revolución en las tecnologías de la información posibilita que estos nuevos actores adopten una estructura en red, similar a la que tienen muchas empresas con el fin de gestionar más eficazmente la información y sobrevivir en un mercado cambiante (**Castells**, 1997: 229-243; **Nichiporuk, Builder**, 1997: 312-313).

Redes han existido siempre. Lo que las hace ahora especialmente aptas y poderosas son los adelantos tecnológicos, que permiten su coordinación en la concepción, ejecución y retroalimentación de sus operaciones. Internet y el resto de tecnologías de la información ofrecen grandes posibilidades en cuestión de difusión de la agenda política, reclutamiento, recaudación de fondos, coordinación y comunicación entre grupos e intra-grupo, acopio de información e inteligencia, anonimato y secreto en las ac-

tividades tanto rutinarias como tácticas (**Flemming, Stohl**, 2000).

En el nuevo contexto son además superiores a las jerarquías, pues éstas reaccionan más despacio y con menos eficacia a los cambios que se producen en un ambiente altamente informativo y en constante mutación. A la vez son menos vulnerables, pues la pérdida de uno de los elementos puede ser reemplazada por la actuación de otros. Las redes, a diferencia de las instituciones jerárquicas, están configuradas en estructuras de mando y control descentralizado, siendo por ello más resistentes a la decapitación.

Todas estas características son aplicables al caso que nos ocupa. *Al Qaida* (en árabe “La Base”, designada así por **Bin Laden**, pero no como base física, sino como base de datos) es una red formada por células terroristas que cuentan con el apoyo financiero, logístico y moral de individuos y colectivos islamistas radicales presentes en varias regiones del planeta, incluidas Europa y EUA.

Al mismo tiempo la organización mantiene relaciones “reticulares” con otros grupos terroristas independientes que reciben su respaldo y actúan en Chechenia, Tayikistán, Somalia, Yemen, Egipto, Filipinas y Cachemira (**Shay, Schweitzer**, 2000). Esta red ha contado además con la ayuda de algunos estados, siendo uno de ellos el desaparecido régimen talibán. Además es posible que la red se beneficie también del apoyo indirecto del gobierno de Irak (que permite la presencia en su territorio de organizaciones terroristas como *Abu Nidal*, o el *Frente para la Liberación de Palestina*) (**Simon**, 1999: 219), y de algunos dirigentes de Irán (*Guardia de la Revolución y Ministerio de Inteligencia y Seguridad* que, en cualquier caso, apoyan abiertamente a *Hizbollah*, grupo relacionado también con *Al*

# d Portal

Portal desarrollado por  
EVER TEAM de gestión  
de contenidos e información

**Loris**

El sistema de gestión integral de Bibliotecas y Centros de Documentación

**Clara**

El sistema de gestión integral de archivos

**Taurus +**

El sistema de archivo electrónico documental, COLD, OCR e ICR

**Flora**

El sistema de gestión de los ciclos de producción de documentos Docflow

**Maxim**

Herramienta de desarrollo para la integración de imágenes

**Doris**

El sistema integral de gestión documental

**Ultimus**

Sistema de automatización de procesos Workflow



**EVER**

El **conocimiento** en acción

**EVER documéntica, S.A.**

Avda. de la Industria, 32  
28108 Alcobendas, MADRID  
ESPAÑA  
Tel. (34) 91 663 02 58

Fax: (34) 91 663 01 99  
e-mail: [ever@everdoc.com](mailto:ever@everdoc.com)  
web: [www.everdoc.com](http://www.everdoc.com)  
[www.ever-team.com](http://www.ever-team.com)

**EVER Team:** Francia

**EVER luk:** Alemania

**EVER América:** Canadá y EE.UU.

*Qaida*). Con anterioridad a 1998 *Al Qaida* contó con el apoyo del régimen de Sudán. Sin embargo, desde 2000 el gobierno sudanés ha iniciado cierta cooperación con EUA en materia de antiterrorismo, aunque se teme que en el país existan todavía elementos relacionados con **Bin Laden** (*US State Department*, 2000).

