¿ES EL YIHADISMO UNA CIBER-AMENAZA?

Manuel R. Torres Soriano[1]

Versión *preprint*: TORRES SORIANO, Manuel R. "¿Es el yihadismo una ciber-amenaza?", *Revista de Occidente*, nº 406, marzo 2015, pp. 20-34.

INTRODUCCIÓN

A pesar de la ausencia de precedentes, existe la percepción generalizada de que es relativamente fácil utilizar Internet para provocar daños de carácter catastrófico utilizando cualquier objetivo conectado a la red, incluyendo las infraestructuras críticas que sustentan el modelo de organización económica y social de los países más desarrollados. De entre los múltiples actores a los cuales se les atribuye un claro interés por estos escenarios apocalípticos, destacan las organizaciones terroristas, debido a su inclinación por la espectacularidad y la búsqueda del pánico entre las poblaciones atacadas.

La débil barrera de entrada que aparentemente presenta el uso de las ciber-armas, así como la preferencia de estos grupos por el conflicto asimétrico, habría convertido el ciberespacio en el terreno en el cual los terroristas estarían llamados a desarrollar el grueso de sus actividades. Así, por ejemplo, en el inicio del nuevo milenio era habitual afirmar que el ciber-terrorismo no sólo era más barato y anónimo que los métodos tradicionales, sin que además ofrecía la posibilidad de alcanzar a un número mayor de objetivos que empleando la violencia física.

Sin embargo, buena parte de estos pronósticos están basados en una visión distorsionada sobre la naturaleza del ciberespacio y los requisitos necesarios para operar en él. Uno de los principales problemas para entender la verdadera magnitud de este fenómeno es la confusión existente sobre qué engloba el concepto de ciber-terrorismo. Ha sido habitual

[1] Profesor Titular de Ciencia Política en el Departamento de Derecho Público de la Universidad Pablo de Olavide de Sevilla. Es Investigador Asociado de la Universidad Autónoma de Chile, e Investigador Senior del Grupo de Estudios en Seguridad Internacional (GESI). Su último libro se titula: *Al Andalus 2.0. La ciber-yihad contra España* (Granada: GESI, 2014).

incluir en él, desde el *hacktivismo* (el activismo político a través del sabotaje o filtración de contenidos digitales) hasta el uso de internet para llevar a cabo las actividades habituales del terrorismo como la propaganda, la financiación, la obtención de información, o la comunicación privada entre sus miembros. Sin embargo, el ciber-terrorismo en sentido estricto sólo implica el uso del ciberespacio como un instrumento para provocar daños físicos a las personas u objetos, algo que resulta infinitamente más complejo que el resto de actividades a las que se cataloga de manera poco rigurosa con este término.

Los excesos a la hora de emplear este concepto han sido alimentados por las dramáticas declaraciones de algunos responsables políticos de alto nivel. El subsecretario de Defensa norteamericano William Lynn afirmaba en un congreso sobre ciber-seguridad celebrado en 2011: *"es posible para un grupo terrorista desarrollar un instrumento de ciber-ataque por sus propios medios o comprarlo en el mercado negro (…) Una docena de programadores talentosos vistiendo chanclas y bebiendo Red Bull pueden hacer mucho daño"*. Un año más tarde, el Secretario de Defensa estadounidense Leon Panetta no dudaba en emplear la expresión "ciber Pearl Harbour" para aludir a cuál sería el sentimiento de vulnerabilidad de sus compatriotas si algún grupo extremista consiguiese realizar un ataque cibernético capaz de *"descarrilar los trenes de pasajeros…contaminar el abastecimiento de agua de las grandes ciudades, y hacer caer la red eléctrica en grandes partes del país"*.

La convergencia entre terrorismo y ciberespacio también ha alcanzado un elevadísimo impacto en el ámbito académico. A mediados de 2014, podían contabilizarse treinta y un mil artículos sobre este tema en revistas científicas y profesionales, a pesar de que el número de personas heridas o muertas por este tipo de ataques era igual a cero.

¿Realmente está fundamentada la alarma sobre la amenaza proveniente del ciber-terrorismo? En este artículo mantengo la tesis de que los grupos terroristas, y de manera más específica, los de inspiración yihadista, a pesar de su indudable interés, no sólo carecen actualmente de capacidades para utilizar el ciberespacio como instrumento para llevar a cabo atentados, sino que es bastante improbable que en el futuro sean capaces de invertir esta situación.

