SOLEDAD SEGOVIANO MONTERRUBIO

Al Qaeda en la red

Si se quiere entender cómo Al Qaeda ha sido capaz de sobrevivir y adaptarse después de la guerra en Afganistán, a la vez que evolucionar de forma progresiva de la organización terrorista que cometió los atentados del 11-S al movimiento de alcance global que es en la actualidad, es necesario detenerse en el análisis y estudio de sus estrategias de comunicación a través de Internet como uno de los factores fundamentales.

Soledad Segoviano Monterrubio es profesora de Relaciones Internacionales en la Universidad Complutense de Madrid

En el contexto de la era de la información y la globalización propio de la sociedad internacional actual, la revolución tecnológica e informativa representa el elemento determinante para analizar la progresiva transformación de los distintos actores, relaciones, factores y conflictos de la sociedad del siglo XXI. De acuerdo con la interpretación de John Arquilla y David Ronfeldt, esta transformación se ve impulsada por dos razones.[1] En primer lugar, porque la revolución tecnológica favorece y fortalece las formas de organización estructuradas en red que dan un mayor protagonismo a los actores no estatales —como grupos de terroristas, de narcotraficantes, delincuencia organizada, disidentes, movimientos sociales— frente a las formas estatales tradicionales y jerárquicas, que son menos flexibles y adaptables. La segunda razón se encuentra en la propia dinámica del desarrollo tecnológico, ya que según avance la revolución de las nuevas tecnologías, la gestión, evolución y resultado de los conflictos internacionales dependerá cada vez más de la información y de las comunicaciones y, por extensión, del manejo y control de la percepción social. Estos elementos han incidido en los logros de la organización Al Qaeda.[2]

El uso de las nuevas tecnologías por parte de estos actores no estatales permite el contacto y la integración de los miembros, favoreciendo el nacimiento de unas formas de organización, doctrina y estrategia en red que ante todo se carac-

1 John Arquilla y David Ronfeldt, "Redes y guerra en red: el futuro del terrorismo, el crimen organizado y el activismo político", Alianza Editorial, Madrid, 2003, p. 31.

2 Paul Eedle, "Al Qaeda´s superweapon: the internet", en http://outtherenews.com

terizan por su flexibilidad y adaptabilidad.[3] Este tipo de estructura, ya se trate de red en forma de cadena, en forma de eje o red multicanal o de matriz resulta muy efectiva tanto en operaciones ofensivas como defensivas.[4] En el ataque, las redes de enjambre deben ser capaces de unirse rápida y sigilosamente sobre el objetivo para disolverse y volver a dispersarse luego.[5] Por tanto, en los nuevos conflictos caracterizados por la guerra en red, se producirán operaciones ofensivas en forma de enjambres en detrimento de los tradicionales frentes de batalla.

En lo que se refiere a su capacidad de defensa, las redes se caracterizan por su gran elasticidad lo que las convierte en resistentes a todo tipo de ataques, difíciles de romper, de derrotar y de destruir en su totalidad. "Quien proyecte atacar una red se encontrará limitado: generalmente sólo es posible encontrar y enfrentarse a pequeños fragmentos de una red", según Arquilla y Ronfeldt. "Además, la capacidad de rechazo inherente a las redes permitiría sencillamente absorber una serie de ataques a determinados nodos, haciendo creer al atacante que la red ha sido dañada y ha quedado inoperativa cuando, en realidad, permanece efectiva y en busca de nuevas oportunidades para una sorpresa táctica".[6]

Estos planteamientos teóricos han tenido una clara correspondencia con la estrategia en red desarrollada por Al Qaeda, cuyo nivel de sofisticación y capacidad de "enjambramiento" se ha ido consolidando de forma alarmante tras los atentados del 11-S, gracias, entre otros aspectos, a las ventajas de comunicación e interconexión que ofrece Internet.[7] Según Paul Eedle, "si el propio Bin Laden o el teórico egipcio de Al Qaeda, Ayman al-Zawahiri y sus colegas se encuentran en las montañas de la India o viviendo con sus barbas afeitadas en un suburbio de Karachi, ya no es relevante para la organización. Ellos pueden inspirar y guiar el movimiento global sin la necesidad de encontrarse con sus seguidores, sin ni siquiera saber quiénes son".[8]