Como decimos, la propia organización de **Bin Laden** tiene estructura de red. Se trata de diferentes células y grupos que actúan bajo su financiación y de acuerdo con sus objetivos estratégicos (*Jane's Information Group*, 2001). Una configuración que se deduce del modo de proceder de *Al Qaida* incluso antes del 11 de septiembre. Los ataques fallidos o exitosos en los que ha tenido relación —bien es cierto que en algunos de ellos esa implicación no se encuentra del todo confirmada, aunque existen importantes indicios— han tenido como escenario Somalia, Arabia Saudí, Yemen, Kenia, Tanzania, Francia, Gran Bretaña, Filipinas, EUA, Albania y Australia.

La nacionalidad y origen de los que han participado en dichas acciones es también muy variada (tunecinos, marroquíes, egipcios, argelinos, afganos, saudíes, pakistaníes, etc.) (**Shay, Schweitzer**, 2000). El modo de operar desvela también dicha estructura en red, pues muchos de los que han participado en la preparación o realización de los atentados era la primera vez que lo hacían y, muchas veces, residían en los países objetivo. Es decir, sus cuadros permanentes formaban grupos a partir de los recursos presentes en el lugar de ejecución. Esas células locales contaban con la financiación y el apoyo moral de **Bin Laden**, pero llevaban a cabo sus acciones de manera autónoma. En la acción del 11 de septiembre se dio sin embargo una mayor coordinación, y —según revela uno de los vídeos capturados

en Afganistán— el propio magnate saudí estaba al corriente de los planes del ataque.

Los medios que han hecho posible la acción de la red se encuentran disponibles en el entorno globalizado y de la sociedad de la información, y eso es lo que le concede una enorme superioridad. Además de los sistemas de comunicación convencionales (teléfonos móviles, fax e internet), que le resultan esenciales para su eficacia, estos grupos se han beneficiado de la capacidad que ofrecen los sistemas de diseño por ordenador para falsificar pasaportes y billetes de avión, del dinero electrónico para surtir a los diferentes grupos, de medios de visión nocturna comerciales y de la posibilidad de aprender a volar aviones de pasajeros en las academias privadas del propio país objetivo. Y todo ello además, por una suma de dinero relativamente baja. En total se calcula que la preparación y el ataque contra las Torres Gemelas y el *Pentágono* se pudo realizar con un presupuesto de 500.000 US\$. Aproximadamente una cuarta parte del valor de uno solo de los misiles *Tomahawk* lanzados en los primeros días de la ofensiva contra Afganistán.

Las tecnologías de la información benefician notablemente a las células terroristas, pudiendo actuar a pesar de las distancias geográficas y realizar actividades complementarias entre ellos. El empleo de internet incrementa la velocidad en la transmisión de los mensajes, proporciona abundante información e inteligencia, permitiendo un mayor diálogo y coordinación entre sus miembros. Esto aumenta también la flexibilidad de la organización y la cooperación con actores externos a la misma. Los individuos con una agenda común pueden formar grupos y, tras una acción determinada, poner fin a su relación temporal.

Al parecer, **Bin Laden** ha realizado un uso intenso de las tecnologías de la información desde su antiguo cuartel general en Afganistán, gracias a un sistema instalado por miembros egipcios de *Al Qaida* (**Arquilla, Ronfeldt, Zanini**, 1999: 65). También ha empleado cd-rom para difundir manuales de empleo de explosivos y de tácticas terroristas. Dentro de la red *Al Qaida* es frecuente el empleo de las salas públicas de internet en la coordinación de las operaciones, tal como hicieron los pilotos suicidas del 11 de septiembre.

«La mayor parte de los grupos terroristas disponen actualmente de su propia página web»

Otros grupos terroristas también aprovechan la Red. Es el caso de *Hamas*, que emplea habitualmente internet para coordinar sus actividades, planteando grandes dificultades a los servicios de seguridad israelíes que se ven desbordados para controlar todo el tráfico de información digital. Además, los terroristas también se benefician de los programas de encriptación que hay disponibles en la Red. Algunos de ellos son métodos de encriptación muy sofisticados como la esteganografía que consiste en esconder los datos dentro de otros, como por ejemplo un mensaje dentro de una imagen (**Zanini, Edwards**, 2001: 37-38).

Mayor importancia de los aspectos informativos y relacionados con la percepción

Ésta es una de las características que más varía con respecto a los conflictos tradicionales. La batalla se extiende también al terreno de la percepción, que concede justificación y legitimación al empleo de la fuerza y sostiene la voluntad

política para adoptar las medidas precisas para vencer. Aunque el aspecto informativo siempre ha sido tenido en cuenta en las contiendas (propaganda, guerra psicológica, etc.), en la actualidad abandona el lugar subsidiario que venía ocupando y adquiere una posición preeminente y decisiva. No es que antes no existiera, sino que ahora adquiere una importancia casi determinante.

