EL *TWITTER* DE SUN TZU

Carlos GARAU PÉREZ-CRESPO

S día 11 de septiembre de 2021, cerca de Las Vegas (Estados Unidos), la presa Hoover, de 230 m de altura, abre las compuertas y deja pasar 685.000 m^3/seg. de agua, destruyendo dos presas menores caudal abajo e inundando la zona del condado de Riverside, lo que ocasiona la muerte a más de 2.000 personas. Mientras, de forma aproximadamente simultánea, ocurren los siguientes hechos en distintas partes del globo:

— En Madrid los servicios de urgencia de la mayoría de hospitales se han saturado tras recibir miles de pacientes con síntomas de intoxicación causada por lo que parece un envenenamiento del suministro del agua.
— En Leeds, en dos accidentes prácticamente simultáneos, se estrellan dos *Boeing 747* con resultado de un gran número de pérdidas de vidas humanas.
— En varias zonas de Noruega se suceden fallos graves de la red de suministro eléctrico, dejando sin energía a todo el norte del país, provocando numerosos problemas de abastecimiento en infraestructuras críticas y activando todos los servicios de emergencia del país para evitar muertes por congelación.
— En Washington D. C. fallecen 53 personas mayores; entre ellas el presidente de la Reserva Federal. Todos tenían colocado un mismo modelo de marcapasos instalado en el mismo hospital.
— En Francia se suceden altercados graves en las calles de varias ciudades, con decenas de muertos y centenares de heridos, debido a las protestas de la comunidad islámica ante la publicación de varias opiniones y artículos de contenido laicista radical en varias *webs* y *blogs* del Gobierno.
— Las bolsas mundiales caen en picado, el Dow Jones pierde un 11 por 100 de media tras los hechos anteriores, sumados a la previsión catas-

trófica de crecimiento y paro en Estados Unidos, supuestamente hecha por varios economistas de prestigio en las redes sociales y en varios de los *blogs* financieros más reconocidos.

Todo lo anterior es pura fantasía, no responde a ningún estudio serio sobre posibles amenazas ni es probable que una serie de hechos de tanto impacto, tan distintos y separados geográficamente, puedan planearse y ejecutarse de forma coordinada. Sin embargo, esta introducción debiera servir para despertar al lector de las posibles amenazas, armas y efectos a los que hoy en día se enfrentan Estados, organizaciones, empresas y particulares en la guerra, o suma prácticamente infinita de batallas y conflictos que se libran en el ciberespacio 24 horas al día, todos los días del año. Individualmente, todos los hechos imaginarios relatados, o al menos muy similares, no pueden descartarse como posibles logros de diferentes tipos de ciberataques. Algunos, de hecho, han ocurrido prácticamente tal cual se han relatado.

Pensemos por un momento en el sector bancario. No nos constan ataques directos de *hackers* a bancos llevándose dinero de sus arcas. ¿Realmente los bancos gozan de suficiente ciberseguridad como parece inferirse de la ausencia de noticias en sentido contrario? El exdirector de Inteligencia Nacional de Estados Unidos, almirante Michael McConnell, dijo (1) en 2010 que existía una «conspiración» de secreto en torno a la escala de los riesgos cibernéticos. Según esta opinión ninguna compañía de tarjetas de crédito dirá la frecuencia o la facilidad con la que es engañada. Ningún banco dirá cuán cerca ha estado de que le roben electrónicamente. Como resultado de esta «conspiración», las leyes, normas, conceptos o hábitos que podrían hacer Internet más segura no se discuten.

La seguridad informática ha evolucionado en 20 años de una disciplina técnica a un concepto estratégico. La amenaza percibida es tal que el US Cyber Command ha declarado el ciberespacio como el quinto dominio de la guerra —tierra, mar, aire, espacio y ciberespacio—, y la prevención de los ciberataques está en el *top-3* (2) de prioridades del FBI. Todos los países empiezan a invertir en tecnología, organizaciones y doctrina de ciberseguridad. España muy recientemente ha creado el Mando Conjunto de Ciberdefensa en el ámbito del EMAD, y tras el nombramiento de su Mando se publicaron el verano pasado las vacantes para cubrir su primera plantilla.

¿El mundo occidental estaría preparado si llega el temido «Pearl Harbor electrónico»? (3) Quizá en otro artículo valga la pena comentar el enfoque y los medios que dedica España, y en concreto las FAS, a la ciberseguridad.

