LA LETALIDAD DEL CIBERTERRORISMO

Ignacio NIETO FERNÁNDEZ

Introducción

AS declaraciones de altos cargos de la Administración de los Estados Unidos sobre la posibilidad de un ciberataque con consecuencias similares a las de los atentados del 11-S (1) o de sufrir un *Cyber Pearl Harbor* (2) han convulsionado a la opinión pública. Los medios de comunicación ya se han encargado de divulgar, sin apenas rigor científico, la posibilidad de sufrir una agresión terrorista, auspiciada desde el ciberespacio, de dimensiones catastróficas.

Ríos de tinta agoreros se han escrito alineados con estas declaraciones desde hace ya bastante tiempo. Por ejemplo, el informe publicado hace más de 23 años de la Corporación RAND (3) sobre la inminente ciberguerra. El mundo lógico, que no se percibe como amenaza y apenas es comprendido por la gente de a pie, unido a la falta de información relacionada con estos asuntos, no permite rebatir estas afirmaciones.

Esta prolongada alerta apocalíptica ha terminado por anestesiar a la opinión pública occidental. Hasta

---

(1) Frase utilizada por NAPOLITANO, Janet: *US Homeland Security Secretary,* en enero de 2013. CHARLES, Deborah: «US homeland chief: cyber 9/11 could happen imminently». *Reuters*, 24 de enero de 2013.

(2) Palabras del secretario de Defensa de los Estados Unidos Leon Panetta en la revista *Cybersecurity to the Business Executives for National Security*, 11 de octubre de 2012. *http://archive.defense.gov/transcripts/transcript.aspx?transcriptid=5136*.

(3) La Corporación RAND (Research ANd Development) es un laboratorio de ideas (*think tank*) estadounidense. Tiene alrededor de 1.600 empleados distribuidos en seis sedes repartidas en Estados Unidos, Europa y Asia. El informe está disponible en *http://www.rand.org/-pubs/reprints/RP223.html*.

se llega a dar por segura la capacidad de grupos terroristas de perpetrar ataques contra países de consecuencias devastadoras, apuntando incluso a las infraestructuras críticas (en adelante IC) (4), por ejemplo a las nucleares y por supuesto a las marítimas. Como bien indica el periodista Joseph M. Sanmartí: «Esto conduce a referenciar exageraciones, recoger errores e incluso mentiras, sucumbir a manipulaciones de toda laya, sin riesgo a ser descubiertos por lo menos a corto plazo a causa de la oquedad de los temas tratados».

Cabe por lo tanto estudiar si las capacidades de los grupos terroristas son tan letales como algunos proclaman, o si tan solo entran dentro del campo de la posibilidad, del todo lejana, y no de una probabilidad real de materializarse.

Acotando el asunto

Si la definición de terrorismo no tiene una aceptación general, aún menos un término tan bisoño como el ciberterrorismo. Tendiendo a la simplificación se podría denominar como la convergencia del ciberespacio y del terrorismo que fue adoptada por el creador del término ciberterrorismo, Barry Collin.

Posteriormente sus teorías fueron rebatidas por Mark Pollit, un agente del FBI que proporcionó una definición más precisa: ciberterrorismo es el ataque premeditado y políticamente motivado contra información, sistemas computacionales, programas de computadoras y datos que puedan resultar en violencia contra objetivos no combatientes por parte de grupos subnacionales o agentes clandestinos. A efectos de este artículo, se abraza el concepto asociado de violencia para ser catalogado como ciberterrorismo, por lo que quedan excluidos aquellos ataques que no generen violencia. El término ciberataque también resulta complejo y depende de un número de variables muy extenso que entiendo se escapan del ámbito de este apartado. A afectos de simplificar, se denomina ciberataque a todo hecho malicioso que conlleve el uso del ciberespacio.

Los ciberataques pueden desarrollarse en el mundo físico, como puede ser la destrucción de un ordenador, o en el denominado lógico, por ejemplo insertando líneas de código, *botnet* (5) o programas maliciosos que permitan gobernar un determinado *software*, por ejemplo los desarrollados para los sistemas

(4) Según el apartado 2e) de la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas, son infraestructuras críticas «aquellas que proporcionan servicios esenciales y cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales».