Más que nunca los conflictos giran en torno al conocimiento, al *soft power*. El desafío frente al adversario es también epistemológico, pues lo que se busca es transformar la percepción de la sociedad (Arquilla, Ronfeldt, 2001: 20). Se trata de librar la batalla por el relato, por la historia, por lo que justifica o reprueba la adopción de determinadas decisiones. Información y poder se encuentran cada vez más entrelazados. Si uno de los contrincantes se hace con los resortes cognitivos de la sociedad que sostiene al adversario, puede llegar a forzar la voluntad de los decisores políticos o a deslegitimar las medidas tácticas o estratégicas necesarias para lograr la victoria. Aunque no existan impedimentos operativos para realizar determinadas acciones, la derrota en el terreno de la percepción puede dificultar el proceso de toma de decisiones.

Al mismo tiempo, la ocupación efectiva de la infósfera permite también reforzar las lealtades en el propio bando y lograr la participación de otros actores en el esfuerzo conjunto. Toda organización tiene un nivel narrativo que se refiere a los valores, intereses y experiencias. Proporciona identidad y sentido de pertenencia, es lo que hace surgir un “nosotros” frente a “ellos”. Además, el relato ofrece un significado, un sentido de misión, de causa y finalidad. Una buena historia puede lograr cohesión y hacer difícil que se abandone la red y también puede crear co-

nexiones entre diferentes redes (Ronfeldt, Arquilla, 2001: 328-329).

En el caso de *Al Qaida*, los testimonios de miembros arrepentidos o capturados revelan la existencia de dicho relato, muy útil en la captación de nuevos miembros y en que algunos de ellos estén dispuestos incluso a inmolarse por la causa común en atentados suicidas (Jane's Information Group, 2001). A esto se une otro factor que beneficia a la organización terrorista, y es que el terrorismo tiene efectos contagiosos, con lo que el recurso a esta estrategia incita a individuos y grupos (hasta ese momento pasivos) a participar en la violencia. En el caso del 11 de septiembre, la “hazaña” de las Torres Gemelas puso al descubierto la vulnerabilidad occidental; y otros actores pueden sentirse atraídos a emularla.

**«Dentro de *Al Qaida* es frecuente el empleo de las salas públicas de internet en la coordinación de las operaciones, tal como hicieron los pilotos suicidas del 11 de septiembre»**

Un ejemplo de ello habría sido el caso del terrorista de origen británico **Richard Reid**, que en la Navidad de 2001 intentó destruir el vuelo París-Miami con explosivo C4 escondido en su calzado (el cual consiguió además comprándolo en internet). En este caso se trataba de un miembro importante de *Al Qaida*, cuya vinculación con la organización se ha demostrado gracias a las bases de datos informáticas capturadas en Afganistán. Otro ejemplo más claro de imitación (sin ninguna relación con *Al Qaida*) fue el del adolescente norteamericano **Charles Bishop** que estrelló su avioneta contra una torre del *Bank of America* en Tampa

(Florida) en enero de 2002. En sus bolsillos encontraron frases escritas de admiración a **Bin Laden**. En el contexto de la violencia entre israelíes y palestinos, el contagio y la victoria narrativa explicaría la “ciber-yihad” lanzada por hackers aficionados contra sitios comerciales y gubernamentales israelíes en internet desde Marruecos hasta Pakistán.

En el caso de la guerra contra el terrorismo, el terrorista saudí ha demostrado entender las claves cognitivas del conflicto y así lo ha manifestado en sus emisiones en vídeo, especialmente en la primera de todas, al inicio de los bombardeos. En ella los mensajes se dirigen por un lado a las sociedades musulmanas. Pretende que tomen conciencia de su situación de inferioridad y opresión, de la hipocresía de los dirigentes musulmanes que colaboran con EUA, de las oportunidades que surgen con el nuevo tipo de guerra, pidiendo la movilización de todos los musulmanes contra el adversario del Islam.