---

(1) Citado por FALLOWS, J.: «Cyber Warriors», marzo 2010, *The Atlantic*.

(2) GEERS, K.: *Strategic Cyber Security*, junio 2011, CCD COE, Tallin, Estonia.

(3) El exdirector de Inteligencia Nacional de Estados Unidos, almirante Michael McConnell profetizó en 2010 que este país sufriría el equivalente cibernético del 9/11 (Fallows, 2010). El mismo año el almirante auguró la llegada de un «Pearl Harbor electrónico» (Talbot, 2010).

¿Debemos preocuparnos seriamente por la amenaza *hacker*?

Considero de interés exponer algunos datos que ayuden a intuir la magnitud y tipo de amenaza que supone el ciberespacio en todos los ámbitos de la sociedad actual. Empezaré con datos estadísticos que sirvan de orientación sobre el grado de amenaza al que nos enfrentamos y continuaré con ejemplos de algunos de los más importantes incidentes de la historia.

Datos sobre la vulnerabilidad a la ciberamenaza

- En palabras (4) del almirante McConnell, el 98 por 100 del tráfico de comunicaciones clasificadas del Gobierno de Estados Unidos circula por sistemas civiles operados por ellos mismos. El Gobierno ni controla ni protege estas redes.
- Los ordenadores y redes del Gobierno de Estados Unidos son muestreadas continuamente, por lo que su protección es una tarea enorme. Se estima que más de 100 agencias de inteligencia extranjeras intentan acceder a sus sistemas. En un día, los ordenadores del DoD (Departamento de Defensa de Estados Unidos) acceden a Internet más de 1.000 millones de veces. El DoD opera 15.000 redes a través de 4.000 instalaciones en 88 países. Emplea más de siete millones de dispositivos informáticos. Se requieren más de 90.000 personas y miles de millones de dólares para administrar y defender estas redes.
- El 63 por 100 de las compañías españolas han formado parte de *botnets* (5) en 2013, y el 54 por 100 ha experimentado pérdida de datos. Según los registros del CCN (6) (Centro Criptológico Nacional) de 2013, el 69 por 100 de la ciudadanía fue víctima en alguna ocasión de ciberdelitos, y el 65 por 100 lo ha sido en el último año. Este problema tiene un coste neto total de 5.900 millones de euros en España.
- En Estados Unidos los ataques a ordenadores y redes del Gobierno crecieron de 4.095 en 2005 a 37.258 en 2008, con daños valorados en 1.000 millones de dólares. La pérdida por tiempo *off-line* de infraestructura crítica de Estados Unidos debido a ciberataques, suponía ya en 2008 más de seis millones de dólares diarios.

(4) Citado por TALBOT, Jensen E.: «Cyber Warfare and Precautions Against the Effects of Attacks», 2010, *Texas Law Review*, vol. 88, 1533.

(5) Redes zombis de ordenadores que son controlados remotamente de forma oculta para actos maliciosos.

(6) Conferencia «Protección de datos en tiempo real». Jornadas SID 2013, 11 abril 2013. SEGINFO, EMAD, Ministerio de Defensa.

— En el año 2008 la mayoría de los más de 200 países conectados a Internet aún no tenía capacidad de ciberseguridad (7) o era muy escasa.
— Un informe, basado en una encuesta a más de 600 ejecutivos de seguridad y TI (Tecnologías de la Información) de infraestructuras críticas en 14 países, indica la existencia de ataques continuos a estas infraestructuras por adversarios con elevada capacidad tecnológica (8).

Ciberataques históricos

Desde hace más de 20 años los ciberataques han logrado todo tipo de éxitos en múltiples facetas: espionaje, sabotaje, crimen, propaganda, etc. A continuación expongo una breve referencia a algunos de los más importantes.

Ataques a infraestructuras críticas:

— 1982: la CIA logra hacer explotar un gaseoducto siberiano ruso empleando una «bomba lógica».
— 2000: ataque individual a una planta depuradora de agua en Australia. Se descargan en el suministro de agua 1.100.000 litros de aguas fecales no tratadas.
— 2005 y 2007: ataques a la red eléctrica de Brasil que deja sin electricidad a millones de ciudadanos (no confirmado).
— 2007: Israel inutiliza la defensa aérea siria antes de realizar un ataque con aviones de combate a un reactor nuclear (no confirmado).
— 2010: Israel consigue destruir las infraestructuras del programa nuclear iraní mediante un ciberataque con el gusano Stuxnet.