(5) Microsoft define así *botnet*: «El término *bot* es el diminutivo de robot. Los delincuentes distribuyen *software* malintencionado (también conocido como *malware*) que puede convertir su equipo en un *bot* (también conocido como *zombi*)».

industriales, como los SCADA (6). Es importante destacar que el número de ciberataques perpetrados por organizaciones terroristas con daños significativos ha sido prácticamente nulo (7), o por lo menos sin trascendencia mediática. Sin embargo, a diario, España sufre ataques desde el ciberespacio y la tendencia es creciente, me atrevería a decir exponencialmente (8).

Esta tendencia no guarda relación con la posible letalidad de los mismos, como reconoce el Centro Criptológico Nacional en su informe ejecutivo sobre *Ciberamenazas y Tendencias 2017* (9), que no atribuye una capacidad letal al ciberterrorismo: «El terrorismo yihadista emplea la dimensión del ciberespacio para tareas que no implican la comisión directa de un atentado, sino labores de adoctrinamiento, reclutamiento y logística».

Sin embargo, la percepción de inseguridad es elevada. Hay que destacar el informe de evaluación de infraestructuras críticas elaborado por la empresa McAfee (10), donde expone que el 48 por 100 de los representantes de organizaciones que cuentan con infraestructura crítica afirmaron que en un período de tres años es muy probable que un ataque de este tipo pueda dañar las instalaciones e incluso causar la pérdida de vidas humanas.

Nuestra *Estrategia de Seguridad Nacional* reconoce la importancia del espacio marítimo para el comercio mundial, de gran importancia para España como potencia marítima. Entre otros aspectos, las rutas marítimas son vitales para las transacciones comerciales y el transporte. En la *Estrategia de Seguridad Nacional de 2017*, dentro de las líneas de acción estratégicas de la Seguridad Marítima, se encuentra «mejorar la ciberseguridad en el ámbito marítimo».

Los Estados Unidos plasmaron en 2015 estas inquietudes en una *Estrategia Ciber para la Guardia Costera,* donde se reconoce la vulnerabilidad de las infraestructuras críticas marítimas a los ataques desde el ciberespacio. Asimismo, la reciente *Estrategia de Seguridad Nacional de los Estados Unidos* otorga importancia a un potencial ataque a las infraestructuras críticas, donde las marítimas son esenciales: *Cyberattacks offer adversaries low-cost and de-*

---

(6) Es el acrónimo de *Supervisory Control And Data Adquisition*, en español Supervisión, Control y Adquisición de Datos, que es un *software* para ordenadores que permite el control y la supervisión de procesos industriales a distancia.

(7) Incluso ampliando el abanico de ataques, del estudio de los recientes ataques cibernéticos se desprende que incluso aquellos que han resultado más exitosos han sido benignos para la integridad del ser humano, sin generar violencia contra el ser humano, tal y como expresa el periodista Kaspersky.

(8) Así lo reconoce Miguel Ángel Abad, jefe del Servicio de Ciberseguridad del CNPIC en la entrevista otorgada a la revista *Cuadernos de Seguridad,* donde reconoce los siguientes ataques a las IC: 17 (2013), 63 (2014), 134 (2015) y, en el primer semestre del 2016, 231.

(9) Centro Criptológico Nacional. Informe *Ciberamenazas y Tendencias 2017*. *https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/2221-ccn-cert-ia-16-17-ciberamenzas-y-tendencias-edicion-2017-resumen-ejecutivo-1/file.html*.

(10) *http://www.mcafee.com/us/resources/reports/rp-aspen-holding-line-cyberthreats.pdf*, p. 5.

niable opportunities to seriously damage or disrupt critical infrastructure, cripple American businesses, weaken our Federal networks, and attack the tools and devices that Americans use every day to communicate and conduct business.

Casos históricos de posible aplicación

Cabe estudiar, desde el prisma de la historia, aquellas agresiones exitosas desde el ciberespacio hacia las IC para poder inferir qué tipo de ciberataques son más factibles y poder contrastarlos con las capacidades de los grupos terroristas, de manera que nos permitan determinar si existen posibilidades reales de conducir un ataque de estas características.

