CIBERATAQUE A INFRAESTRUCTURAS CRÍTICAS. ¿REALIDAD O FICCIÓN?

Carlos GARAU PÉREZ-CRESPO

O vemos en las películas y en ocasiones la prensa flirtea con el tema; terroristas, ejércitos o agencias de inteligencia atacan instalaciones de una potencia o ente hostil mediante un ciberataque a un reactor nuclear, una planta depuradora de agua o una instalación energética. En estos hipotéticos supuestos se producen consecuencias muy graves, incluso fatales y en ocasiones puede que alcancen proporciones semejantes a las que producirían armas de destrucción masiva.

Imaginemos un ciberataque al sistema financiero mundial o a uno de sus principales focos. Quizá de alguna manera los efectos de la reciente crisis financiera nos proporcionan una buena imagen de algunas posibles consecuencias. Un caso más claro y de efectos más inmediatos es un fallo de suministro eléctrico generalizado en todo el país. La vida moderna sin electricidad durante periodos prolongados no es nada fácil. Las casas y los alimentos no pueden mantener la temperatura, las gasolineras no pueden alimentar las bombas de servicio, las comunicaciones se degradan rápidamente y los altercados en la calle puede que aumenten con rapidez. Este escenario se puede extender a muchos servicios proporcionados por otras infraestructuras; ¿qué ocurriría en una ciudad sin agua potable durante un mes?, ¿y sin la distribución de alimentos?, ¿cómo afectaría al país un fallo masivo del control del tráfico aéreo?

Antes de entrar de lleno en los argumentos para juzgar el nivel de ciberamenaza a las infraestructuras críticas (en adelante IICC) hay que poner en común el significado de este término. Para ello emplearé la definición de

infraestructura según el NIPC (1) (Centro Nacional de Protección de Infraestructura de Estados Unidos): «Aquellos sistemas físicos o cibernéticos esenciales para el mantenimiento vital de la economía y el gobierno, incluyendo telecomunicaciones, energía, banca y finanzas, transporte, sistemas de agua potable y sistemas de emergencias, tanto públicos como privados».

Los factores que debemos considerar para saber si esta amenaza es actual o inminente, solo una posibilidad teórica o algo simplemente imposible son varios:

— El grado de mentalización y preparación de los gestores de infraestructuras críticas a la amenaza cibernética y el grado de seguridad implantado en sus sistemas informáticos. En resumen, el grado de vulnerabilidad de las infraestructuras.
— La capacidad técnica de *hacktivistas* (2), terroristas, naciones o *lobbies* hostiles para realizar un ataque con éxito a infraestructuras críticas.
— El grado de eficacia y seguridad y la relación entre coste/beneficio que ofrece el ataque cibernético frente a un ataque convencional.
— Conocer si hay datos que avalen que, de hecho, ya ha habido algún ataque planeado y ejecutado con éxito contra alguna infraestructura crítica.

La preocupación existe; de hecho muchos países, entre ellos España, disponen ya de un Centro Nacional de Protección de Infraestructura Crítica (CNPIC) dedicado a defenderse de cualquier tipo de ataque, y específicamente a enfrentarse a los retos de la amenaza cibernética.

Sistemas SCADA (3) y otras vulnerabilidades de las infraestructuras

El foco de atención en la amenaza a IICC es el empleo generalizado de los sistemas SCADA (Control de Supervisión y Adquisición de Datos). Este tipo de sistemas controla un gran número de infraestructuras y es cada vez más empleado. Son el interfaz entre la instalación, sus sensores y actuadores analógicos y el mundo digital.

Los sistemas SCADA se emplean para medir y controlar otros sistemas, y por tanto no crean solamente efectos en el mundo «virtual», sino también en el físico. Con frecuencia estos sistemas están conectados a Internet de una u otra forma para transmitir datos e instrucciones de control en lugar de emplear

(1) *National Infrastructure Protection Center*, Estados Unidos.
(2) *Hackers* activistas que tienen motivación de tipo patriótico o de cualquier otro tipo; por ejemplo, ecologista.
(3) *Supervisory Control and Data Acquisition*.

sus propias redes, como era el caso antes del *boom* de las nuevas tecnologías. Si se accede a estos sistemas, se puede tomar control efectivo de la instalación. Una de las vulnerabilidades más evidentes es la del ataque cibernético por un exempleado resentido.