Ataques «patrióticos»:

— 1999: conflicto checheno. Propaganda por parte de *webs* chechenas y ciberataques a estas por parte de Rusia.
— 1999: *hackers* pro serbios atacaron la infraestructura Internet de las fuerzas de la OTAN, Estados Unidos y Reino Unido durante la Guerra de los Balcanes.

---

(7) GOODMAN, S. E.: *Critical Information Infrastructure Protection,* 2008, IOS PRESS, International Affairs and Computing. Georgia Institute of Technology, Atlanta, USA.

(8) Informe del Center for Strategic and International Studies (CSIS) y McAfee, Inc. sobre una encuesta a más de 600 ejecutivos de seguridad e IT de infraestructuras críticas en 14 países sobre prácticas, actitudes y políticas de seguridad. Citado por TALBOT JENSEN, E.: *op. cit.*

— 2000: ataques realizados por los israelíes a *webs* palestinas y de otras facciones enemigas. Gran represalia palestina sobre *webs* y servicios israelíes y estadounidenses.
— 2006: *hackers* palestinos denegaron servicios a 700 dominios israelíes.
— 2007: tres semanas de ataques pro rusos sobre redes del Gobierno de Estonia, afectando a su sistema judicial, bancario y mediático.

Espionaje:

— 1988: ataque Moonlight Maze. Supuestamente ideado por Rusia, llevaba al menos dos años en ejecución contra instituciones de interés estratégico para la defensa en Estados Unidos.
— 2002: ataque Titan Rain. Ataques coordinados contra instalaciones de Defensa de Estados Unidos, NASA, DoD, Lockheed Martin y otros, por lo que se consideran células apoyadas por el Gobierno de China, que consiguieron descargar 20 *terabytes* (9) (TB) de datos. Estos ataques se consideraron posiblemente como una prueba de las capacidades de ciberdefensa de Estados Unidos.
— 2007: el Pentágono admite el ataque de los militares de China a la oficina del ministro de Defensa. El mismo año informa que *hackers* militares habían preparado un plan de ciberataque devastador para inutilizar la flota aeronaval de Estados Unidos. Antes de terminar el año, *hackers* de China se infiltran en las redes del US Naval War College, obligando al apagado de sus sistemas durante varias semanas.
— 2008: *hackers* desconocidos provocan la mayor brecha hasta la fecha en redes clasificadas del Departamento de Defensa de Estados Unidos.
— 2008: *hackers* desconocidos (indicios apuntaban a China) comprometen sistemas informáticos del Gobierno del Tíbet en el exilio.
— 2008: *hackers*, de origen probable de China o Rusia, comprometieron información sensible de las campañas presidenciales de Barack Obama y John McCain.
— 2009: se descubre Ghostnet, *botnet* de espionaje formada por más de 1.000 ordenadores infectados y orientada a la obtención de información diplomática, política, económica y militar en 103 países.
— 2009: el periódico *Wall Street Journal* publica información del Pentágono sobre el robo por cibercriminales durante los años 2007 y 2008, de gran cantidad de información, del orden de TB, sobre el diseño del avión de combate *Joint Strike Fighter* (JSF). Según publica *Forrest Hare* el mismo año, la información fue robada de redes de la industria

(9) *Terabyte* = 1.024.000 *megabytes*.

privada y afectaba a datos de diseño de la futura capacidad de defensa aérea de varias naciones. En 2012 se publica que China consiguió infiltrarse en redes de BAE, contratista británico del programa JSF, y robó secretos de sus sistemas del avión (información negada por fuentes oficiales del Gobierno de China).

— 2009: Operación Aurora de robo de propiedad intelectual contra Google y otras 20 compañías de Estados Unidos, con origen probable en China.
— 2013: un informe de Mandiant Intelligence Center describe sus descubrimientos sobre las acciones de una de las unidades de ciberespionaje de China, denominada APT1 (*Advanced Persistent Threat*), el más prolífico de los 20 grupos o células conocidos con origen en China. Esta unidad ha estado muy activa desde al menos 2006. En el primer informe de 2010 el grupo de análisis no podía asegurar el carácter oficial o el apoyo del Gobierno chino al APT1. Sin embargo, en 2013 la actualización de dicho informe indica que este grupo pertenece a una unidad (10) del Ejército de China, que ha robado de forma sistemática TB de información de al menos 141 organizaciones y mantiene infraestructuras informáticas por todo el mundo. El tamaño de esta infraestructura indica una organización grande, con al menos docenas de operadores y potencialmente cientos.