Los ciberataques, en el ámbito nacional, se producen con frecuencia, incluyendo las IC, aunque es cierto que, aun siendo exitosos, apenas infringen daños (11). Aunque es verdad que la historia nos deja significativos ejemplos de vulnerabilidades, el caso de mayor trascendencia fue el ataque a Irán con el *Stuxnet* (12) o el de la central nuclear de Ignalina (13). También es destacable el incidente producido en la central nuclear americana de Davis-Basse, detallado por la revista *Security Focus* (14), que dejó la planta con importantes averías durante más de ocho horas.

Stuxnet fue sin duda el gusano informático que abrió los ojos al mundo sobre la capacidad de realizar ciberataques en una planta nuclear y ha sido incluso catalogado como la primera ciberarma. Demostró la necesidad de tener sistemas informáticos aislados sin posibilidad de insertar memorias USB; a partir de este momento, la no interconexión de redes (privadas y públicas) no es un garante de no poder recibir un ataque. Estudios posteriores determinaron la enorme complejidad en el desarrollo de esta ciberarma, que estaba tan solo al alcance de los países más desarrollados, y algunos autores apuntan claramente a Estados Unidos y a Israel como colaboradores. Su complejidad en el desarrollo fue de tal dimensión que ese mismo embrión ha sido la cepa para el desarrollo posterior de otros troyanos. Sin embargo, los efectos del ciberataque no fueron del todo positivos: es verdad que retrasó el

---

(11) La revista *Ciber Elcano,* en su número 7, afirma que en un período de 48 meses, comenzando en 2010 y finalizando en octubre de 2014, se registraron más de 1.300 ciberataques sobre infraestructuras críticas energéticas estadounidenses, siendo 159 de ellos exitosos.

(12) El gusano *Stuxnet* es ampliamente explicado en el libro de SINGER, P.W.: *Ciberseguridad y Ciberguerra*.

(13) Un técnico de la central nuclear Ignalina, en Lituania, introdujo un virus en un ordenador que controlaba los sistemas auxiliares de la central. Al parecer, el objetivo del trabajador no era sabotear el funcionamiento de la central, sino demostrar la existencia de una vulnerabilidad en los sistemas de control (CORRALES, 2007, p. 32).

(14) Disponible en *http://www.securityfocus.com/news/6767*.

programa nuclear iraní durante más de dos años, pero a la vez hizo que percibiera claramente sus vulnerabilidades y decidiera emprender una carrera en la mejora de su ciberseguridad, que le ha convertido en un país líder en este sentido y, por lo tanto, poco susceptible de recibir este tipo de ataques.

Los ciberataques

En general existen dos caminos para perpetrar un ciberataque y el más sofisticado es desarrollar una ciberarma, algo similar al *Stuxnet*. También pueden perpetrarlo de forma combinada entre lo lógico y lo físico. Ambos demandan acceder a información sensible sobre la IC, el ciberespionaje. El Centro Criptológico Nacional, en su informe *Ciberamenazas y Tendencias 2017,* lo clasifica como la amenaza más importante para la Seguridad Nacional.

Aunque el desarrollo de una ciberarma por parte de un grupo terrorista está muy cuestionado (como se verá en el apartado siguiente), existen otros factores que pudieran facilitar la adquisición de una ciberarma. Especialmente si consideramos la incertidumbre que se ciñe sobre la evolución de internet.

En primer lugar, el *software* malicioso está creciendo exponencialmente y se encuentra disponible en internet, de adquisición gratuita o razonablemente económica. En segundo lugar, porque existe un incremento en la dependencia de *software* comercial, el tan manido *Commercial off-the-shelf*, COTS, que siempre representa una vulnerabilidad fácil de explotar. En tercer lugar, los estados están desarrollando ciberarmas, algunos de ellos pudieran trasferir este tipo de tecnología (por ejemplo Irán o Corea del Norte) a un grupo terrorista. Aunque es cierto que las represalias de la comunidad internacional serían contundentes, no se puede descartar que, al amparo del anonimato que ofrece internet, se pueda producir esa transferencia. Tampoco es descartable que algunos de los desarrolladores de las aplicaciones se conviertan en adeptos al grupo terrorista y terminen por compartir este tipo de tecnología.