Muy pocos elementos digitales de las infraestructuras críticas fueron diseñados o instalados con la seguridad como elemento prioritario o siquiera fue esta considerada en absoluto. Gran parte de la infraestructura se instaló hace muchos años, antes de la existencia del control por ordenador o, cuando menos, antes de que la seguridad de las redes informáticas fuera un asunto serio. La mayoría de los sistemas SCADA están plagados de vulnerabilidades (4). Muchos de los sistemas de control están basados en sistemas operativos estándar de Windows o Linux y, en palabras de los *hackers*, se tardaría tan solo una semana en conseguir acceso a la mayoría de ellos.

Según algunas fuentes (5), el 17 por 100 de fallos en los sistemas SCADA se debe al acceso directo al sistema desde Internet. Otras posibilidades de conexión son a través de redes privadas virtuales (VPN) (6) o módem. A pesar de que el acceso remoto no es recomendable por motivos de seguridad, la necesidad de reducir costes y la posibilidad de control remoto y centralizado de varios sistemas SCADA/instalaciones llevó a muchas compañías a establecer esta arquitectura de comunicaciones. En una encuesta realizada en 1997, se descubrió que el 40 por 100 de las instalaciones de agua permitían a sus operadores el acceso directo a Internet y el 60 por 100 de los sistemas SCADA podían ser conectados vía módem.

La mayoría de expertos coincide en que los peores escenarios solo son posibles por la falta de protección adecuada. En un estudio (7), las administraciones de Estados Unidos fueron auditadas para comprobar su adherencia a una norma de 2002 sobre medidas de seguridad en tecnologías de la información. La nota media global fue «D +» (8). Lo peor es que el Department of Homeland Security (Ministerio de Interior), responsable de ciberseguridad, obtuvo una calificación de «F» (9).

No es el sector público el único al que culpar. Más del 80 por 100 de las infraestructuras críticas pertenecen a entidades privadas. Muchas de ellas

---

(4) GOODMAN S. E.: «Fuentes informales», en *Critical Information Infrastructure Protection*. IOS Press, International Affairs and Computing. Georgia Institute of Technology. Atlanta, USA, 2008.

(5) BRUNST, P. W.: *Use of the Internet by Terrorists. A Threat Analysis*. IOS Press, Responses to Cyber Terrorism, Centre of Excellence Defence Against Terrorism, Ankara, Turkey, 2008.

(6) *Virtual Private Networks*. Son redes lógicas cifradas; forman «túneles» privados en redes físicas menos restringidas o abiertas.

(7) BRUNST, P. W.: *op. cit.*

(8) Nota escolar equivalente en España a un «5 raspado».

(9) Nota escolar equivalente en España a «4» o inferior.

tampoco disponen de una mínima seguridad informática. Es cierto que en muchos casos, cuando la seguridad no fue parte del diseño inicial de los SCADA, existen dificultades para implementarla:

— Los elementos de seguridad a veces no son compatibles con el espacio, el requerimiento de aplicación en tiempo real o las necesidades de alimentación eléctrica y respaldo. La implementación de seguridad puede reducir las prestaciones y provocar problemas de sincronización con otros procesos de nivel superior.
— Muchos de estos sistemas pertenecen al sector mixto o privado y los propietarios y/o gestores pueden no tener recursos disponibles suficientes para realizar la inversión requerida en seguridad.

Las consecuencias potenciales de una combinación de sistemas SCADA conectados a Internet pudieron verse en 2003 cuando 21 plantas de la red de distribución eléctrica y otras instituciones críticas del nordeste de Estados Unidos sufrieron un apagón. Hasta donde alcanza el conocimiento de dominio público estos fallos se debieron al gusano W32.Lovsan. Este código malicioso empleaba el mismo puerto para aprovecharse de una vulnerabilidad en ordenadores personales que el que usaban las plantas eléctricas para comunicarse entre sí. La colisión en el protocolo de comunicaciones resultó en un gran apagón en Estados Unidos y este de Canadá, que afectó a 60 millones de hogares.