Ataques políticos/estratégicos:

— 2006: 37 *webs* de los medios y partidos opositores al Gobierno de Bielorusia quedaron inaccesibles durante las elecciones a la presidencia.
— 2008: ciberataques a Georgia desde Rusia indican la ejecución coordinada con las operaciones militares rusas de invasión contra Georgia.
— 2009: durante una crisis política doméstica en el Estado de Kirguistán, ataques DoS (11) (*Denial Of Service*) durante dos semanas interrumpieron el servicio de dos de los cuatro ISP que ofrecían el 80 por 100 del ancho de banda del país.
— 2010: ataques supuestamente de *hackers* patrióticos iraníes a Baidu, el buscador número uno en China (propiedad del Gobierno) y principal competidor de Google.cn. La interrupción por varias horas del servicio del buscador fue provocada por la aparición de una bandera iraní en la portada con el texto *Iranian Cyber Army*. A pesar de que las autoridades de China mostraron escepticismo sobre el origen de

(10) *2nd Bureau of the People's Liberation Army (PLA) General Staff Department's (GSD) 3rd Department*, conocida habitualmente por su código «Unidad 61398».
(11) Denegación de Servicio.

los ataques, el grupo *hacker* patriótico Honker Union tomó represalias, sustituyendo varias *webs* iraníes con banderas de China y eslóganes patrióticos. La opinión generalizada en China fue que el origen real de los ataques provenía de intereses occidentales con objetivo de enturbiar las relaciones Irán-China y entorpecer su colaboración en el programa nuclear iraní. De hecho la agencia china de noticias Xinhua informó que Baidu había denunciado por negligencia a la empresa norteamericana que gestiona su registro de dominio de Internet.

Ataques criminales:

— 2008: la *botnet* Mariposa, creada por DDP Team (Días de Pesadilla), compuesta por ocho o doce millones de ordenadores zombis, se extendió a todo el mundo ofreciendo su alquiler para múltiples servicios criminales, incluyendo recopilación de números de tarjetas de crédito, números de cuenta y robo de información personal (datos de 800.000 personas en poder de los detenidos para robos de identidad).
— 2008: el gusano Conficker se expandió hasta tener infectados el 6 por 100 de los ordenadores del mundo en marzo de 2009. Este gusano, aún activo pero para el que existen parches y herramientas de eliminación, puede recabar información personal o instalar nuevo *malware* en las víctimas.
— 2011: la empresa Epsilon sufrió un ciberataque con daños económicos estimados en 225 a 4.000 millones de dólares.
— 2011: 77 millones de cuentas de usuarios de la red Playstation Network y Sony Online Entertainment, incluyendo la información de tarjetas de crédito y débito, fueron robadas por un grupo desconocido de *hackers*. La paralización de la red para atajar la intrusión tuvo un coste entre 1.000 y 2.000 millones de dólares.

Internet: víctima de su éxito

En la arquitectura y diseño del acceso a Internet (fácil, barato y universal), nunca se consideró la seguridad como un factor primario. Los protocolos utilizados hoy derivan de los establecidos en los primeros días de ARPANET (12), donde solamente unos pocos y muy respetados investigadores utilizaban la infraestructura. En consecuencia, las consideraciones de seguridad no

(12) ARPANET *(Advanced Research Project Agency Network)*. Red desarrollada por el Departamento de Defensa de Estados Unidos y que fue el embrión de Internet.

fueron integradas en el «núcleo» tecnológico de Internet. Todas las medidas de ciberseguridad que se toman hoy en día son complementarias y no remedian las deficiencias de seguridad integrales al concepto de la red. Al haberse adoptado los mismos protocolos de Internet para formar las redes corporativas tipo Intranet, muchas de las vulnerabilidades y carencias de seguridad nativas de Internet se han expandido de forma universal a casi todas las redes.

