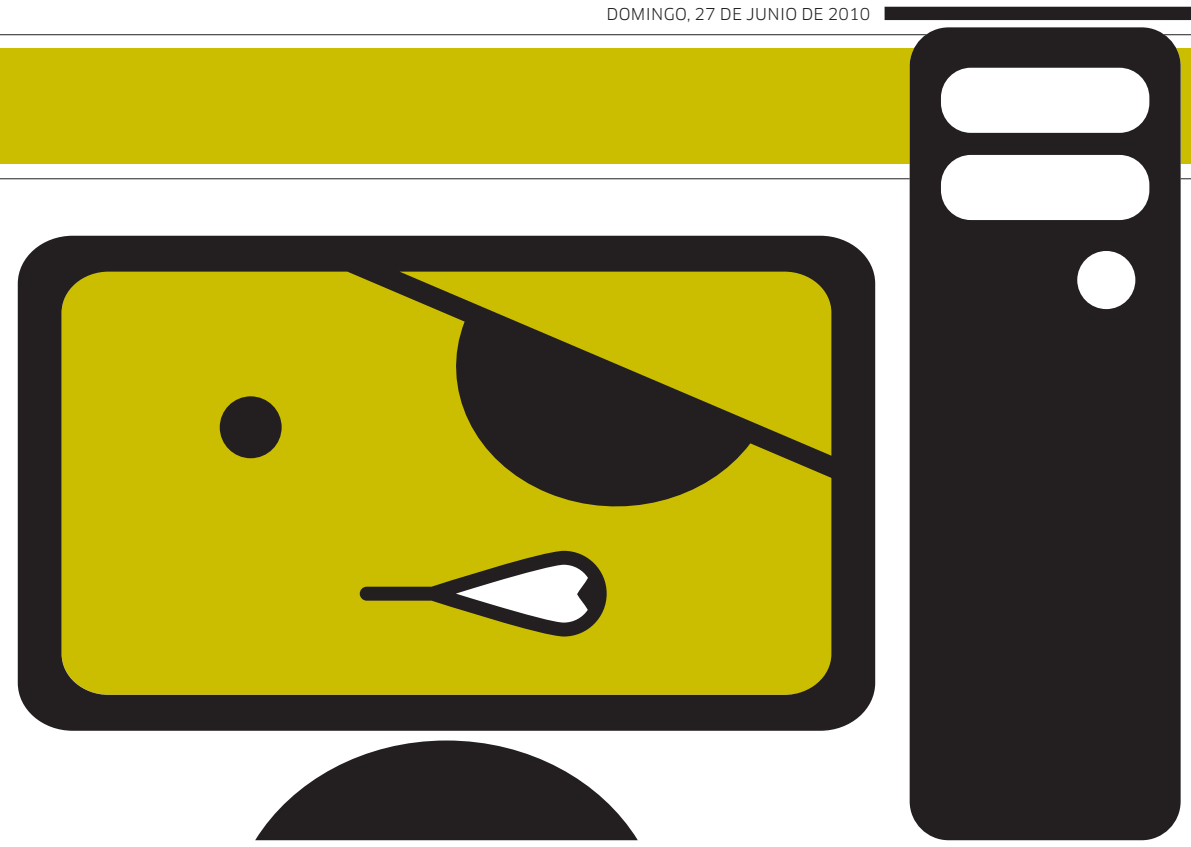
Ciencias



Francia encarga al ejército investigar «armas digitales» para la «lucha informática ofensiva» // Los grandes del armamento mundial –EEUU, Reino Unido, China, Rusia, Israel– se preparan para blindar sus infraestructuras

LA CIBERGUERRA PASA AL ATAQUE

Público en PARÍS

ANDRÉS PÉREZ
CORRESPONSAL

Seis centros crearán armas tecnológicas por una argucia jurídica

Preparan códigos maliciosos, software espía y virus 'caballo de Troya'

Thales negocia con la OTAN la construcción de un 'ciberbúnker'

El gran teórico de la guerra total, el barón Von Clausewitz, escribió que "el soldado duerme, come, anda, se entrena y descansa, todo ello para combatir en el momento y el lugar precisos que le ordenen". Desde hace unos meses, en Francia, al igual que en Estados Unidos, China, Israel, Gran Bretaña y Rusia, el soldado se inicializa, carga su memoria, prepara una bomba lógica y penetra los ordenadores zombis rivales, todo ello para combatir en lo que llaman la "lucha informática ofensiva" que ya está en marcha, abiertamente, en los estados mayores.