---

3 El concepto de guerra en red (*netwar*), formulado por John Arquilla y David Ronfeldt en distintos estudios, como "The Advent of Network" (1996), hace referencia a un modo emergente de conflicto en el que los protagonistas utilizan la organización en red, estrategias y tecnologías con el fin de coordinar sus acciones sin un mando central concreto. Según estos autores, los protagonistas de esta guerra en red suman un conjunto de nodos diversos y dispersos que comparten un conjunto de ideas e intereses, preparados para actuar de un modo completamente interconectado a través de múltiples canales.

4 John Arquilla y David Ronfeldt, *op. cit.,* p. 38.

5 El "enjambramiento" es una manera aparentemente amorfa, pero deliberadamente estructurada, coordinada y estratégica de golpear a uno o varios puntos desde todos los frentes, mediante un pulso sostenido de fuego, tanto de cerca como de posiciones alejadas. El enjambramiento ocurre cuando pequeñas unidades dispersas de una red convergen sobre un blanco desde múltiples direcciones, en Arquilla y Ronfeldt, *op. cit*., pp. 42 y 43.

6 *Ibídem*.

7 Según Arquilla y Ronfeldt, existen informes donde se constata que las comunicaciones entre los miembros de Al Qaeda combinan elementos propios de una estructura axial (en la que los nodos se comunican con Bin Laden y sus más estrechos consejeros en Afganistán) y una estructura de rueda (en la que los nodos se comunican unos con otros sin referencia a Bin Laden).

8 Paul Eedle, "Terrorism.com", *The Guardian,* 17 de julio de 2002.

La "ciberplanificación"

Según Timothy L. Thomas, este es el poder y el peligro de la denominada "ciberplanificación" que aporta Internet a organizaciones terroristas como Al Qaeda.[9] La ciberplanificación "se refiere a la coordinación digital de un plan integrado que se extiende a lo largo de las fronteras y que puede resultar o no en una matanza. Puede incluir el ciberterrorismo como parte del plan conjunto". Por tanto, de acuerdo con esta interpretación, la ciberplanificación resulta al menos tan importante como el ciberterrorismo.[10] Se trata de una herramienta que permite a los grupos terroristas dirigir y controlar de forma eficaz y desde el anonimato todos los recursos y estrategias de la organización con el fin de coordinar e integrar las opciones de ataque y defensa.

La historia de la presencia de los grupos terroristas en el ciberespacio no ha hecho más que empezar, según Gabriel Weimann.[11] En 1998, sólo la mitad de las treinta organizaciones terroristas internacionales, de acuerdo con la ley antiterrorista estadounidense de 1996 (*US Antiterrorism and Effective Death Penalty Act*) —aprobada por el Gobierno de Clinton—, poseían un dominio en la red. En 2000, prácticamente todos los grupos han establecido su presencia en *Internet.* En 2004, de acuerdo con Weimann, ya se pueden contabilizar más de 4.000 *websites*, incluyendo las de tendencia *yihadista* —predominantes en la red—.[12]

La historia de la presencia de los grupos terroristas en el ciberespacio no ha hecho más que empezar

Sin embargo, y a pesar de la creciente presencia de las organizaciones terroristas en el ciberespacio, tal como denuncian Eedle, Thomas y el propio Weimann, la principal preocupación de políticos, académicos y periodistas se centra en el desafío que supone el ciberterrorismo, minusvalorando la importancia del estudio de los distintos usos que las organizaciones terroristas hacen de Internet, entre los que destacan la realización de campañas para la obtención de fondos, recluta-

---

9 Timothy L. Thomas, "Al Qaeda and the Internet: the Danger of Cyberplanning", artículo obtenido en los fondos de Foreign Military Studies Office Publications, Fort Leavenworth, KS. Este artículo fue previamente publicado en *Paramenters,* primavera de 2003.