Estas ideas se ven reforzadas por las imágenes de muertes de civiles provocadas por los bombardeos norteamericanos en Afganistán transmitidas por la cadena *Al Yazira* y el resto de cadenas mundiales. Muy especialmente por la coincidencia en el tiempo de imágenes de las acciones de represalia del ejército israelí contra los palestinos, que no provocan sin embargo una respuesta de EUA y Europa tan contundente como la llevada a cabo en Afganistán. Por otra parte, la estrategia informativa de **Bin Laden** tiene también como objetivo a las sociedades occidentales. La finalidad es doble.

Los atentados y la guerra se dirigen a provocar el terror y la inseguridad (acabando con la aparente invulnerabilidad de las retaguardias norteamericana y europea cuando sus ejércitos participaban en operaciones militares en regio-

nes lejanas). Y a su vez a crear el desconcierto sobre la legitimidad de la política occidental hacia el mundo árabe y (en general) hacia el mundo no desarrollado. Para ello se utilizan diversos medios: las declaraciones del propio terrorista en su primera grabación; la emisión de imágenes de los daños civiles producidos por los bombardeos occidentales; el debate abierto sobre la cuestión en el espacio público de las sociedades occidentales, e incluso el silencio de **Bin Laden** sobre su responsabilidad personal en los atentados del 11 de septiembre (que alimentaría las “teorías de la conspiración”, convirtiendo a la víctima en posible culpable).

A largo plazo la lucha en la infósfera podría resultar desfavorable para los gobiernos norteamericano y europeos. Aunque en el terreno militar se lograsen avances claros (como ha sido la caída del régimen talibán y la expulsión de *Al Qaida* de Afganistán, o el posible bombardeo a campos de entrenamiento terroristas en Somalia, Yemen u otros países), la opinión pública interior puede ponerse en contra de estas medidas y dificultarlas en el futuro si considera que no resuelven el problema y que se trata del ejercicio arbitrario de la supremacía militar occidental sobre el mundo subdesarrollado.

De hecho, en EUA el debate está abierto desde hace meses —a pesar de que en esta parte del Atlántico parezca que aquella nación es un bloque monolítico, ya que es la idea que nos transmiten nuestros medios de comunicación pero que se desmiente si se consulta la prensa de aquel país—, y en Europa las voces críticas sobre el modo en que se está conduciendo la campaña antiterrorista se hacen oír cada vez más. Esto no significa que el hecho de disentir implique ponerse del lado de los terroristas. Las democracias se caracterizan

por la libertad de prensa y de opinión, y éstas no deben verse afectadas negativamente en la lucha contra el terrorismo, pues de lo contrario se habría asestado un golpe fatal al sistema.

Precisamente esa libertad dificulta la realización de acciones ilegítimas en la lucha contra el terror. Pero también es preciso reconocer que la apertura informativa y el debate público de las democracias pueden ser utilizados hábilmente por el enemigo a través de esa lucha por la percepción, con el fin de lograr objetivos injustos. Esto obliga a que en un contexto de conflicto el debate público sea especialmente riguroso y responsable. La aliada del adversario no es la libertad, sino la frivolidad de las opiniones expresadas en los medios de comunicación.

**«En el caso de *Al Qaida* no existen noticias de que dicha organización haya realizado ataques ciberterroristas»**


En esta estrategia de lucha por la percepción, los nuevos actores cuentan con la ventaja de que los sistemas de comunicación existentes en la infósfera no resultan tan fácilmente controlables como hace unas décadas. Internet está variando la difusión de “uno a muchos” propia de la televisión, radio y prensa, a un sistema interactivo de “muchos a muchos”. La mayor parte de los grupos terroristas disponen actualmente de su propia página web (en este artículo no detallaremos sus direcciones para no hacerles propaganda y también porque visitar sus sitios puede tener efectos maliciosos, ya que en algunos de ellos se realiza un rastreo de las visitas). Así pueden publicar notas de prensa tras los atentados, justificando sus acciones y

exponiendo los motivos que le llevan a mantener la lucha.

A veces se muestran en ellos imágenes muy cruentas, que sirven de estímulo a sus activistas (para *Hizbollah*, un procedimiento normal es realizar una grabación en vídeo de cada atentado que después se emite con fines propagandísticos y de captación). En el caso que nos ocupa, es muy probable que *Al Qaida* haya utilizado la red para hacer llegar a la cadena *Al Yazira* sus mensajes, aunque el modo concreto como fueron transmitidos desde el lugar en que se grabaron constituye todavía un secreto.