Lo comentado se refiere al diseño de los protocolos de comunicaciones. Si por otro lado pensamos en la arquitectura de comunicaciones de Internet, observamos que el 90 por 100 del tráfico mundial circula por cables de fibra submarinos aglomerados en unos pocos puntos de congestión (13); y si nos fijamos en la «columna vertebral» de la red, este tráfico es dirigido por solamente 13 *clusters* de servidores DNS (potencialmente vulnerables; el *hacker* quinceañero Mafia Boy atacó nueve de ellos en el año 2000).

En resumen puede decirse que los mismos factores que han hecho de Internet lo que es, una plataforma accesible, colaborativa y que emplea tecnología disponible y abierta, la hacen vulnerable a ataques noveles y susceptible de daños masivos con efecto inmediato.

Para ser consciente del alto grado de vulnerabilidad a la ciberamenaza conviene citar otros factores que facilitan las acciones de los atacantes:

— La velocidad y campo de acción sobre el que es posible atacar. Desde la teoría, un ataque podría dirigirse contra toda la Internet a la vez y a la «velocidad de la luz».
— «El rincón del *hacker*». Existen *kits* «automatizados» para ataques cibernéticos, bases de datos de vulnerabilidades y manuales de instrucciones para realizar operaciones ofensivas en el ciberespacio. No es necesario ser un gurú para realizar un ataque dañino; algunos de los ciberataques más visibles han sido realizados por personal inexperto y sin demasiado conocimiento informático.
— «Caballo de Troya» desde la producción. Existe posibilidad de *malware* integrado en el *firmware* (14) o *hardware* de productos civiles o militares. Un ejemplo de esta preocupación es lo publicado por *The Independent* (15) sobre el supuesto veto de la CIA y el MI6 al fabricante Lenovo (socio mayoritario es el Gobierno de China) a raíz de un informe del año 2000 por el que un servicio de inteligencia

---

(13) BRET MICHAEL, J.; TIKK, E.; WAHLGREN, P.; WINGFIELD, T. C.: *From Chaos to Collective Defense*, IEEE Computer Society, agosto 2010.

(14) Parte programable del *hardware* que realiza el interfaz lógico entre las órdenes del ordenador y las acciones propias del periférico.

(15) *http://www.independent.co.uk/news/uk/home-news/mi6-and-mi5-refuse-to-use-lenovo-computers-over-claims-chinese-company-makes-them-vulnerable-to-hacking-8737072.html*

británico informó de amenazas escondidas en *hardware* y vulnerabilidades en el *firmware* de productos Lenovo. Esto ha llevado al veto de sus productos en sistemas clasificados de Estados Unidos, Canadá, Nueva Zelanda, Australia y Reino Unido. Temores parecidos han surgido del Gobierno de Estados Unidos hacia el fabricante chino Huawei.

— Algunos factores persistentes en la mayoría del desarrollo de *software* dificultan alcanzar una mayor seguridad (16):

  - El alto coste de producción de *software* de calidad y los retos asociados al desarrollo de parches *software*.
  - La vulnerabilidad de algunos lenguajes de programación muy utilizados en algunos métodos de ataque (17).
  - El empleo de derechos de «administrador» por programas rutinarios de usuarios y sistema.

Por todo ello no deja de haber expertos que defienden con vehemencia la necesidad imperiosa de crear, cuanto antes, un plan B (18), una red de respaldo que, sin necesidad de tener las mismas prestaciones que Internet, fuera capaz de mantener los servicios imprescindibles, al margen de Internet, en caso necesario (Hills, 2013). Otros expresan el mismo tipo de preocupación por la necesidad de redes de respaldo garantizadas para los sistemas críticos militares, de la industria y del Gobierno (Solomon, 2011).

Sun Tzu, el analógico

Sun Tzu estableció los principios que durante siglos serían considerados la Biblia de la estrategia militar. Hasta ahora, los consejos y principios de *El Arte de la Guerra* se han demostrado aplicables y eficaces en todos los dominios, a pesar de la evolución de las armas y las guerras.

Sin embargo el quinto dominio, el ciberespacio, tiene características tan particulares y excepcionales que contradicen en parte algunos principios consagrados de la guerra. Para que Occidente se enfrente a este entorno con éxito, se requiere de un gran esfuerzo de mentalización y adaptación de los niveles de decisión a los principios de la ciberguerra.

---

(16) GEERS, K.: *op. cit.*

(17) Los lenguajes C/C++, que han sido muy empleados en el desarrollo de *software* en general, son vulnerables al *buffer overflow* e inyección de código.