El ejército francés acaba de traspasar la línea roja que separa la defensa del ataque militar en el terreno de la guerra virtual, considerado por muchos como la madre de los campos de batalla. Seis laboratorios en todo el país y al menos una unidad del ejército del aire han recibido autorización para investigar sobre "armas digitales", capaces de llevar a cabo una "lucha informática ofensiva" en caso de ataque coordinado enemigo contra las webs gubernamentales, las redes internas de la administración o los sistemas informáticos vitales para el país.

Es lo que se desprende de los anuncios efectuados la semana pasada por la industria militar gala en el principal salón mundial del armamento de tierra, el Eurosatory 2010 de París. Y también coincide con el discurso del secretario general del Elíseo, Claude Guéant, en el congreso del Consejo Superior de la Formación y la Investigación Estratégicas (CSFRS), nuevo centro de doctrina estratégica creado por Nicolas Sarkozy.

El aparato militar francés ha puesto ya en marcha la preparación de códigos maliciosos, software espía y virus *caballo de troya* –que se instalan en el PC del usuario sin que este lo sepa– . Todo ello para dotarse de la "capacidad de neutralización en el interior mismo de los centros de operaciones adversas", "saber combatir al adversario en la fuente misma de la agresión, mediante modos de acción ofensivos" y "garantizar la capacidad de perseguir y reprimir a los agresores", objetivos todos ellos fijados por la doctrina estratégica del nuevo Libro Blanco de la Defensa francés, elaborado en 2008.

Los seis laboratorios privados con control estatal, llamados CESTI, han recibido la autorización para desarrollar "armas digitales", bajo una argucia jurídica. Como intentar penetrar o destrozar un sistema informático ajeno es delito tipificado en el código penal francés, no se les podía dar un permiso general. Por eso, el Secretariado General de la Defensa Nacional (SGDN) se lo dio bajo un eufemismo: los CESTI, en el marco de su trabajo sobre sistemas de defensa frente a ataques informáticos, disponen del derecho a desarrollar "test de penetración". Y, obviamente, para efectuar esas pruebas, necesitan desarrollar y conservar "armas digitales" que penetran. Ofensivas, pues.

Contratos a especialistas

Por otra parte, al menos una célula especializada de la base aérea BA 110 de Créil, al norte de París, trabaja en el desarrollo de armas digitales de combate, según fuentes del sector. En otro terreno, la DGSE, principal servicio de inteligencia exterior francés, ha recibido presupuesto para contratar a cien ingenieros informáticos por año, para operaciones secretas de penetración en servidores ajenos. Especialmente solicitados son los especialistas en *downgrading* (capaces de transformar de manera invisible un protocolo seguro en otro que lo sea un poco menos), en retroconcepción (desmontar, como un motor en un garaje, el

Cómo colapsar un servidor web

El ataque 'DoS'

Es el método con más éxito dada la sencillez del proceso: **se dirige de manera simultánea a miles de máquinas contra el objetivo, que se bloquea** ante la imposibilidad de dar una respuesta a cada solicitud

Fue el tipo de ofensiva que sufrió Estonia, cuando en mayo de 2007, diferentes ataques colapsaron las redes de la banca, el Gobierno y los medios de comunicación de este país. Aunque no se conoce la autoría, **se cree que el ataque tuvo origen en Rusia**

1 Se inicia el asalto

Se instalan varios agentes remotos en diferentes computadoras

2 Los zombis conectan en masa con el objetivo

a MAESTROS

El atacante consigue coordinar varios agentes remotos para infectar más ordenadores