INTERÉS VS. CAPACIDADES

Grupos terroristas como Al Qaeda y el llamado Estado Islámico, han demostrado sobradamente su destreza a la hora de emplear las nuevas tecnologías de la información como una herramienta para potenciar sus actividades tradicionales. Por extensión, se ha asumido como evidente que los yihadistas estarían preparándose para utilizar el ciberespacio como un territorio donde proyectar nuevos ataques contra sus enemigos.

En 2002, Abu Ubayd Al-Qurashi, uno de los colaboradores más cercanos de Osama Bin Laden, y autor de numerosos trabajos sobre cómo debería orientarse la estrategia del movimiento yihadista, no dudaba en amenazar a los Estados Unidos, con la "yihad en Internet", la cual se convertiría, según él, en una de las "pesadillas" a las que tendría que hacer frente el país en un futuro cercano.

La producción propagandística de Al Qaeda ha tratado de espolear las iniciativas individuales de sus partidarios en el ámbito cibernético. Un video de mediados de 2011 titulado "No confíes en otros, toma la responsabilidad por ti mismo" realizaba un llamamiento a que cualquier musulmán con estos conocimientos especializados llevase a cabo "*en armonía con el plan general de los muyahidín (…) ataques contra los websites y las redes electrónicas de las grandes empresas y las administraciones públicas de los países que atacan a musulmanes…*"

Los foros yihadistas de Internet han sido uno de los escenarios habituales donde los partidarios del terrorismo han dado rienda suelta a sus fantasías sobre la capacidad destructiva de las ciber-armas y contra qué objetivos deberían emplearse. Alguno de estos internautas llegó incluso a especular con la posibilidad de que un ciber-sabotaje contra Estados Unidos diese como resultado el lanzamiento remoto de alguna de sus armas nucleares contra China o Rusia, y que este fuese el inicio de una guerra que terminaría exterminando a los "enemigos del Islam". Sin embargo, estos proyectos, lejos de formar parte del planeamiento terrorista, han sido reflexiones en voz alta con la esperanza de que algún "hermano" con las habilidades necesarias se sintiese inspirado.

La revisión de la información disponible en fuentes abiertas evidencia como el número de incidentes de este tipo es escaso y de baja entidad. La mayoría son indicios de cómo algunos militantes estarían intentado formarse, o incluso experimentando con la realización de atentados a través de Internet. Uno de los ejemplos más citados es el de los archivos hallados por las tropas estadounidenses en Afganistán tras los atentados del 11 de septiembre de 2001. En los ordenadores incautados en una de las casas ocupadas por

operativos de Al Qaeda se encontró planos de presas, y *software* que simulaba los efectos de un fallo catastrófico de las mismas. Sin embargo, no hay constancia de que estos operativos supieran imprimir un sentido práctico a la información que habían recopilado.

La primera constancia sobre la ejecución de algo similar a un ciber-ataque por parte de un yihadista, se encuentra en la documentación del juicio en Estados Unidos contra el mauritano Mohamedou Ould Slahi. Este reclutador de Al Qaeda, con experiencia profesional como administrador de sistemas, tuvo conocimiento de cómo su grupo llevó a cabo una serie de ciber-ataques contra redes informáticas gubernamentales en el año 2001. Sin embargo, dichas operaciones se limitaron a sabotajes temporales de páginas webs públicas (como la del primer ministro israelí) a través de los llamados ataques de denegación de servicio, un tipo de acción que dista mucho de poder calificarse como ciber-terrorismo. De hecho este tipo de acciones no sólo no requiere ninguna sofisticación, sino que incluso puede ser llevada a cabo por aplicaciones automatizas de acceso abierto, fácilmente utilizables por cualquier internauta.

En los últimos años han hecho su aparición pública supuestos grupos formados por "hackers" de inspiración yihadista, cuyo propósito declarado era utilizar sus habilidades informáticas para llevar a cabo la "yihad electrónica". Estos grupos (generalmente de duración efímera), han sido los autores de algunos de los contenidos técnicos colgados en los foros yihadistas de internet, así como los responsables de administrar páginas webs donde se reflexionaba sobre cómo llevar a cabo la lucha contra sus enemigos a través del ciberespacio. Sin embargo, más allá de su discurso triunfalista sobre la capacidad de los *muyahidín* para degradar la economía occidental, la realidad es que el bagaje operativo de estos "grupos de expertos" se ha limitado a colgar en la red manuales y tutoriales fácilmente localizables por otras vías y con un escaso valor práctico.