10 El FBI define el ciberterror como "el uso ilegal de la fuerza o la violencia contra personas o propiedades con el fin de intimidar o coaccionar a los Gobiernos, la población civil o cualquier otro segmento en la consecución de objetivos políticos y sociales". Los objetivos pueden ser desde redes de oleoductos, pasando por ferrocarriles, autopistas, banca, telecomomunicaciones, sistemas de defensa, servicios de emergencia, hasta Internet. Para una aproximación a la temática relacionada con el ciberterrorismo ver: http://www.cybercrimes.net/Terrorism/overview/page1.htm1; http://www.isr.umd.edu/gemstone/infosec/ver2/papers/socialeng.htm1; http://www.online.securityfocus.com/iforuc/1638.

11 Gabriel Weimann es profesor de Comunicación en la Universidad de Haifa (Israel) y responsable de un proyecto sobre el uso que los grupos terroristas hacen de la red. Parte de los resultados de su investigación, que inició ya hace siete años, han sido publicados por United States Institute for Peace (USIP), http://www.usip.org. Gabriel Weiman, "How Modern Terrorism Uses the Internet", *United States Institute for Peace*, Special Report 116, marzo de 2004.

12 Conferencia pronunciada por Weimann en el Jewish Institute for National Security Affairs (JINSA) en agosto de 2004, en JINSA Online, http://www.jinsa.org/articles/print.html/documentid/2621.

miento, entrenamiento, guerra psicológica, a la vez que organización, planificación y movilización.

El ciberespacio se ha convertido en el entorno de operaciones ideal para las organizaciones que han sabido poner al servicio de sus intereses tácticos y estratégicos las innumerables ventajas que ofrece Internet. La red ofrece facilidad de acceso y mantenimiento, escasa regulación y control gubernamental, anonimato, facilidad y rapidez en el intercambio de información, entorno multimedia, acceso a la opinión pública internacional y facilidad para la planificación y coordinación de operaciones. Además, éstas resultan rentables tanto en términos de recursos invertidos como en términos de impacto internacional gracias a la fuerza multiplicadora de la red.[13] De esta manera, pueden determinar la agenda política de Gobiernos y medios de comunicación que, cada vez más, se basan y dependen de Internet como fuente de referencia.[14]

Teniendo en cuenta las posibilidades que ofrece la red, su tremendo potencial y los macabros objetivos de las organizaciones terroristas en general y de Al Qaeda en particular, resulta imprescindible dar mayor prioridad al estudio, análisis y seguimiento de los usos, contenidos y estrategias de planificación desplegados en Internet con el objetivo de comprender mejor el discurso político de estas organizaciones y contrarrestar, en la medida de lo posible, su capacidad de actuación y sus campañas de propaganda.

El "ciberterrorismo" tras el 11-S

Tras los atentados del 11-S, las agencias de seguridad estadounidenses entendieron la importancia y el tremendo poder de esta herramienta en manos de Al Qaeda por lo que comenzaron a desarrollar una campaña de vigilancia y control de todas las páginas web que pudieran contener elementos de ciberplanificación (información para activistas y simpatizantes, llamadas a la acción, direcciones de operativos). Los resultados son más que interesantes. Por ejemplo, alneda.com (alneda significa "la llamada" o "el llamamiento"), un sitio web identificado con Al Qaeda, se encontraba bajo los auspicios de una entidad llamada Islamic Studies and Research Center que funcionaba como un verdadero grupo de comunicación de la organización terrorista. Hasta que fue cerrado por las autoridades estadounidenses en el verano de 2002, el sitio era considerado el principal punto de salida y referencia de los mensajes "oficiales" proclamados por los dirigentes Bin Landen, al-Zawahiri y Abu Gaith. Desde alneda.com, Al Qaeda se atribuyó la responsabilidad de los atentados de Bali, Mombasa o contra el navío USS Cole, entre otros.[15]

---

13 Magnus Ranstorp, "Al Qaeda en el ciberespacio: desafíos del terrorismo en la era de la información", en Reinares, Fernando y Antonio Elorza, *El Nuevo Terrorismo Islamista: del 11S al 11M,* Ediciones Temas de Hoy, Madrid, 2004, p. 207.