Internet ofrece otras posibilidades para hacer propaganda que, sin embargo, *Al Qaida* no ha utilizado. Se trata de mensajes de correo electrónico empleados como instrumento de presión. Este tipo de *spam* fue algo común durante la campaña aérea de la *Otan* en Kosovo. Un gran número de periodistas y líderes de opinión de los países aliados recibieron mensajes de diferente origen (en algunos casos de personas individuales y en otros muy posiblemente del gobierno), procedentes de Yugoslavia condenando los bombardeos y pidiendo el apoyo para la población civil serbia. En este mismo caso, la propia *Alianza* realizó una campaña informativa sobre la opinión pública serbia con el fin de legitimar sus acciones y hacer perder apoyo al régimen de **Milosevic**. Por ello, aunque la televisión y la radio serbia (controladas por el gobierno) fueron bombardeadas en varias ocasiones, se evitó dañar los sistemas de conexión a internet con el fin de que la población tuviera acceso a fuentes de información exteriores (**Denning**, 2001).

Otro ejemplo de uso del mail con fines propagandísticos es el comentado a continuación. Aunque muy posiblemente no fue difundido por *Al Qaida*, el tráfico de mensajes electrónicos sí que sirvió



# En primera línea en Sistemas de Información y Gestión del Conocimiento.

- Informática Documental
- Internet, Intranet
- Edición de Bases de Datos en CD-Rom
- Base de Datos PRENSA BARATZ (Internet y CD-Rom)
- Sistema Integrado de Gestión Bibliotecaria Absys
- Catalogación Retrospectiva
- Sistema Integrado de Gestión de Centros Archivísticos Albalá



Raimundo Fernández Villaverde, 28  
28003 Madrid (España)  
Teléfono +34 91 456 03 60 - Fax +34 91 533 09 58  
[www.baratz.es](http://www.baratz.es) - E-mail: [informa@baratz.es](mailto:informa@baratz.es)



en los primeros días de consternación tras el 11 de septiembre para esparcir el rumor de que las imágenes de la *CNN* con niños palestinos celebrando los atentados correspondían a la guerra del Golfo. Esta habladuría fue rápidamente desmentida, pero constituye un ejemplo de cómo la Red fue utilizada como un arma informativa para atribuir intenciones perversas a uno de los símbolos de la supremacía estadounidense.

### El ciberespacio ¿campo de batalla del futuro?

En el caso de *Al Qaida* no existen noticias de que dicha organización haya realizado ataques ciberterroristas. No obstante, dedicaremos algunas líneas de este artículo a tratar el tema. Además de la importancia que tiene para la transmisión de ideas y mensajes, el ciberespacio se está convirtiendo en uno más de los lugares de la guerra, uniéndose a los tradicionales de tierra, mar y aire. Sin embargo, no conviene por el momento magnificar esta nueva dimensión. La mayor parte de los daños de gran magnitud causados por ataques cibernéticos han sido obra de hackers movidos por retos personales o simple afán de lucro, pero sin una agenda política como la que pueden tener grupos terroristas o un gobierno hostil. Ciertamente, durante la guerra de Kosovo y tras el inicio de la *Intifada* se han producido ataques contra los sitios web de uno y otro lado, pero su alcance ha sido escaso, consistiendo las más de las veces en una negación de servicio temporal de la web objetivo.

Es muy posible que esta tendencia cambie en el futuro a un mayor empleo de la Red como medio de violencia. Por un lado, las economías avanzadas son cada vez más dependientes de las infraestructuras de comunicaciones. Y los ejercicios simulados por las pro-

pias fuerzas armadas de EUA han demostrado lo vulnerables que pueden ser sus sistemas estratégicos frente a un ataque informático con software disponible en la propia Red (**Adams, 2001: 100-101**).

Por otra parte, aunque los grupos terroristas y los ejércitos, como cualquier otra organización, son tradicionales en sus métodos y tardan en sacar el máximo partido de las ventajas tecnológicas que aparecen en el mercado, también pueden apostar por esta nueva dimensión como complemento de acciones que lleven en otros campos. Además la conexión en red de los grupos puede estimular y favorecer la adopción de dichos medios y tácticas, si alguno de ellos comienza a cosechar éxitos en este terreno.