El carácter de "universidad abierta de la yihad" que los radicales han pretendido otorgar a Internet, tiene más una finalidad propagandística y de motivación de sus seguidores, que de capacitación de futuros ciber-terroristas. La difusión indiscriminada de información técnica, es contradictoria con el hermetismo y el carácter sorpresivo que exige la implementación de un ciber-ataque exitoso. La difusión de este tipo de contenidos no hace sino desvelar los procedimientos y vulnerabilidades que serán explotadas, dando una oportunidad a sus potenciales víctimas para prevenir estas acciones hostiles.

Las "operaciones" de aquellos grupos de los cuales era esperable un mayor nivel de sofisticación se han limitado a simples ataques en fuerza contra algunas páginas webs escasamente protegidas. En ocasiones, sus sabotajes contra aquellos contenidos virtuales que consideran ofensivos desde una perspectiva islámica, se han implementado a través de procedimientos carentes de cualquier componente técnico, como, por ejemplo, la obtención de las contraseñas de las páginas atacadas a través de "ingeniería social", o incluso el envío de mensajes amenazantes a las empresas que prestan el servicios de alojamiento virtual, para forzarlas a descolgar estos contenidos del ciberespacio.

Uno de los temas habituales en las páginas yihadistas es la necesidad de que los *muyahidín* desconfíen de las herramientas y servicios más populares de Internet. Su origen occidental las habría convertido en armas en manos del enemigo. En este sentido, el logro técnico más destacado de estos grupos ha sido el desarrollo de aplicaciones informáticas propias destinadas a proteger el anonimato y la seguridad de las comunicaciones virtuales de sus partidarios. Sin embargo, esta iniciativa tampoco permite deducir la existencia de un nivel de sofisticación suficiente para llevar a cabo un ciberataque complejo. El desarrollo a partir de 2007 de las diferentes versiones del programa informático *Mujahideen Secrets*, no sólo no ha ofrecido ninguna novedad con respecto a programas existentes que realizaban la misma función, sino que se ha basado directamente en ellos. El producto informático yihadista más célebre, al igual que sus sucesores, no ha dejado de ser otra iniciativa propagandística para mejorar la autoestima de sus seguidores y transmitirles seguridad en un momento en el que aumentaba la desconfianza hacia el uso de las nuevas tecnologías.

LAS BARRERAS DEL CIBER-CONFLICTO

Las proyecciones más alarmistas sobre la viabilidad del ciber-terrorismo están basadas en el resultado de los ejercicios que algunas instituciones gubernamentales llevaron a cabo a finales de la década de los noventa, con la intención de evaluar la seguridad de sus sistemas informáticos. Uno de los experimentos más destacados fue llevado a cabo en 1998 por el Departamento de Defensa estadounidense bajo el nombre de *Eligible Receiver*. Esta simulación confirmó la vulnerabilidad de los sistemas informáticos de control y mando de la defensa, la infraestructura de comunicaciones y el abastecimiento eléctrico del país, cuyo sabotaje podía ser alcanzado por un actor no gubernamental

utilizando únicamente una conexión a internet, así como *software* y *hardware* fácilmente adquiribles en el mercado.

Sin embargo, estos resultados no son directamente trasladables a lo que podría conseguir una organización terrorista que se plantease el mismo objetivo. Difícilmente un actor no estatal obligado moverse en la clandestinidad, y que dedique gran parte de sus esfuerzos a la autoprotección de sus miembros, puede generar un "equipo rojo" como el que llevó a cabo este ataque simulado, el cual estaba compuesto por treinta y cinco de los mejores expertos de la Agencia de Seguridad Nacional (NSA), con capacidad para coordinarse y dedicarse en exclusiva a un objetivo común.

Movilizar a semejante masa crítica y ofrecerles un entorno seguro en el cual poder cooperar, no es la única dificultad a la que debería enfrentarse un grupo terrorista. Muchas de las vulnerabilidades que fueron detectadas y explotadas por este equipo son propias de un periodo donde aún persistían algunas brechas graves en el diseño de los sistemas e infraestructura que sustentan el ciberespacio. Ejercicios como *Elegible Receiver* y una mayor concienciación sobre la necesidad de adoptar una actitud de permanente actualización de los sistemas de información públicos y privados, ha creado un entorno mucho más exigente en cuanto a las capacidades y habilidades que debería desarrollar un actor con intenciones hostiles.