Además, factores como la globalización, la ausencia de fronteras o la legislación garantista de los países occidentales también favorecen el delito en el mundo cibernético. Hay que considerar que nos encontramos en un campo de batalla con diferentes reglas de juego. Por una parte, el sistema de gobernanza del mundo lógico apenas dispone de herramientas de eficacia integral y la disuasión apenas tiene efecto alguno. Por otra, las normas legales se basan en criterios territoriales que son manifiestamente ineficaces en el entorno virtual; además, determinar la localización del ataque o demostrar la complicidad del estado es harto complicado. Básicamente, internet fue creado para ser útil y sencillo, no para ser seguro. Si este panorama lo asociamos a que los terroristas operan en la internet profunda, por ejemplo la

red TOR (15), cuyo tamaño se estima 500 veces superior a la internet superficial, con un nivel de anonimato muy elevado, se antoja complicado de articular, bajo el amparo de las reglas de la comunidad internacional, una respuesta contundente. Aunque desde mi perspectiva, caso de producirse, sería un solo estado el que lideraría la acción de forma unilateral.

Estas circunstancias hacen que en el presente quizás los terroristas no puedan desarrollar ni obtener una ciberarma que pueda resultar efectiva contra una IC (que actualmente solo está en manos de los estados más desarrollados tecnológicamente), pero sí disponer de una capacidad de sabotear algunas capacidades de la instalación nuclear que les permita generar terror sobre la población civil, pues es una de sus finalidades. El futuro, sin embargo, se torna complicado y dependerá de la evolución de internet, aunque inicialmente todo apunta a que el tiempo juega a su favor.

La cuestión es que los terroristas tienen formas más sencillas de perpetrar un ataque cibernético. Por ejemplo, de la mano de un infiltrado podrían introducir un gusano informático en el sistema de control de la infraestructura crítica. Esta posibilidad se antoja como la más sencilla, aunque de consecuencias imprevisibles, pues depende del tipo de planta. En los Estados Unidos, un reciente informe del Department of Homeland Security advierte de que en ningún caso tendría consecuencias devastadoras, principalmente porque el reactor tiene redundancia en su apagado y las lecturas de los indicadores también son redundantes. Una alteración del sistema de control de la infraestructura en ningún caso podría derivar en un suceso trágico.

La opción de combinar una acción cibernética con otra física es realmente la más factible, no es compleja tecnológicamente y desde luego el impacto mediático sería muy importante. No en vano la amenaza de sabotaje, en la que está encuadrado el ciberterrorismo, es la más preocupante, siendo incluida en uno de los cinco planes de la Cumbre de Washington, en concreto el referente a la Iniciativa Global Contra el Terrorismo Nuclear (IGTN).

Hay que considerar que en el entorno de internet existen multitud de virus que permiten extraer información de un ordenador particular. La falta de cultura de seguridad de muchos ingenieros y altos directivos hace que el acceso a esta información sea factible. En este sentido, es probable que los ataques tipo *ransomware* se incrementen, exigiendo dinero los atacantes a los usuarios/empresas que hayan perdido información (activo muy valioso en las empresas).

---

(15) TOR (*The Onion Router*) es un proyecto diseñado e implementado por la Marina de los Estados Unidos, posteriormente patrocinado por la EFF (Electronic Frontier Foundation, un organismo en defensa de los derechos digitales). Actualmente subsiste como TOR Project, una institución sin ánimo de lucro galardonada en 2011 por la Free Software Foundation por permitir que millones de personas en el mundo tengan libertad de acceso y expresión en internet manteniendo su privacidad y anonimato.

Existen otros virus, como el *Duqu* (evolución del *Stuxnet*, pero con diferente propósito), que fueron utilizados en un laboratorio de investigación de la Universidad de Tecnología y Economía de Budapest. Su propósito (16) era obtener información de infraestructuras críticas para perpetrar un posterior ataque.