b ESCLAVOS

Los zombis realizan peticiones de forma masiva

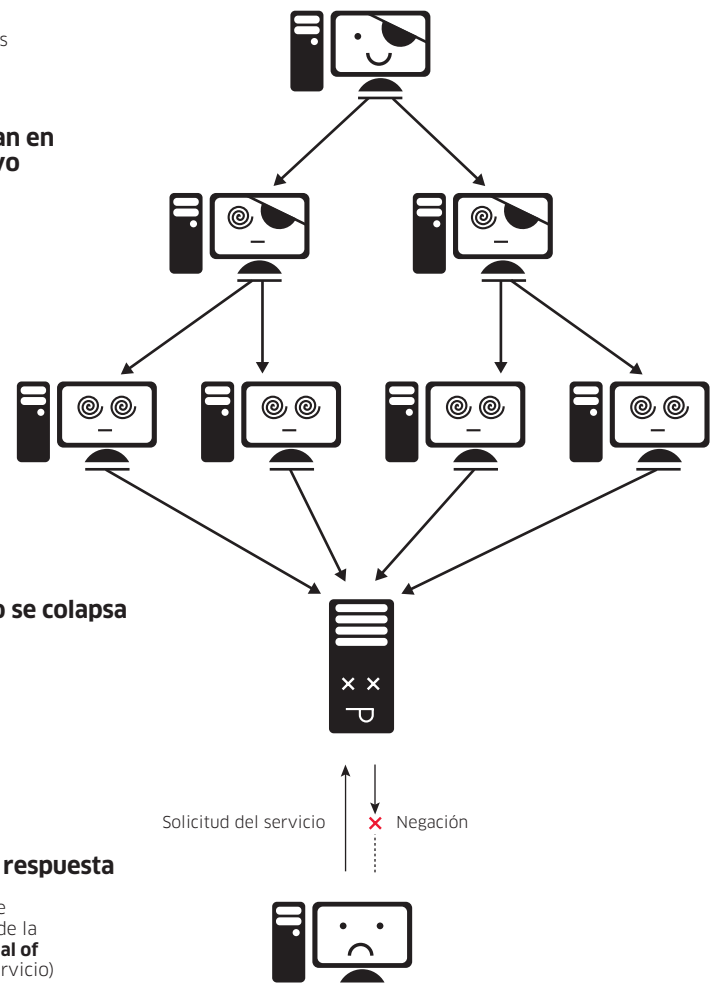
3 El servidor atacado se colapsa

Superado por la **solicitud simultánea** de cientos o **miles de máquinas**, rechaza o ralentiza las operaciones del usuario

Solicitud del servicio — Negación

4 El usuario no tiene respuesta

El nombre de este tipo de ataques, **'DoS'**, proviene de la expresión en inglés **'Denial of Service'** (Negación del Servicio)



FUENTE: ELABORACIÓN PROPIA

infografia@publico.es

WWW.PUBLICO.ES
Responsable de la edición: Patricia Fernández de Lis → ciencias@publico.es

sistema de algoritmos del enemigo para comprenderlo), exploración de vulnerabilidades, sistemas de penetración furtivos y códigos ofuscados (sistemas de explotación cuyas líneas de código están pensadas para que resulten incomprensibles). Las candidaturas de estos expertos, por cierto, son aceptadas sólo por correo postal, y no por email.

Y poco más se puede saber oficialmente de lo que está haciendo en concreto un mundo que avanza bajo el sello *top secret*, pese a que sí hay algo que aparece ya a la luz: los presupuestos. El gigante francés Thales, por ejemplo, adelanta oficiosamente que negocia con el Gobierno francés y con la OTAN para el despliegue de sus búnkeres informáticos Cybels y Nexium en el campo militar. "Para el Estado francés, el coste sería de varios cientos de millones de euros", explicó a *Público* el coronel de marina Stanislas de Maupeou, responsable de ciberdefensa en Thales y ex responsable del SGDN.

Comprender en qué están trabajando exactamente los ejércitos de Estados Unidos, China, Gran Bretaña, Francia, Rusia e Israel requiere lo que Claude Guéant, secretario general del Elíseo, calificó de "agilidad en la posición intelectual" y "capacidad para comprender y arrojar luz sobre las señales imperceptibles que envían nuestros enemigos invisibles y multiformes".

Diferentes escenarios

Tres escenarios principales, sacados de los actos de ciberguerra de los últimos años, están labrando las mentes de los estados mayores. El primero y más temido consiste en un ataque contra los llamados SCADA, es decir, los sistemas informatizados que gestionan infraestructuras críticas como plantas nucleares, red ferroviaria o aeropuertos: para los militares,

La Inteligencia Exterior contrata a cien ingenieros informáticos al año

Los militares creen que causarán daños similares a un bombardeo físico

El hundimiento de páginas web de administraciones provocaría el caos

es plausible pensar que puedan provocar –"en los próximos quince años", según el Libro Blanco de Defensa francés– destrozos similares o superiores a un bombardeo físico.