A pesar de las percepciones populares, el uso ofensivo del ciberespacio no es una actividad exenta de costes económicos. Otro ejercicio similar llevado a cabo en 2002 por el *U.S. Naval War College* denominado *Digital Pearl Harbor***,** llegaba a la conclusión de que la realización de un acto de ciber-terrorismo complejo requeriría de un presupuesto de 200 millones de dólares, así como un plazo de cinco años para poder implementarse.

Estas barreras de entrada no han hecho sino incrementarse con el paso de los años. Así, por ejemplo, cuando se utiliza el caso de troyano *Stuxnet* como ejemplo de la capacidad destructiva de un "simple" programa informático, suele pasarse por alto la verdadera entidad de este ciber-ataque. La destrucción de las centrifugadoras instaladas en algunas de las plantas nucleares iraníes requirió de un conocimiento profundo de los mecanismos que iban a ser atacados. El caso *Stuxnet* es obra de un equipo multidisciplinar que engloba a expertos de tareas tan diversas la física nuclear y la ingeniería de un componente

específico de los productos industriales comercializados por la marca Siemens, pero también de la obtención de inteligencia operativa, el reconocimiento de objetivos y la capacidad de insertar físicamente el programa dentro de una red de ordenadores que por seguridad permanecían aislados de Internet.

El troyano basaba su efectividad en el uso de al menos cuatro vulnerabilidades del "día cero", las cuales habían permanecido inéditas hasta el lanzamiento de este ciber-ataque. El uso simultáneo de varias brechas críticas de seguridad resulta especialmente exigente, teniendo en cuenta su escasez, así como la considerable cantidad de dinero que debe emplearse para adquirirlas en el mercado negro de *exploits*. El precio de estas vulnerabilidades puede oscilar considerablemente dependiendo de la popularidad del *software* afectado, y también de la gravedad del impacto que podría tener un uso malicioso de las mismas. Los *exploits* que apuntan a errores en el diseño interno del *hardware* (como fue el caso de *Stuxnet*), y que por tanto, no pueden ser rápidamente parcheados como sucede con los fallos de programación, pueden superar los varios millones de dólares la unidad. El presupuesto estimado para 2013 de la Agencia de Seguridad Nacional (NSA) para sumar a su ciber-arsenal este tipo de recursos, supero los 25 millones de dólares. Sin embargo, las capacidades del principal organismo estadounidense en el ámbito de la ciber-seguridad no dependen tanto de su poder adquisitivo, sino de sus propios medios para desarrollar y convertir en armas sus *exploits,* los cuales no son comercializados, ni compartidos con ningún otro actor.

La disponibilidad del conocimiento especializado es tan escasa en los grupos terroristas como en el resto de la sociedad. A pesar de las proclamas de la propaganda yihadista, la cual cifra en miles los partidarios que estudian informática para poner a disposición de la lucha estos conocimientos, la realidad es que sólo un número marginal de activistas han contado con una formación avanzada en informática o algún otro tipo de disciplina potencialmente útil para implementar un ciberataque complejo.

Frente a ello, NSA (por citar sólo uno de los organismos occidentales con atribuciones en ciberguerra) tiene en plantilla a más de mil de matemáticos, novecientos doctores en diferentes disciplinas científicas y técnicas, y cuatro mil informáticos, lo cual supone la mayor concentración mundial de este tipo de *expertise* en una única organización.

La disparidad de recursos humanos entre los grupos yihadistas y sus adversarios se ve agravada por el hecho de que la formación reglada es insuficiente para adquirir las

habilidades necesarias para implementar este tipo de operaciones. La transformación del ciberespacio en un nuevo dominio para el conflicto violento es resultado de un esfuerzo que se proyecta en el largo plazo, y que debe sostenerse en una estrategia agresiva de captación del talento. Se estima que *Olympic Games*, nombre con el que se bautizó el programa estadounidense de acciones encubiertas en el ciberespacio contra el programa nuclear iraní, empleó un presupuesto de 300 millones de dólares, y al menos tres años de trabajo hasta producir una ciber-arma operativa. Hablamos, por tanto, de una inversión en tiempo y dinero que no todos los actores pueden afrontar.