### **«Los ejercicios simulados por EUA han demostrado lo vulnerables que pueden ser sus sistemas estratégicos frente a un ataque informático con software disponible en la Red»**

Es evidente que los conflictos del futuro no se librarán sólo a través de fibra óptica. A pesar de los daños económicos u organizativos que pueda producir, un ataque informático no sustituye el dramatismo de las muertes que provoca un atentado terrorista y no elimina la posibilidad de que se prefiera causar esas pérdidas colocando un explosivo en el sistema informático en cuestión, sin emplear para ello la Red. No obstante, lo más probable es que la ciberguerra y el ciberterrorismo adquieran mayor importancia en el futuro (con las generaciones educadas en internet), y que los países desarrollados mejoren en consecuencia sus propios procedimientos de seguridad informática.

### Necesidad de readaptar los mecanismos de seguridad tradicionales

Ante el tipo de amenaza que plantea un adversario como *Al Qaida* resulta necesario amoldar los instrumentos de seguridad de las sociedades avanzadas: tanto los ejércitos, como las fuerzas y cuerpos de seguridad internos. Este tema necesitaría mucho más espacio que el epígrafe final del artículo, así que nos limitaremos a enunciar tres principios que pueden ser útiles para la reforma de las agencias de seguridad.

En primer lugar es preciso llevar a cabo cambios organizativos que permitan procesar más rápidamente la información y responder de la manera más adecuada a las contingencias y amenazas que se puedan plantear. Posiblemente la estructura a adoptar debería asemejarse a una red en la que se integren los diferentes ejércitos, cuerpos policiales, servicios de inteligencia, gabinetes de comunicación y empresas privadas que puedan jugar un papel destacable en cualquiera de los aspectos relacionados con el conflicto. La gestión del conocimiento y la cooperación interagencias van a ser cuestiones clave, y en eso el sector privado puede tener mucho que enseñar a las estructuras, en ocasiones, excesivamente jerarquizadas y con importantes rivalidades entre sí, de las agencias estatales de seguridad.

La segunda clave también tiene que ver con la gestión de la información, y consiste en prestar mayor atención a la dimensión epistemológica del conflicto. La victoria va a depender tanto de la supremacía y el éxito en la infosfera (en el terreno de las percepciones e ideas) como en el campo material donde se desarrolla la lucha armada. Para esto va a ser necesario un liderazgo político que mida el alcance cognitivo de todas las medidas adoptadas y que defina una estrategia

comprehensiva para obtener el éxito en todos los frentes. Es decir, una combinación acertada de *hard* y *soft power*.

El tercer aspecto consiste en aprovechar las ventajas tecnológicas, lo que puede plantear dilemas importantes entre seguridad y libertad. Las actividades y la comunicación de los grupos terroristas se verían seriamente dificultadas si se consiguen desarrollar y aplicar sistemas que permitan un mayor control de las comunicaciones. Sin embargo también afectaría a la privacidad de las comunicaciones del resto de los ciudadanos. Por ello lo más prudente parece ser realizar esos rastreos con permiso judicial y sólo sobre personas concretas.

Aunque esto suponga un impedimento en la lucha contra el terrorismo (y por tanto una vulnerabilidad real), es un coste en seguridad que hay que aceptar si se quiere seguir gozando del resto de libertades. Los avances en biomedición (reconocimiento digital del rostro, detectores de mentiras, llaves biológicas) también pueden aportar herramientas útiles en el esfuerzo antiterrorista. Al mismo tiempo, el principio de sacar el máximo rendimiento de los adelantos tecnológicos también es aplicable al empleo de la fuerza armada. La campaña en Afganistán ha demostrado hasta qué punto son importantes las armas de última generación (empleadas junto a otros sistemas

más antiguos) a la hora de derrotar físicamente al adversario.

La aplicación a la defensa de los avances en materia de tecnologías de la información —que están haciendo posible lo que en los estudios de seguridad se denomina la “revolución en los asuntos militares”— proporciona una supremacía armada que limita la libertad de maniobra del adversario. En el caso concreto de esta guerra, **Bin Laden** sufre la restricción de permanecer constantemente en paradero desconocido, ya que las capacidades militares de EUA tienen un alcance global.

Pero, a pesar de todos estos medios, el escenario actual de seguridad resulta demasiado complejo para que ninguna de las medidas que se adopten pueda ofrecer una solución del todo satisfactoria. El traspaso del poder y de la capacidad de destrucción a actores no estatales hace menos controlable el empleo de la violencia terrorista, que podrá ser quizás contenida en unos límites aceptables, pero no erradicada.