El segundo escenario es un ataque contra la parte visible de Internet, esto es, las webs y las intranets de administraciones clave, como presidencia, policía, impuestos y hospitales. El hundimiento de esas páginas provocaría caos y desprestigio de un Estado ante sus ciudadanos y ante las potencias extranjeras.

El tercer escenario prevé simplemente la integración de cualquiera de esos ataques informáticos en el marco de una secuencia clásica de guerra convencional.

Las soluciones de ciberbúnker, del tipo Cybels y Nexium, han tenido hasta ahora una aplicación civil para grandes empresas. Esos sistemas analizan, en tiempo real, los flujos entrantes y salientes de un sistema, para detectar automáticamente hasta 75 millones de "eventos". A partir de esos sucesos, escanean otros cientos de millones de procesos para estudiar si hay correlación con un eventual intento de ataque, con lo que localizan 85 "alertas posibles" al día, estudiadas más en profundidad. De ellas, entre cuatro y diez deberán pasar cada día un examen humano efectuado por los 400 ingenieros que, por ejemplo, ocupan los ciberbúnkeres de Thales.

Para la industria privada de altos vuelos, esa capacidad en tiempo real es la garantía frente a los *crackers* (delincuentes informáticos): se acaba la era de los llaneros solitarios. Para los ejércitos, esos centros de lucha de la guerra digital son la retaguardia sólida para contener en tiempo real los ataques desde servidores blindados, comprender la generación de ordenadores zombis –que se pueden controlar desde un único ordenador y obedecen sus órdenes–, identificar al atacante y lanzar contramedidas.

"El ciberespacio ya es un campo de batalla; es más, es el principal campo de batalla, porque hoy el funcionamiento de un Gobierno o un ejército en el campo de batalla real ya depende enteramente de las redes", explica Stanislas de Maupeou.

El 9 de junio pasado, Bernard Barbier, director técnico de la DGSE, es decir, jefe de sistemas de la agencia de acción-intervención, fue muy claro en la conferencia anual SSTIC de Rennes. "Francia lleva 10 años de retraso respecto a China", explicó, según relatan diversas fuentes presentes en el foro. Y confirmó que París va a quemar etapas. Eso sí: como la mayoría de las operaciones ofensivas previstas están prohibidas, serán efectuadas de manera furtiva y, cuando sea posible, desde fuera del territorio francés. ✱

CRONOLOGÍA

Los ciberataques certificados más célebres

2003
'TITAN RAIN'
En 2003 se produjo un ataque, probablemente de origen chino, bautizado como 'Titan Rain' contra administraciones y empresas estratégicas de EEUU. Fueron atacados ordenadores de Lockheed Martin y la NASA.

2007
RUSIA CONTRA ESTONIA
En mayo de 2007 se produjo un ataque de denegación de servicio (ver gráfico) contra la mayoría de los servidores del Estado, la banca y los medios de comunicación estonios. Se le atribuye origen ruso, por coincidir con un conflicto entre los dos países acerca de la retirada de una estatua al soldado soviético en la capital estonia. Este ataque fue el desencadenante del inicio de la reflexión militar en la OTAN y en EEUU sobre la ciberguerra.

2008
RUSIA CONTRA GEORGIA
Coincidiendo con la operación militar rusa de represalias con bombas reales, varias webs gubernamentales fueron atacadas con el troyano BlackEnergy. Los rusos, considerados autores del ataque, lograron paralizar ciertas páginas gubernamentales. Lo más espectacular fue la toma de control de la web del presidente georgiano, en la que los rusos colocaron durante días fotos de Shalikashvili y de Hitler.

2009
IRAK
Soldados estadounidenses en Irak capturaron a combatientes de un grupo chiíta rebelde que disponían en sus ordenadores de imágenes tomadas por los aviones robot 'predator'. Según los expertos, los piratas tomaron el control del sistema informático de transmisión de las imágenes del avión.