Un ejemplo de la vulnerabilidad de algunas ICC, incluyendo las de tipo más peligroso, es el ocurrido en Arizona en 1998: un niño de 12 años fue capaz de entrar en el sistema informático que controlaba una presa de hidráulica. Autoridades federales luego informaron (10) que el joven tuvo control absoluto del sistema SCADA que manejaba las compuertas de inundación. Imaginemos si este acceso hubiera sido logrado por terroristas en una gran presa. La historia nos proporciona una aterradora imagen de las posibles consecuencias: en 1975 las presas de Bangiao y Shimantan, pertenecientes al sistema fluvial del río Huang He (río Amarillo), fallaron y provocaron inmensas inundaciones; el caudal destruyó 64 presas más pequeñas río abajo, causando la muerte de al menos 85.000 personas.

Las vulnerabilidades de las IICC y la naturaleza discreta de la amenaza cibernética hacen que en ocasiones ni siquiera se haya advertido el ataque. Más adelante se explicará un caso real de ataque a una planta depuradora en el que tras 40 accesos al sistema SCADA para verter agua sucia ni uno solo de

(10) BRUNST, P. W.: *op. cit*. Parece que los detalles del ataque están en disputa. Mientras que *The Washington Post* dice que el niño de 12 años accedió al sistema en 1998, otras fuentes argumentan que tenía 27 años y accedió en 1994. También hay dudas sobre el nivel de control de la presa que consiguió.

ellos fue detectado. Una vulnerabilidad significativa existe también en las infraestructuras críticas de información (CII) (11) por la propia disposición y despliegue de sus redes «troncales». El ataque a una o dos de estas conexiones podría tener un impacto global en Internet (12). En el pasado, daños accidentales a cables han producido efectos; en una ocasión un cable subterráneo entre China y Estados Unidos sufrió daños y se informó de que el 97 por 100 de los usuarios de China tuvieron problemas para acceder a *webs* extranjeras y el 57 por 100 dijo que su vida y trabajo habían sido afectados por los daños. Otro de los enfoques convencionales de ataque a CII sería contra los llamados *peering points* (en adelante «interconexión») que conectan diferentes redes en Internet. La interconexión alemana DE-CIX de Frankfurt maneja el 80 por 100 del tráfico de Alemania, y el 35 por 100 del europeo (13). El LINX (London Internet Exchange) es la interconexión más grande del mundo y en 2006 fue un objetivo de un ataque frustrado a tiempo por Scotland Yard.

El empleo de sistemas que emplean circuitos integrados digitales para el control de IICC conlleva otra vulnerabilidad más que se expondrá muy brevemente por ser una amenaza no estrictamente cibernética. El empleo de dispositivos no nucleares, portables o vehiculares, incluso de fabricación «casera» (14) tipo EMP/IEMI (15) (Pulso Electromagnético/Interferencia Electromagnética Intencionada) contra IICC puede tener consecuencias drásticas al dejar la instalación inoperativa, producir daños irreparables (pérdida de datos) e impedir cualquier análisis forense digital (circuitos quemados). Se estima que las armas EMP serían efectivas contra toda instalación, y son muchas, que no disponga de protección específica contra este tipo de dispositivos.

¿Existe la capacidad técnica de ataque a infraestructuras?

En 2001 se publicó (16) que el Departamento de Defensa de Estados Unidos (en adelante DoD) (17) realizó en 1997 una prueba real denominada *Eligible Receiver*. Treinta y cinco miembros de la NSA (18) (Agencia Nacio-

---

(11) *Critical Information Infrastructure*.

(12) BRUNST, P. W.: *op. cit*.

(13) Ídem.

(14) «La tecnología para crear armas de radiofrecuencia está siendo cada vez más accesible y disponible a través de cursos en universidades y conferencias públicas. Además, los dispositivos, incluyendo las partes y los planos de construcción, están disponibles en Internet». *Computer Security Update*, septiembre 2009. Vol.10, n.º 9, Worldwide Videotex, *www.wvpubs.com*.