Sin embargo, la barrera más importante para que un grupo terrorista pudiese completar el proceso de desarrollo de una ciber-arma, es la posibilidad de experimentar reiteradamente con el *software* desarrollado, y evaluar su efectividad sobre objetivos reales. En el caso de *Stuxnet*, antes de su despliegue, había sido testado contra instalaciones nucleares experimentales situadas en Estados Unidos, las cuales habían sido dotadas de un equipamiento idéntico al existente en suelo iraní, y configuradas de manera exacta al objetivo atacado.

Las ciber-armas son productos creados específicamente para operar contra un objetivo concreto y bajo unas condiciones singulares que difícilmente pueden encontrarse en otras víctimas. La "liberación" de ciber-armas y el conocimiento de su código por parte de otros actores no suponen necesariamente un peligro de proliferación. Un grupo terrorista que se hiciese con una copia de este programa, se encontraría con que no puede ser utilizado contra ninguna otra instalación nuclear del planeta. Incluso aunque decidiese volver a emplearlo contra el objetivo para el cual fue creado, sería igualmente inútil, ya que las autoridades iraníes (así como las de otros países) se apresuraron a parchear las vulnerabilidades que habían hecho posible la efectividad del troyano. Si bien es cierto, que a través de ingeniería inversa puede obtenerse información útil sobre la arquitectura y la lógica de funcionamiento de este programas, se trata de un conocimiento que sólo tiene utilidad para inspirar las futuras innovaciones de aquellos actores que poseen los recursos humanos y materiales mencionadas anteriormente.

Las limitaciones técnicas y logísticas de los actores no estatales son tan evidentes, que es habitual que algunas previsiones sobre el ciber-terrorismo estén basadas en la cuestionable certeza de que los terroristas estén inmersos en una curva de aprendizaje que les llevará de manera inevitable a sortear todos estos problemas. Así, por ejemplo, Mike McConnell, antiguo Director de Inteligencia de los Estados Unidos, afirmaba: "*Los*

grupos terroristas de hoy día se sitúan en la parte inferior de la capacidad de ciberguerra (…), pero tarde o temprano lograrán la ciber-sofisticación. Es igual que la proliferación nuclear, sólo que más fácil."

Sin embargo, no hay ningún argumento que justifique que el mero paso del tiempo juegue a favor de las aspiraciones cibernéticas del yihadismo. Al igual que sucedió con el hipotético uso terrorista de armas químicas, bacteriológicas y nucleares, el cual a pesar de ser profetizado una y otra vez como un desenlace inminente, nunca llegó a materializarse, debido a la incapacidad de los terroristas para acceder a los recursos críticos y dominar la complejidad de este tipo de instrumentos. De manera similar, los yihadistas lejos de encontrarse en un proceso de sofisticación progresiva, pueden quedarse estancados de manera indefinida en las capas más superficiales del uso bélico del ciber-espacio.

Un escenario de colaboración en el ámbito cibernético entre el yihadismo y otro tipo de actores también plantea serias dudas sobre su viabilidad. Aunque es habitual que se especule con la posibilidad de que el terrorismo podría subcontratar estas capacidades en grupos de ciber-delincuencia, los cuales han demostrado una sofisticación técnica mayor, lo cierto es que estos últimos se enfrentan a las mismas dificultades logísticas y de capacitación. De hecho, parece poco probable que este tipo de organizaciones estuviesen dispuestas a abrir esa "línea de negocio" con las organizaciones terroristas. Aunque su motivación es el lucro económico, este tipo de grupos obtienen ganancias muy superiores a las que puede ofrecer el terrorismo, operando de manera transfronteriza a través de fraudes bancarios contra particulares, la extorsión, y el robo y venta de datos a través de Internet. El crimen organizado es consciente que la presión a la que se ven sometidos por parte de las agencias policiales es infinitamente menor que a la que tendrían que enfrentarse, si abandonan su "zona de confort" y deciden convertirse en colaborares de una organización terrorista.

La transferencia de un ciber-arma por parte de un Estado se enfrenta a problemas muy similares a los que han impedido la proliferación hacia grupos terroristas de armas de destrucción masiva. Existen pocos incentivos para que gobierno decida perder el control directo sobre uno de los bienes más preciados de sus arsenales y asuma el riesgo de transferirlo a un grupo que en última instancia pueden emplearlo contra su benefactor. La principal ventaja teórica podría ser su empleo contra un enemigo, permitiendo al Estado

eludir las represalias al mantener su capacidad de negación. Aunque el ámbito cibernético y el del armamento no convencional comparten la complejidad que supone establecer de manera fehaciente quien ha empleado esos recursos, esta atribución de autoría no es imposible, lo que resta atractivo a esta tipo de colaboración con grupos terroristas.