## Bibliografía

- Adams, J.** “Virtual defense”. En: *Foreign affairs*, 2001, May-June, pp. 98-112.
- Arquilla, J.; Ronfeldt, D.** *The emergence of Noopolitik: toward an America information strategy*. Rand: Santa Monica, 1999.
- Arquilla, J.; Ronfeldt, D.; Zanini, M.** “Networks, netwar and information age terrorism”. En: **Lesser, I. O.; Hoffman, B.; Arquilla, J.; Ronfeldt, D. R.; Zanini, M.; Jenkins, B. M.**

*Countering the new terrorism*. Rand: Santa Monica, 1999, pp. 39-84.

**Arquilla, J.; Ronfeldt, D.** “The advent of netwar (revisited). En: **Arquilla, J.; Ronfeldt, D.** (eds.). *Networks and netwars: the future of terror, crime, and militancy*. Rand: Santa Monica, 2001, pp. 1-25.

**Castells, M.** *La era de la información*. En: *Economía, sociedad y cultura. Volumen I. La sociedad red*. Madrid: Alianza Editorial, 1997.

**Denning, D. E.** “Activism, hacktivism, and cyberterrorism: the internet as a tool for influencing foreign policy”. En: **Arquilla, J.; Ronfeldt, D.** (eds.). *Networks and netwars: the future of terror, crime, and militancy*. Santa Monica: Rand, 2001, pp. 239-288.

**Flemming, P.; Stohl, M.** *Myths and realities of cyberterrorism*. Office of International Programs and the Center for Education and Research in Information Assurance and Security, 2000.

[http://www.ippu.purdue.edu/info/gsp/cyberterror\\_intro.html](http://www.ippu.purdue.edu/info/gsp/cyberterror_intro.html)

**Freedman, L.** *The revolution in strategic affairs*. En: *Adelphi paper*, n. 318, Iiss, London, 1998.

**Gray, C. S.** *Modern strategy*. Oxford University Press, 1999.

*Jane's Information Group. Penetrating Al-Qaida*. 2001, 14 September.

[http://www.janes.com/security/international\\_security/news/jir/jir010914\\_1\\_n.shtml](http://www.janes.com/security/international_security/news/jir/jir010914_1_n.shtml)

**Katzman, K.** “Terrorism: near Eastern groups and state sponsors, 2001”. En: *CRS report for Congress*, 2001, Washington, September 10.

**Nichiporuk, B.; Builder, C. H.** “Societal implications”. En: **Arquilla, J.; Ronfeldt, D.** *In Athena's camp. Preparing conflict in the information age*. Santa Monica: Rand, 1997, pp. 295-314.

**Ronfeldt, D.; Arquilla, J.** “What next for networks and netwars”. En: **Arquilla, J.; Ronfeldt, D.** (eds.). *Networks and netwars: the future of terror, crime, and militancy*. Santa Monica: Rand, 2001, pp. 311-361.

**Shay, S.; Schweitzer, Y.** *The afghan alumni terrorism. Islamic militants against the rest of the world*, 2000, November 6.

<http://www.ict.org.il/articles/articleDet.cfm?articleid=140>

**Simon, R.** *The new jackals: Ramzi Yousef, Osama bin Laden and the future of terrorism*. London: André Deutsch, 1999.

**State Department.** *Patterns of global terrorism*. Department of State Publication 10687, Office of the Secretary of State, Office of the Coordinator for Counterterrorism, Released April 2000.

**Zanini, M.; Edwards, S. J.** “The networking of terror in the information age”. En: **Arquilla, J.; Ronfeldt, D.** (eds.). *Networks and netwars: the future of terror, crime, and militancy*, 2001, pp. 29-60.

**Javier Jordán**  
[jjordan@ugr.es](mailto:jjordan@ugr.es)

El profesional de la información está abierto a todos los bibliotecarios, documentalistas y otros profesionales de la información, así como a las empresas y organizaciones del sector para que puedan exponer sus noticias, productos, servicios, experiencias y opiniones.

Dirigir todas las colaboraciones para publicar a:

*El profesional de la información*

Apartado 32.280

08080 Barcelona

Fax: +34-934 250 029

[epi@sarnet.es](mailto:epi@sarnet.es)