(15) *Electro Magnetic Pulse/Intentional Electro Magnetic Interference*.

(16) Según *Strategic Cyber Security*, de Geers K., James Adams lo publicó en 2001 en la revista *Foreign Affairs*.

(17) Department of Defence.

(18) National Security Agency.

nal de Seguridad de Estados Unidos), simulando *hackers* norcoreanos, emplearon una variedad de herramienta y técnicas de ciberguerra, incluyendo la transmisión de órdenes y notas de prensa, para atacar el US Navy Pacific Command desde el ciberespacio. El equipo de *hackers* tuvo un éxito rotundo. La estructura humana de Mando y Control se paralizó por completo debido a la desconfianza, y nadie, ni el presidente, podía creerse nada de lo que circulaba por los sistemas del centro de mando.

En un informe (19) de 2010 del Center for Strategic and International Studies (CSIS) y McAfee Inc. sobre una encuesta a más de 600 ejecutivos de seguridad e IT de IICC en 14 países, en la que se inquiría por: las prácticas, actitudes y políticas de seguridad, su relación con el Gobierno, medidas específicas de seguridad empleadas en sus redes y los tipos de ataque a los que hacen frente; se obtuvieron respuestas que indicaban la ejecución de ataques continuos a las IICC por adversarios con elevada capacidad tecnológica. Datos de 2008 indicaban ya una pérdida por tiempo *off-line* de infraestructura crítica de Estados Unidos debido a ciberataques de más de seis millones de dólares diarios, y la frecuencia y coste de estos estaba en aumento. A pesar de que la mayoría piensa que gobiernos extranjeros están involucrados en los ataques, no hay manera segura de saberlo, aunque es cierto que la mayoría de datos que se rastrean acaban en direcciones IP en China.

No parece por tanto nada descabellado pensar que al menos las naciones más desarrolladas tecnológicamente tienen capacidades (armas) cibernéticas que serían capaces de atacar sistemas SCADA, incluyendo la propia infraestructura de Internet.

¿Compensa el ataque cibernético?

No parece probable que, pese a la posibilidad y capacidad técnica de realizar un ataque a través del ciberespacio se elija esta vía, sí es más fiable y/o barato realizar un ataque convencional, salvo que:

— Exista voluntad de ocultar el mismo hecho del ataque, la identidad del atacante o se quiera inculpar a un tercero.
— Se busque un efecto psicológico y/o mediático mayor que el que produciría un ataque más «convencional».

En el caso de terroristas, estos pueden estar poco convencidos de probar métodos nuevos mientras funcionen los viejos, más aún cuando los nuevos

(19) TALBOT JENSEN, E.: «Cyber Warfare and Precautions Against the Effects of Attacks».

requieren considerable conocimiento y habilidad. Es posible que prefieran mantener los métodos que conocen bien y funcionan. Novedad y sofisticación puede ser mucho menos importante que eficacia. Por eso el coche-bomba es una amenaza mucho mayor que la bomba lógica, por ahora. La principal ventaja del medio cibernético para los terroristas sería la inmensa cobertura e interés mediático que es previsible que genere este tipo de ataque.

Para otros casos, no el terrorista, el ciberataque no solo compensa, sino que forma en sí una nueva oportunidad de operaciones, principalmente desde el poder e intereses del Estado, con objetivos que las armas físicas no pueden alcanzar o en las que tienen serias desventajas. Es el caso por ejemplo de operaciones de inteligencia que requieran discreción o de las que deban evitar daños colaterales.

Historia de ataques a IICC

Como ya se habló al principio de este texto, un factor evidente para discernir la realidad de la amenaza es conocer si de hecho ya se han producido ataques. Hay pocos casos de dominio público de ataques a IICC, pero los hay. De forma poco sorprendente parece que son poderes estatales los que han demostrado esta capacidad en operaciones que podrían denominarse militares (caso Stuxnet, detallado más adelante). No hay casos conocidos de ataques terroristas, pero sí los hay de ataques criminales y posibles ataques por *hacktivistas* patrióticos.