TEN CUIDADO CON LO QUE PIENSAS

A pesar de estos inhibidores, la obsesión sobre el riesgo que supone el ciber-terrorismo puede convertirse en una profecía parcialmente auto-cumplida. La reiteración del discurso sobre la facilidad con la que pueden provocar efectos catastróficos a través del ciberespacio, no hace sino incentivar el interés y la determinación de estos grupos para seguir experimentando. Aunque una mayor práctica no les permitirá sortear las importantes barreras que hemos comentado anteriormente, sí que les puede llevar a adquirir ciertas destrezas en otra serie de actuaciones con un elevado impacto mediático. Es el caso de la destrucción de datos, el robo de información privada o la suplantación de identidad a través del ciberespacio. Este tipo de acciones si están a su alcance, y a pesar de su baja sofisticación, si se emplean reiteradamente contra objetivos cargados de simbolismo, pueden proyectar a la opinión pública la percepción de que los terroristas dominan el ciberespacio y pueden hacer realidad sus amenazas más descabelladas.

No sería la primera vez que tiene lugar ese efecto paradójico en el ámbito del terrorismo yihadista. La misma inflación que actualmente sufre el discurso público sobre la viabilidad del ciber-terrorismo, fue experimentada a mediados de la década de los noventa con respecto al hipotético uso de armas no convencionales por parte del terrorismo. El presidente estadounidense Bill Clinton estaba convencido, según relata su asesor sobre terrorismo Richard Clarke, que "*había un cien por cien de posibilidades"* de que en la próxima década hubiese un ataque con armas químicas o biológicas en su país. Este alarmismo terminó despertando en Al Qaeda su interés por este tipo de sustancias. En una carta hallada en el Afganistán, Ayman Al Zawahiri, entonces número dos de la organización, reconocía que: "*sólo fuimos conscientes de estas armas cuando el enemigo dirigió nuestra atención hacia ellas, expresando repetidamente su preocupación por cómo podían ser fabricadas con materiales fácilmente accesibles"*. El resultado de este falta de prudencia a la hora de valorar este amenaza no convencional fue que Osama Bin Laden autorizó la puesta en marcha en una de sus bases afganas, de un primitivo e

infradotado programa de desarrollo de armas químicas. Aunque los resultados de esta iniciativa fueron muy pobres, la lección a aprender es que el grupo no se había planteado desviar ni un sólo recurso de su estrategia convencional, hasta que su enemigo se obstinó en señalarle las supuestas ventajas de esta vía alternativa de acción.

BIBLIOGRAFÍA

Bergen, Peter L., *The Longest War. The Enduring Conflict between America and Al-Qaeda* (Nueva York: Free Press, 2011).

Conway, Maura, "Reality Check: assessing the (un)likelihood of cyberterrorism", en Chen, Tom; Jarvis**,** Lee y Macdonald**,** Stuart (coord.), *Cyber Terrorism: Understanding, Assessment and Response* (Nueva York: Springer, 2014), 103-122.

Heffelfinger, Christopher, "The Risks Posed by Jihadist Hackers", *CTC Sentinel*, 7 (2013)

Kenney, Michael, "Cyber-Terrorism in a Post-Stuxnet World", *Orbis,* winter (2015): 111-128.

Singer, Peter W. y Friedman, Allan, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (New York: Oxford University Press, 2014)

Stalinsky, Steven y Sosnow R., "From Al-Qaeda to the Islamic State (ISIS), Jihadi Groups Engage in Cyber Jihad"*, MEMRI, Inquiry & Analysis Series,* 1136 (2014).

Torres, Manuel R., "Ciberguerra" en Jordán, Javier (coord.), *Manual de Estudios Estratégicos y Seguridad Internacional* (Madrid: Plaza & Valdés, 2013), 329-348.

Wagner, Abraham R., "Terrorism and the Internet: Use and Abuse" en Last, Mark y Kandel, Abraham (coord.), *Fighting Terror In Cyberspace* (Singapur: World Scientific Publishing, 2005).

Weimann, Gabriel, "Cyberterrorism: How Real Is the Threat?", *United States Institute of Peace Special Report*, 119 (2004).

Zetter, Kim, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon* (Nueva York: Crown, 2014)