14 Gabriel Weimann, "How Modern Terrorism... ", *op. cit.*, p. 3.

15 Información obtenida de la investigación elaborada por el Institute for Security Technology Studies (ISTS) en *Examining the Cyber Capabilities of Islamic Terrorist Groups*, Tecnical Analysis Group, Dartmouth College, marzo de 2004.

Según las autoridades estadounidenses, alneda.com era utilizada para transmitir mensajes secretos a los operativos de Al Qaeda repartidos por el mundo, bien a través de archivos encriptados, transmisiones esteganográficas o palabras clave difundidas mediante *chats* y videoconferencias. El sitio también fue usado para publicar toda una variedad de artículos, libros e incluso *fatwas* declarando la guerra a Occidente, a EEUU, al cristianismo o al judaísmo. Esta estrategia resultó de gran utilidad para cubrir las necesidades operativas tras la guerra en Afganistán en noviembre de 2001, cuando la organización fue desalojada de su base de operaciones. Con la mayoría de sus miembros dispersos en distintos países del mundo, *Internet* se convirtió en el punto de encuentro de operativos y simpatizantes que, a través de *e-mails, chatrooms* y páginas web pudieron seguir en contacto y coordinados, manteniendo la seguridad, la compartimentación y el anonimato en una eficaz y letal estrategia terrorista que Weimann califica como "guerra virtual con víctimas reales".[16]

Además de alneda.com, Al Qaeda también contaba con otros sitios importantes, como assam.com, que ha servido como un auténtico portavoz de la *yihad* en Afganistán, Chechenia y Palestina. La página qassam.net se encontraba vinculada a Al Qaeda y Hamas, según las autoridades estadounidenses. El sitio jihadunspun.net mostraba un video con discursos, rezos y amenazas de Osama Bin Laden, mientras que 7hj.7hj.com explicaba a los interesados técnicas de *hackactivismo* para infectar los sistemas de gobiernos y corporaciones con gusanos y virus informáticos. La página aloswa.org justificaba los atentados del 11-S y la guerra contra Occidente, de acuerdo con la interpretación de Bin Laden. En mwhoob.net y aljehad.online se podían escuchar canciones con un mensaje político y religioso, acompañadas de fotografías de musulmanes perseguidos por denunciar la política de EEUU y de los países árabes aliados, especialmente de Arabia Saudí. En otras como drasat.com**,** jehad.net**,** alsaha.com e islammemo.com se encontraron mensajes y proclamas de Al Qaeda incitando a la acción y aportando información sobre direcciones de operativos de la organización.[17]

La guerra psicológica en la web

Además de la ciberplanificación, Internet también ofrece una multiplicidad de usos y aplicaciones igualmente relevantes que amplifican las capacidades de las organizaciones terroristas. Estas van desde el reclutamiento y la movilización de voluntarios a operaciones de guerra psicológica.[18] Estas últimas revisten importancia ya

16 Gabriel Weimann, JINSA Online, *op. cit.*, p. 1.

17 Gabriel Weimann. "How Modern Terrorism Uses... ", *op. cit.*, pp. 10 y 11; Timothy L. Thomas, "Al Qaeda and the Internet: the Danger of Cyberplanning", *op. cit.*, p. 2; Marie-Hèlene Boccara, "Islamist Websites and Their Hosts", en http://www.memri.org/bin/articles.cgi?Area=jihad&ID=SR3104; también Habib Trabelsi, "Al Qaeda Wages Cyber War against US", *Middle East Times,* Dubai, 27 de junio de 2002.

18 Weimann identifica en su investigación ocho usos de *Internet* por parte de las organizaciones terroristas. Algunas aplicaciones coinciden con las de cualquier usuario

que el terrorismo es ante todo una guerra psicológica donde las víctimas no son sólo los heridos o los muertos de un atentado, sino también todos aquellos que han tenido noticia del acto terrorista y a los que se ha logrado infundir miedo o temor. Tal como afirma Fernando Reinares: "Hablar de terrorismo es hablar de violencia. Pero no de cualquier violencia. Ante todo podemos considerar terrorista a un acto de violencia cuando el impacto psíquico que provoca en una determinada sociedad o en un sector de la misma sobrepasa con creces sus consecuencias puramente materiales (…) Aunque se trate de una violencia cuyo alcance y magnitud sean menores que otras violencias posibles, quienes instigan o ejecutan el terrorismo pretenden, inoculando el temor, condicionar las actitudes y los comportamientos de la población (…)".[19]