La historia de sabotajes a IICC por medios no físicos comienza en 1982, cuando la CIA (20) logra hacer explotar un gaseoducto siberiano ruso empleando una «bomba lógica». Desde entonces se conocen unos pocos casos que creo que resultan interesantes:

Ataque individual a un aeropuerto en 1997

En 1997 un joven fue capaz de entrar en los sistemas de comunicaciones del aeropuerto de Worcester, Massachusetts (Estados Unidos). La acción interrumpió el servicio telefónico de la torre de administración de la aviación federal del aeropuerto, el departamento de bomberos del mismo y otros servicios relacionados, como seguridad, meteorología y varias compañías privadas de transporte aéreo. El circuito que habilitaba a las aeronaves a mandar señales de activación de las luces de la pista al aproximarse fueron deshabilitadas. Por suerte, el ataque no produjo accidentes.

(20) Central Intelligence Agency.

Ataque individual a una planta depuradora de agua en Australia en 2000

Los empleados resentidos, comprados o infiltrados, son la principal vulnerabilidad de IICC con sistemas SCADA conectados a Internet. Vitek Boden era un informático resentido y con sed de venganza, exempleado de una planta depuradora de la costa este de Australia. Boden conectó su ordenador a un transceptor inalámbrico, y desde su coche, durante dos meses y en total en 46 ocasiones, accedió al sistema de tratamiento de agua de la ciudad. Dio órdenes al sistema, con éxito, para que vertiera 1.100.000 litros de aguas negras a ríos, parques y zonas públicas. La policía lo descubrió, por suerte, al parar el coche y observar que tenía una pila de equipamiento informático en los asientos.

Ataques a redes de distribución eléctrica. Brasil 2005 y 2007

Un analista de la CIA en 2008 reveló algunos datos que en su momento resultaron muy inquietantes. Ante un auditorio formado por un numeroso grupo de funcionarios, ingenieros y gestores de seguridad de varios países relacionados con las industrias eléctricas, de agua, petróleo y gas y otras IICC de Estados Unidos, reconoció la existencia de ciberintrusiones frecuentes en IICC de Estados Unidos con motivo de realizar extorsiones. También informó de ataques que, vía Internet y con origen y motivo desconocido, tuvieron como objetivo plantas energéticas de otras regiones del mundo, donde lograron interrumpir el suministro eléctrico de varias ciudades. En mayo de 2009 el presidente de Estados Unidos, Barack Obama, anunció que se conocían ciberataques que en el pasado habían conseguido dejar ciudades enteras en la oscuridad.

Todo indica que estas informaciones se refieren a los apagones de 2005 y 2007 en Brasil, que dejaron sin electricidad a millones de ciudadanos, sin que aún se conozca el origen del ataque.

Ataques «militares» en 2007 y 2010

Existe información no confirmada de que en 2007 Israel inutilizó la defensa aérea siria por medio de un ciberataque antes de atacar con su aviación un reactor nuclear sirio.

Todo apunta a que se puede atribuir a Israel o a Estados Unidos la creación de la pieza de código malicioso más admirada por los expertos: el gusano Stuxnet. Por medio de este *malware* (21) en 2010 se destruyeron

(21) Denominación genérica del código informático malicioso que engloba todo tipo de productos lógicos: virus, gusanos, troyanos, bombas lógicas, *root-kits*, *phising*, etcétera.

infraestructuras del programa nuclear iraní. Se consiguió con un gusano lo que no pudieron cinco años de resoluciones de Consejo de Seguridad de las Naciones Unidas (CSNU): interrumpir el esfuerzo iraní de obtención de la capacidad militar nuclear. De confirmarse esta acción, un código de medio MB (22) habría sido más efectivo que un ataque militar y habría evitado una posible crisis internacional surgida de los probables daños colaterales.

El gusano Stuxnet atacó los sistemas SCADA de las infraestructuras iraníes. La estrategia de propagación usada por Stuxnet es un misterio. Se sabe que empleó al menos cuatro vulnerabilidades *zero-day* (23) y dos certificados digitales robados. Este es capaz de atacar redes *air-gapped* (24) mediantes memorias USB y un diseño tan refinado e inteligente que intenta el acceso al control de la infraestructura solo cuando detecta que está conectado en un entorno SCADA.