(18) HILLS, D.: *The Internet could crash. We need a plan B*. TEDTalks (vídeo *podcast*), 18 de marzo de 2013.

Consideremos como aproximación los siguientes principios, específicos del ciberespacio, enfrentados a la concepción clásica de Sun Tzu (19):

— Sobre la *evaluación* (doctrina, tiempo, terreno, disciplina, mando). La rápida proliferación de las TI, incluyendo herramientas y tácticas de *hacking*, hace que sea imposible que ninguna organización esté familiarizada con todas ellas. A lo largo de los años los atacantes han logrado romper un número cada vez mayor de sistemas operativos, aplicaciones y protocolos de comunicaciones. Los defensores tienen excesivo terreno tecnológico que cubrir. Los ciberataques son más flexibles que cualquier arma que haya visto el mundo; pueden utilizarse, entre otros fines, para propaganda, espionaje y destrucción de infraestructura crítica. De los cinco factores postulados por Sun Tzu para la evaluación, ninguno parece que pueda tener peso específico en el ciberespacio.
— Sobre la *topología* y las *clases de terreno*. No es posible conocer el terreno ni considerar si es favorable o contrario porque las continuas actualizaciones de *software* y reconfiguraciones de redes hacen que la «geografía» de Internet y otras redes cambie de forma continua e impredecible.
— Sobre la *firmeza*; sobre *lo lleno y lo vacío*; sobre *el enfrentamiento directo e indirecto*. La cercanía física de los adversarios pierde toda su relevancia: en el ciberespacio todos somos vecinos (20). En contra del entendimiento histórico en el que el defensor gozaba del «factor campo», la naturaleza asimétrica de los ciberataques favorece mucho al atacante. La brecha ataque/defensa en la relación «coste/beneficio» es enorme. Cuesta muy poco realizar un ataque y hay escasa o ninguna penalización en caso de fracaso. Se pueden rastrear y analizar las redes buscando vulnerabilidades sin sufrir represalias. Una vez que el sistema ha sido comprometido, la recompensa puede ser inmediata. En cambio la ciberdefensa es cara, demandante y no hay un beneficio tangible.
— Sobre *las proposiciones de la victoria y la derrota*. La guerra cibernética implica un gran desconcierto; incluso el saber si uno está o no bajo un ataque puede ser un enorme reto. Puede que una larga y costosa guerra cibernética no sea conocida más que por los contendientes. En el ciberespacio las estimaciones son muy complicadas de realizar con un mínimo grado de realismo. Su naturaleza intangible hace que

(19) Los siguientes apartados comienzan referenciando los capítulos de El *arte de la Guerra* con los que se comparan algunas características de las operaciones en el ciberespacio.

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

el cálculo de la victoria, la derrota o la estimación de daños sea complicado y muy subjetivo. Ataques que se esperan puedan tener éxito, luego no lo tienen, y viceversa. Un ataque sobre una víctima funciona y sobre otra no; un ataque que funciona una vez puede no funcionar la siguiente.

¿Quién ha sido?

Los ciberataques pueden realizarse con tanto anonimato que las estrategias tanto de defensa como de disuasión y represalia no tienen credibilidad. Los *hackers* pueden ocultarse encaminando los ataques a través de países con gobiernos poco colaborativos y empleando redes de terceros. Es habitual que la investigación forense de un ataque acabe en un ordenador *hackeado* (21) y abandonado, sin más rastros. La «posibilidad de denegación» (22) también juega a su favor. Un sospechoso siempre puede decir que su ordenador ha sido *hackeado* y empleado por otros. Internet es perfecto para operaciones de *false flagging* (23), encaminadas a echar la culpa de forma deliberada a otro «jugador».

Este es uno de los mayores problemas a los que se enfrenta la ciberdefensa: la imposibilidad de la «atribución» (24), lo que dificulta enormemente el tratamiento legal y jurisdiccional de los ciberataques, así como la posible consideración de los ataques bajo el prisma del derecho de la guerra (25).

Conclusiones

Las amenazas de tipo criminal, terrorista, de espionaje, de acciones contra infraestructuras críticas, de operaciones de información, etc., tienen un entorno fértil en el que desarrollarse: el ciberespacio. Este dominio sigue unas

---

(21) Ordenador comprometido por un ciberataque.