Hay que recordar que en noviembre de 2012, el grupo Anonymous proclamó haber hackeado la página de la IAEA (International Atomic Energy Agency) y haber obtenido sensibles datos del programa nuclear israelí. Tampoco podemos olvidar el incidente de la operadora surcoreana y el robo de manuales de centrales nucleares.

Los límites del ciberconflicto

Es comprensible pensar que es sencillo perpetrar un ataque efectivo desde el ciberespacio, en especial a tenor de declaraciones como la del subsecretario de Defensa William Lynn (17), que llegó a afirmar en un congreso sobre ciberseguridad que «es posible para un grupo terrorista desarrollar un instrumento de ciberataque 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».

La verdad es que la realidad nos lleva a pensar de forma diferente, pues no se producen ataques realmente nocivos de grupos terroristas desde el ciberespacio. A nadie se le escapa que si tuvieran esa capacidad, la ejecutarían; de esto no creo que quepa duda alguna. Por ello resulta razonable pensar que no disponen de esa capacidad y que el ciberconflicto de alta intensidad tiene límites. Desde luego, no parece estar en manos de informáticos en un garaje bebiendo líquidos isotónicos.

Existen barreras, de diversa índole, que inhiben el desarrollo de una ciberarma por parte de organizaciones terroristas. En primer lugar, lejos de lo que se piensa, la evolución de esta ciberarma demanda un importante recurso económico. Valga como ejemplo el ejercicio realizado en el US Naval College, denominado *Digital Pearl Harbor,* que arrojó la conclusión de que un acto de ciberterrorismo requeriría un presupuesto de 200 millones de dólares y cinco años de trabajo de laboratorio. Ni que decir tiene que el desarrollo de gusanos como el *Stuxnet* demanda el trabajo de un equipo multidisciplinar que englobe físicos, ingenieros, informáticos y otros muchos y largos años de trabajo que

---

(16) Información extraída del informe de la compañía Symantec sobre el virus *Duqu*. W32. *https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepa.pers/w32_duqu_the_precursor_to_the_next_stuxnet.pdf*.

(17) *http://armedforcesjournal.com/the-cyber-terror-bogeyman/*.

han de ser sufragados. Pero sin lugar a dudas, la barrera inhibidora más importante es el nivel tecnológico necesario para poder desarrollar una ciberarma con capacidad de atacar con efectividad una infraestructura crítica.

Volviendo al *Stuxnet* hay que indicar que fue desarrollado al amparo de la Operación OLYMPIC GAMES, una campaña de sabotaje dirigida contra las plantas nucleares de Irán, que contó con la colaboración del Servicio Secreto israelí, en especial con su capacidad de Inteligencia de Señales (18). El presupuesto general fue de 300 millones de dólares, abarcando otros gusanos como el *Flame* y al menos tres años de trabajo.

Esta complejidad nos lleva a pensar que es realmente difícil que un grupo terrorista logre desarrollar una ciberarma de estas características, e incluso que al hacerlo se encontraría con la dificultad de tener que experimentar para poder verificar su fiabilidad y mejorar su capacidad de ataque. Todo ello bajo un entorno hostil, donde no se dispone de libertad de acción física ni digital, como es el que tienen los terroristas. Aun disponiendo del código fuente del *Stuxnet* u otro similar, su lanzamiento sobre otra infraestructura crítica es del todo inútil, pues en este ámbito cada gusano lleva la impronta de su víctima y es inútil para el resto de infraestructuras críticas (19).

En resumen, disponer de una ciberarma con capacidad de causar daños importantes o provocar la muerte de seres humanos se antoja realmente complejo por parte de los grupos terroristas. El futuro, desde luego, será diferente, y la participación de los estados, tanto en el desarrollo y comercialización como en el control de las mismas, es un asunto vital pero a la vez muy complejo de predecir.

Hipótesis más probable

Descartada la opción de que los grupos terroristas dispongan de una ciberarma, lo más probable es que intenten dar publicidad a un ataque exitoso sobre algunos de los sistemas de la central nuclear que generara una sensación de inseguridad y de pánico ante lo mediático de las vulnerabilidades de las infraestructuras críticas.