Un escenario «cercano»

Todo lo escrito no deja de parecer algo lejano a nuestro ámbito. Algunos se preguntarán si este tema tiene interés o aplicación como amenaza a un buque o fuerza naval. La mayor parte de la tecnología a bordo de los buques de guerra de hoy es COTS (25), especialmente las redes informáticas, incluidas las del sistema de combate del buque. No es en absoluto descartable que un atacante logre introducir un código malicioso en el sistema de combate de un barco, o de una clase completa, con impacto en su capacidad operativa de Mando y Control y de empleo de sus sensores y armas.

Si un buque de guerra debe o no ser considerado como una infraestructura crítica es discutible, pero a los efectos del siguiente escenario lo consideraremos como tal. El propósito del escenario planteado en forma de hipótesis es observar la analogía de este con los ataques a sistemas SCADA de IICC «convencionales», de los que alguno ya sabemos que ha tenido lugar.

---

(22) Un Megabyte = 1.024 KB = 1024*1024 bytes.

(23) Vulnerabilidad de «Día Cero» son las codiciadas por todo cibercriminal, aquellas que no se conocen, no se han hecho públicas y por tanto para las que no existen parches de seguridad ni pueden ser detectadas por *software* de seguridad.

(24) Sin conexión física a Internet o al medio atacante. La intromisión en el sistema requiere de la introducción, consciente o no, de un dispositivo físico con código dañino.

(25) *Commercial Off the Shelf*. Procedencia comercial, no es tecnología específica militar.

Situación inicial

Las fragatas clase *Álvaro de Bazán*, como el resto de buques de la Armada de reciente construcción, cuentan con un extraordinario —y envidiado por muchas marinas— Sistema Integrado de Control de Plataforma (SICP). Este funciona como un avanzado SCADA, integrando miles de sensores y muchos actuadores que permiten el control total de la plataforma, incluyendo propulsión, gobierno y generación eléctrica desde múltiples puestos del barco, además de ordenadores portátiles. Los elementos de control, consolas, servidores, etc., están conectados por una red ATM (26) en principio «independiente» del resto de redes informáticas del barco. Imaginemos que en su arquitectura de redes uno de los nodos ATM está a su vez conectado por Ethernet (27) a la red LAN-PG (28) del barco, y que esta conexión existe para el envío automático de datos de monitorización y mantenimiento de los sistemas de a bordo a los órganos del Apoyo a la Fuerza. El barco está siempre conectado a la WAN-PG (29): en puerto normalmente por fibra óptica y en la mar vía satélite. La WAN-PG es una red SINCLAS (30), formada por miles de ordenadores y usuarios civiles y militares de todos los empleos y que no requieren de acreditación de seguridad. Por supuesto la WAN-PG y los nodos de conexión a los terminales móviles vía satélite disponen de seguridades (*firewall, router*, sistemas de detección de intrusos, etc.) que vigila el COSDEF (Centro de Operaciones de Seguridad del MINISDEF).

Amenaza

Si una agencia o poder militar hostil planeara y preparara *con tiempo y recursos* acceder al sistema SICP de una fragata en la mar para dejar el barco sin propulsión ni corriente, o provocarle una avería catastrófica atacando uno de los miles terminales de la WAN-PG (físicamente o vía Extranet) y desde allí la LAN-PG del buque y el SICP, ¿lo conseguiría?

---

(26) *Asynchronous Transfer Mode*. Es un protocolo de enlace de datos alternativo a Ethernet o RDSI.

(27) Protocolo de enlace de datos casi universalmente empleado en segmentos físicos de redes LAN.

(28) LAN (*Local Area Network*) de propósito general. Es la red local del buque conectada a la WAN-PG.

(29) WAN (*Wide Area Network*). Intranet de propósito general de Defensa.

(30) De clasificación de seguridad SINCLAS; significa SIN CLASIFICAR; no requiere de medidas de protección ni de acreditaciones de seguridad de sistemas ni personal para su empleo.