(22) *Deniability* es el término empleado en la literatura de referencia para expresar la dificultad de la «atribución» de la acción a personas físicas, puesto que, salvo que exista imagen/vídeo de la manipulación del ordenador, es casi imposible demostrar quién es el autor, sin margen de duda y pese a que existan multitud de indicios.

(23) Operaciones en las que el atacante deja rastros que pretenden engañar sobre el origen del ataque, bien siendo este engaño el fin último del ataque, bien como método de defensa o una mezcla de ambos motivos.

(24) En este contexto la «atribución» se refiere a la posibilidad de identificar de forma positiva al autor de los ataques.

(25) *Ius in Bello*.

leyes o principios que poco tienen que ver con los que rigen para los conflictos o guerras «cinéticas» (26). El Sun Tzu del siglo XXI estaría obligado a incluir un nuevo *hashtag: #Arte de la Ciberguerra*.

Internet es un entorno idóneo para la realización de operaciones asimétricas y operaciones militares anónimas: «ofrece a los líderes políticos y militares infinitas posibilidades de éxito y fracaso» (27) (Geers, 2011).

William Lynn, segundo secretario de Defensa de Estados Unidos, expresa claramente cuál debe ser la línea filosófica de la ciberdefensa: «El Departamento de Defensa ha reconocido formalmente al ciberespacio por lo que es: un dominio semejante a tierra, mar espacio y aire. Un dominio del que dependemos y que debemos proteger. Nuestras defensas deben ser dinámicas. Una mentalidad de fortaleza no funciona en el ciberespacio. No podemos retroceder tras una línea Maginot de *firewalls*. La ciberguerra es semejante a una guerra de maniobra y la tecnología nos permite encontrar y neutralizar intrusiones. Pero debemos maniobrar, si nos quedamos quietos nuestros adversarios nos rebasarán» (Talbot, 2010).

Este artículo introduce con enfoque generalista un problema que tiene muchas y complicadas vertientes. Existen múltiples aspectos de interés sobre los que reflexionar con mayor profundidad en torno a las operaciones en el ciberespacio: consideración de los ciberataques en el derecho de la guerra, posibilidad de represalia cinética a un ataque cibernético, operaciones coordinadas cinéticas-cibernéticas, operaciones militares anónimas, protección de infraestructuras críticas, ciberterrorismo, cibercrimen, ciberespionaje, aspectos de jurisdicción y legalidad, tratados de control de armas cibernéticas, el problema de la atribución, la interacción con la industria y dueños de las infraestructuras de redes, organizaciones, instituciones y soluciones de ciberdefensa, etc. Quizá en otra ocasión pueda comentar algo más sobre alguno de estos temas.

(26) Empleo el término «cinético» para referirme a las acciones físicas militares o «convencionales» como contraste a las que se desarrollan en el ciberespacio.

(27) GEERS, K.: *Sun Tzu and Cyber War*, 9 de febrero de 2011, NCIS, CCD COE, Tallin, Estonia.

OTRAS BIBLIOGRAFÍAS

GEERS, K.: *The Challenge of Cyber Attack Deterrence,* 2010. Naval Criminal Investigative Service (NCIS), Cooperative Cyber Defence Centre of Excellence (CCD COE). Tallin, Estonia.

OTTIS, R.: *Proactive Defense Tactics Against On-Line Cyber Militia*, 2010, CCD COE, Tallin, Estonia.

HARE, F.: *Borders in Cyberspace: Can Sovereignty adapt to the Challenges of Cyber Security?,* School of Public Policy, George Mason University.

HENRY, W.; STANGE, J.; TRIAS, E.: *Pearl Harbor 2.0: When Cyber-Acts Lead to the Battlefield*, Air Force Institute of Technology, WPAFB, USA.

MICHAEL, A.: *Cyber Probing: The Politicization of Virtual Attack*, octubre 2012, Defence Academy of the United Kingdom.

SOLOMON, J.: *Cyberdeterrence between Nation-States Plausible Strategy or a Pipe Dream?*, 2011, Strategic Studies Quarterly-Spring 2011.

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

en.wikipedia.org/wiki/Mariposa_botnet

es.wikipedia.org/wiki/Conficker

intelreport.mandiant.com/

www.theaustralian.com.au/news/world/security-experts-admit-china-stole-secret-fighter-jet-plans/story-fnb64oi6-1226296400154