Partiendo de la base de que el terrorismo puede entenderse como una forma de guerra psicológica, no es de extrañar que las organizaciones desplieguen sus campañas para infundir temor a través de Internet. Entre las diversas técnicas utilizadas están la difusión de horribles imágenes en las que se contempla la decapitación de prisioneros, la divulgación sistemática de mensajes amenazadores que aumentan la percepción de inseguridad, campañas orquestadas de desinformación con el objetivo de crear confusión o el ciberterrorismo, que busca infundir temor a sufrir las consecuencias de ataques terroristas a los sistemas de telecomunicaciones, aerolíneas, hospitales o control de tráfico. Internet ofrece a los grupos terroristas un modo alternativo y eficaz de llegar al público, al margen de las censuras gubernamentales, lo que les permite un mayor control de la percepción social de las audiencias.[20]

Internet ofrece a los grupos terroristas un modo alternativo y eficaz de llegar al público, lo que les permite un mayor control de la percepción social de las audiencias

Desde los atentados del 11-S, la estrategia se ha centrado en la divulgación de una sistemática campaña de amenazas contra los intereses de EEUU y de sus aliados. Estas advertencias, además, han recibido una cobertura considerable por parte de los medios de comunicación internacionales que han contribuido a amplificar la percepción de inseguridad y temor en las audiencias de todo el mundo, en particular las de EEUU y sus aliados. Estas son consideradas como "públicos enemigos" y se pretende estimular en ellas un debate que menoscabe el respaldo popular a los Gobiernos que apoyan la lucha contra el terrorismo liderada por el Gobierno de Bush.[21]

habitual de la web, como la obtención de información, y algunas se parecen al uso que realizan las organizaciones políticas como la obtención de fondos. Otras, sin embargo, son mucho más específicas y están relacionadas con las actividades terroristas como la divulgación de manuales para cometer atentados (Gabriel Weimann, "How Modern Terrorism...", *op. cit.,* p. 5). Una investigación realizada por el ISTS identifica cinco áreas de aplicación de Internet al servicio de los objetivos terroristas (ISTS Tecnical Group, "Examining the Cyber Capabilities").

19 Fernando Reinares, *Terrorismo Global,* Taurus, Madrid, 2003, p. 16.

20 Arquilla y Ronfeldt, "Redes...", *op. cit.*, p. 70.

21 Gabriel Weimann, "How Modern Terrorism...", *op. cit.*, p. 5.

La influencia sobre las opiniones públicas

Es difícil evaluar el verdadero impacto que está teniendo esta agresiva campaña psicológica sobre la opinión pública internacional. Sin embargo, los informes de opinión elaborados recientemente por dos prestigiosas instituciones como Pew Research Center for the People and the Press y Zogby International arrojan resultados reveladores que, cuando menos, deberían ser valorados con seriedad por parte de los gobiernos que lideran la lucha contra el terrorismo a la hora de diseñar y ejecutar una estrategia de comunicación adecuada para contrarrestar la campaña mediática de Al Qaeda.[22]

En lo que se refiere a la opinión pública estadounidense, el 51% de los demócratas y el 45% de los independientes consideran que la política exterior inadecuada de EEUU puede haber sido la causa de los atentados del 11-S, de acuerdo con el informe *Foreign Policy Attitudes Now Driven by 9/11 and Iraq*, elaborado por el Pew Research Center en agosto de 2004. Sin embargo, el 76% de los republicanos rechazan de forma categórica este supuesto, lo que demuestra la clara polarización partidista que vive la sociedad respecto a la política exterior y de seguridad. La división se hace también patente en lo relacionado con la visión de la posición del país en el mundo: mientras que el 80% de los demócratas y el 74% de los independientes consideran que en el momento actual EEUU es menos respetado en el mundo que en el pasado, sólo el 47% de los republicanos considera que el país ha perdido respeto en el contexto internacional.