---

(18) La Inteligencia de Señales ofrece información muy valiosa en el nivel estratégico y superior, pues tiene capacidad de obtener datos de comunicaciones de las más altas autoridades de un determinado país. Es uno de los activos de las naciones más importante y encubierto. Quizás *Stuxnet* fue una de las primeras ocasiones en las que se produjeron colaboraciones entre países en este entorno, pues normalmente residen en el exclusivo ámbito nacional.

(19) De hecho, los ordenadores que se calcula que han sido infectados por el *Stuxnet* hasta verano de 2010 fueron más de 100.000. Su principal víctima fue Irán, pero los sistemas informáticos de otros países también lo fueron. (*Symantec report on stuxnet*, pp. 6-8. *https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.).*

La segunda alternativa es que los terroristas dispongan de apoyo interno, bien de un infiltrado o de una persona extorsionada, que les permita introducir un *malware* en los sistemas de control. Lo más peligroso sería realizar una acción combinada mediante la que entrarían en la IC después de inhabilitar algunos de los servicios de control, como las cámaras de seguridad. Todo ello con apoyo de espionaje para obtener información y poder realizar este tipo de ataques.

Ciberataque a las infraestructuras críticas: ¿realidad o ficción?

Sin lugar a dudas, en el ámbito de un grupo terrorista, actualmente es ficción. Aunque el futuro es ciertamente impredecible, básicamente no es posible porque no disponen de la tecnología suficiente para ello. Por otra parte, existen opciones más sencillas para dañar a una IC marítima o nuclear, por ejemplo un ataque con un avión de pequeña entidad o mediante el lanzamiento de artefactos explosivos.

Incluso si en un futuro dispusieran de una ciberarma poderosa capaz dejar inoperativo un sistema determinado y sus redundantes, es muy discutible que tuviera efectos devastadores sobre el sistema global y que no lograra detenerse con autoprotecciones.

Sin embargo, cada día es más frecuente la alarma sobre la amenaza que supone el ciberterrorismo, sin que hasta la fecha se haya vislumbrado su letalidad real. Esta sensación de desprotección alienta a la inversión pública en ciberseguridad, en la que los Estados sí representan una amenaza real y tienen poderosas capacidades de ataque sobre las infraestructuras críticas, cosa que espero no llegar a ver jamás.

El empleo más probable en el futuro será el relacionado con la capacidad de influir en audiencias concretas: población de un país, grupos sociales determinados... Se ha visto claramente la potencialidad de su empleo combinado con los métodos tradicionales de combate, como ha realizado Rusia en Ucrania (conflicto híbrido) o en procesos electorales como el americano. La reciente controversia de *Facebook* y el posible impacto en las elecciones de los Estados Unidos sobre las filtraciones de millones de datos de los usuarios son un buen ejemplo de ello.

Como conclusión y a pesar de la narrativa de algunos países, los actores más probables y peligrosos que realizarán ciberataques serán los estados y no tanto los grupos terroristas.

BIBLIOGRÁFIA

AGUIRRE ROMERO, J. M. (2004): «Ciberespacio y comunicación: nuevas formas de vertebración social en el siglo XXI». Espéculo. *Revista de estudios literarios,* núm. 27. *http://www.ucm.es/info/especulo/numero27/cibercom.html*.

BAYLON, C.; BRUNT, R.; LIVINGSTONE, D. (2015): *Cyber Security at Civil Nuclear Facilities Understanding the Risks. Chatham House Report. https://www.chathamhouse.org/sites/files/chathamhouse/field/field_document/20151005CyberSecurityNuclearBaylonBruntLivingstoneExecSumUpdate.pdf*.

BERRY, Ken (2007): «Preventing Nuclear Terrorism». *Center for Security Studies ETH Zurich. http://www.ewi.info/pdf/TerrorNukesFeb7.pdf*.

BUN, M.; MALIN, M.; ROTH, N.; TOBEY, W. (2016): *Preventing Nuclear Terrorism. Continuous Improvement or Dangerous Decline? Belfer Center. http://belfercenter.ksg.harvard.edu/files/PreventingNuclear Terrorism-Web.pdf*.