La conexión de la red ATM a la LAN-PG del buque solo sería necesaria si se quiere realizar el ataque «en tiempo real». Si el SICP no está conectado a la LAN-PG (SICP *air gapped*), el ataque tampoco puede descartarse. De forma semejante a lo ocurrido con el gusano *Stuxnet*, se podría introducir el código en el SICP por medio de memorias USB (31). Una vez introducido, el atacante podría haber elegido todo tipo de situaciones (por ejemplo, sonda, velocidad, etc.) para hacer actuar al gusano y provocar los daños que busca.

Conclusiones

Desde la opinión pública y los medios de comunicación, incluyendo películas, se proyecta el miedo de que terroristas puedan infligir enormes daños a Occidente por medio de ciberataques a sus IICC. Hay opiniones (32) en sentido de que no debemos dar por directamente trasladables la existencia de vulnerabilidades en ordenadores a las IICC. Otros (33) nos recuerdan que debe distinguirse entre *hacking* y ciberterrorismo, y que no hacerlo es un error que provoca la exageración de la amenaza, que deriva en la formulación de falsas analogías (por ejemplo, si esto lo puede hacer un niño de 16 años, ¿qué podría hacer un grupo terrorista bien financiado?).

Al contrario de lo que ocurre con la permanente presencia de acciones de *hacking* y cibercrimen en general, no prestamos atención al hecho de la práctica carencia de sucesos de ciberterrorismo. Es probable que al menos por un tiempo los terroristas sigan prefiriendo los ataques convencionales porque la probabilidad de daños físicos reales es mucho mayor. Un hecho que apoyaría este argumento es que el apagón masivo del nordeste de Estados Unidos de 2003, que los medios inicialmente atribuyeron a un ciberataque, no degradó las capacidades militares de Estados Unidos ni dañó la economía ni causó bajas ni terror en la población.

---

(31) La introducción del código dañino podría hacerse de forma consciente (colaboración de alguien de dentro; barco u órganos de apoyo) o inconsciente. En más de una ocasión se han dejado memorias USB cerca de instalaciones con código dañino oculto, de los que los trabajadores de la instalación se apropian e introducen en sus redes. Este método fue probado por una compañía de seguridad que preparó 20 memorias USB y las dejó en las instalaciones de un banco. De ellas, 15 fueron encontradas y conectadas a la red del banco, lo que permitió que el *malware* se extendiera, recopilara contraseñas e información de cuentas y las enviara a los auditores de seguridad. Este método fue también el empleado en los ataques al Departamento de Defensa de EE. UU. en 2008.

(32) GEERS, K.: en *Strategic Cyber Security* cita a James Lewis, del Center for Strategic and International Studies. Junio 2011, CCD COE, Tallin, Estonia.

(33) STOHL, M. cita a Weimann en *Cyber terrorism: a clear and present danger, the sum of all fears, breaking point or patriot games?*, 20 de marzo de 2007, Internet.

Sin embargo no dejemos que los argumentos anteriores, razonamientos que minoran pero no anulan la amenaza ciberterrorista a IICC, nos hagan bajar la guardia. De lo que no cabe ninguna duda es de la amenaza real, que sí supone la capacidad de poderes del ámbito militar y de inteligencia de otras naciones y organizaciones estatales para producir sabotajes u otro tipo de acciones con motivaciones diversas.

¿Realidad o ficción...? Prepárese para lo peor y espere lo mejor.

BIBLIOGRAFÍA

CHARVAT, M. J.: *Cyber Terrorism: A New Dimension in Battlespace*, 2009, Centre of Excellence Defence Against Terrorism, Ankara, Turkey.

GEERS, K.: *Cyber Weapons Convention,* 2010, NCIS, CCD COE, Tallin, Estonia.

GEWIRTZ D.: *How Critical Infrastructure is at Risk of a Cyber Attack*, 2010, Journal of Counterterrorism & Homeland Security International, Vol.15, No.2, International

Association for Counterterrorism & Security Professionals (IACSP). *www.thejournalofcounterterrorism.org*