En cuanto a los países del mundo árabe, ambos estudios demuestran la hostilidad de la opinión pública hacia EEUU. El informe elaborado por Zogby en junio de 2004 muestra que el 94% de los saudíes tienen una visión desfavorable de EEUU; en Jordania, aliado tradicional, el porcentaje se eleva al 78%; y en Egipto, el principal receptor de la ayuda económica y militar estadounidense en todo el mundo durante los últimos 20 años —al margen de Israel—, el porcentaje llega a un alarmante 98%. El informe *A Year After the Iraq War*, elaborado por el Pew Research Center en marzo de 2004, muestra la visión favorable que se tiene de Bin Laden en Pakistán (65%), Jordania (55%), Marruecos (45%) e incluso en Turquía, donde el 31% de la población considera que los ataques suicidas contra los intereses de EEUU y otros países occidentales son justificables. De hecho, la mayoría de la población en los cuatro países analizados coincide en expresar sus dudas sobre la sinceridad de la guerra contra el terrorismo, contemplada como un intento de controlar Oriente Próximo y dominar el mundo.

Por el momento, no hay forma científica de probar que la maquinaria de guerra psicológica de Al Qaeda ha producido estas actitudes. Pero lo que resulta incuestionable es que la visión apocalíptica y el discurso terrorista de Bin Laden, al-Zawahiri o Zarqawi son apoyados por la abrumadora mayoría de la población del

---

22 Los informes completos elaborados por el Pew Research Center pueden ser consultados en http://people-press.org/reports/display.php3?ReportID=222 y http://people-press.org/reports/display.php3?ReportID=206.
Los informes del Zogby International pueden encontrase, previo pago, en: www.zogbyworldwide.com/int/readnewswire.cfm?ID=685.

mundo árabe. Esta cuestión tendrá, sin duda, importantes repercusiones futuras en el conflicto que enfrenta a EEUU con Al Qaeda.

El informe elaborado para el Pentágono en septiembre de 2004 por el Task Force on Strategic Communications expone con claridad esta situación: "La campaña de información (...) es importante en cada esfuerzo de guerra. En esta guerra constituye un objetivo esencial puesto que las metas más ambiciosas de la estrategia de Estados Unidos dependen de la capacidad para separar la gran mayoría de los musulmanes no violentos de aquellos militantes radicales islamistas *yihadistas*. Pero los esfuerzos de Estados Unidos no sólo han fracasado a este respecto, sino que se ha conseguido el resultado opuesto a lo esperado".[23]

Tal como afirma Paul Eedle, para ganar los corazones de la población árabe no es necesario invertir las políticas estadounidenses. Después de todo, la política exterior de EEUU para Oriente Próximo defiende la creación de un Estado palestino y lucha por la consolidación de la democracia en Irak.[24] Lo que sí resulta imprescindible es prestar más atención al mensaje de Al Qaeda desplegado a través de su campaña mediática y pensar en nuevas y serias alternativas políticas, sociales y económicas —y no prioritariamente militares— para contrarrestar con hechos y no sólo con palabras la estrategia de comunicación de la organización terrorista que tan hábilmente explota ideas y sentimientos profundamente enraizados en la mentalidad del mundo árabe.

En tanto no se pongan en práctica nuevas alternativas políticas que lentamente comiencen a dar los resultados más o menos esperados en la guerra contra el terror, los cientos de miles de *yihadistas* dispersos por todo el mundo continuarán colaborando, coordinando, planificando y reforzando su identidad a través de la red con el claro objetivo de salir victoriosos de esta "cruzada". No es de extrañar que los escenarios más preocupantes, quizá en un futuro no muy lejano, se centren en la posibilidad de atentados con armas NBQ (nucleares, biológicas, químicas) o ataques ciberterroristas contra sistemas especialmente sensibles con el objetivo de causar la mayor conmoción posible a escala mundial.

---

23 Para consultar el informe, ver http://acq.osd.mil/dsb/reports/2004-09-Strategic_Communications.pdf. Citado en Paul Eedle, "Al Qaeda´s superweapon: the internet", *op. cit.,* p. 3.

24 Paul Eedle, "Al Qaeda´s superweapon: the internet", *op. cit.*, p. 3.