CARO BEJARANO, M. (2001): «La protección de las Infraestructuras Críticas». Instituto Español de Estudios Estratégicos. Documento de análisis 021/2011. *http://www.ieee.es/Galerias/fichero/docs_analisis/2011/DIEEEA21_2011ProteccionInfraestructurasCriticas.pdf*.

—(2013a): *La nueva dimensión de la amenaza global: la amenaza cibernética*. Instituto Español de Estudios Estratégicos. Documento de análisis 40/13. *http://www.ieee.es/Ga-lerias/fichero/docs_analisis/2013/DIEEEA40-2013_AmenazaCibernetica_MJC.pdf*.

—(2013b): *Los potenciadores del riesgo*. Instituto Español de Estudios Estratégicos. Cuaderno de Estrategia núm 159.

FALLIERE, N. O.; MURCHU, L.; CHIEN, E. (2011): *W32. Stuxnet dossier. California: Symantec security Studies. https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf*.

FUTTER, A. (2016): *Nuclear weapons in the cyber age: New challenges for security, Strategy and stability. Valdai Papers #56. http://valdaiclub.com/a/valdai-papers/valdai-paper-56-nuclear-weapons-in-the-cyber-age-n/*.

GARRIDO REBOLLEDO, V. (2016): «Terrorismo Nuclear: ¿mito o realidad?». *Revista Política Exterior,* 27 abril. *http://www.politicaexterior.com/actualidad/terrorismo-nuclear-mito-o-realidad/*.

—(2013): «Terrorismo Nuclear. ¿Nuevo desafío a la seguridad?». *Política Exterior,* núm. 148, julio-agosto de 2012, pp. 82-92.

KASPERSKY, E. (2012, 11 de diciembre): *Ciberespeluznante: amenazas en la Red,* p. 1. Esglobal.

MIRANZO, M.; DEL RÍO, C. (2014): *La protección de infraestructuras críticas. UNISCI Discussion Papers*, núm. 35 (mayo/mayo 2014).

POLLITT, M. (1999): *Cyberterrorism, Fact or fancy? FBI Laboratory. https://es.scribd.com/document/21173253/Mark-M-Pollitt-Cyber-Terrorism-Fact-or-Fancy*.

REILLY, S. (2015, 11 de septiembre): *Record: energy department struck by cyberattacks. USA Today. http://www.usatoday.com/story/news/2015/09/09/cyber-attacks-doe-energy/71929786/*.

SÁNCHEZ GÓMEZ MERELO, M (2011, 06 de julio): *Infraestructuras Críticas y Ciberseguridad. https://manuelsanchez.com/2011/07/06/infraestructuras-criticas-y-ciberseguridad/*.

SANMARTÍ, J. (2013): «Las ciberguerras, un tema en ascenso en el periodismo internacional». *adComunica. Revista de Estrategias, Tendencias e Innovación en Comunicación*, 2013, núm. 6, pp. 103-114. *https://dialnet.unirioja.es/servlet/articulo?codigo=4663611*.

SINGER, P.; FRIEDMAN, A. (2014): *Cibersecurity and Cyberwar: what everyone needs to know*. Nueva York: Oxford University Press. *https://news.asis.io/sites/default/files/Cybersecurity_and_Cyberwar.pdf*.

SERVITIJA ROCA, J. (2013): *Ciberseguridad, contrainteligencia y operaciones encubiertas en el programa nuclear de irán: de la neutralización selectiva de objetivos al «cuerpo ciber» iraní*. Instituto Español de Estudios Estratégicos. Documento de opinión 42-2013. *http://www.ieee.es/Galerias/fichero/docs_opinion/2013/DIEEEO42-2013_Inteligencia_Iran_XSertvija.pdf*.

TORRES, M. (2015): «¿Es el yihadismo una ciberamenaza?». *Revista de Occidente*, núm. 406, marzo 2015, pp. 20-34.

Washington Post (2012, 2 de junio). *Stuxnet was work of US and Israeli experts, officials say,* p. 1. *https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html?utm_term=.86226d104be2*.