Más información

DATOS DE THALES SOBRE CYBELS Y NEXIUM
http://bit.ly/aByAfE

JUEGOS DE GUERRA

China

EL 'CAOS VÍA INTERNET'
Dos coroneles chinos, Qiao Liang y Wang Xiangsui, escribieron en 1999 'La guerra sin límites', documento teórico clave del Ejército Popular de Liberación. En él se lee que Pekín no necesita la paridad militar convencional o nuclear con Washington. Con mucha anticipación juzgan que "el caos vía Internet no es nada inferior a una guerra, y constituye una semiguerra". Un escenario habla de un ataque contra la moneda de un país, seguido de otro contra su deuda soberana y de un ataque informático, para lo cual bastaría con posicionar algunos buques frente al país, sin lanzar ni una bomba.

EEUU

PRIMER 'CIBERCOMANDANTE'
El general Keith Alexander fue nombrado en mayo pasado primer 'cibercomandante' de la historia del ejército estadounidense en paridad con los comandantes de los otros ejércitos. Desde 2006, EEUU desarrolla armas digitales ofensivas y Obama ha relanzado el programa. En su primer discurso programático, el general Alexander dijo en junio pasado que ve la principal amenaza en "penetraciones contra sistemas para practicar el sabotaje remoto" de infraestructuras críticas. Habló mucho de defensa pasiva, pero también solicitó a Obama "reglas de entrada en combate claras".

Francia

UNA RED EFICAZ DE ESPÍAS
Aunque Francia reconoce un retraso de entre cinco y diez años respecto al 'Top Cinco' (EEUU, Rusia, China, Israel, Gran Bretaña), está segura de poder recuperar un buen lugar gracias a su eficaz red de servicios de inteligencia –más eficaz que la de EEUU por ser más ligera– y a disponer de la escuela de matemáticas fundamentales más importante del mundo. El Libro Blanco de Defensa prevé que "como el ciberespacio ya es un nuevo campo de acción en el que se desarrollan operaciones militares", Francia tendrá que ser capaz de luchar en este espacio, con "las reglas de combate apropiadas".

Rusia

ATAQUES INVISIBLES
Rusia publicó en febrero su nuevo documento de estrategia militar, sustituyendo al de hace diez años. No habla ni un momento de ciberguerra, pero tanto los estados mayores occidentales como un informe MacAfee de noviembre de 2009 juzgan que dispone de armas digitales ofensivas. Los expertos estiman que las numerosas referencias a "la información" y a las "tecnologías de la información" en el documento hay que leerlas como alusiones a la lucha informática. Dice que Rusia "reforzará el papel de la confrontación en la información".

Orígenes

JOSÉ MARÍA
BERMÚDEZ DE CASTRO

El tamaño no lo es todo

El cerebro humano ha multiplicado por cuatro su volumen con respecto a nuestro primer antecesor africano, un logro evolutivo muy importante que explica en parte el incremento cuantitativo y cualitativo de las capacidades cognitivas de nuestra especie. Sin embargo, la capacidad para entender, asimilar y utilizar la información que llega a través de los sentidos y el talento para desarrollar determinadas aptitudes no es sólo una cuestión de tamaño. Las neuronas del cerebro están relacionadas a través de billones de conexiones, por las que circula toda la información que nos llega del exterior y del interior. La conectividad se produce durante el desarrollo, pero sigue produciéndose a lo largo de la vida.

Los humanos disponemos de unos siete años de vida postnatal para que el cerebro alcance su volumen definitivo. Esto representa aproximadamente un cien por cien más de tiempo que en chimpancés. Sin embargo, la conectividad neuronal básica de nuestra especie se produce con una lentitud mucho mayor. Cuando tenemos un año de vida apenas hemos aprendido a caminar, mientras que a la misma edad los chimpancés ya corretean por la selva a toda velocidad. La ventaja de una conectividad ralentizada en un cerebro cuatro veces mayor se manifiesta en la posibilidad de recibir estímulos durante más tiempo. El talento potencial que manifestamos aún en nuestra más tierna infancia puede alcanzar cotas increíbles si recibimos los estímulos adecuados. Disponemos de mucho tiempo para ello y esta ha sido una de las grandes adaptaciones de nuestra especie. Nuestra inteligencia parece pues el resultado de un mayor crecimiento cerebral, junto a una ralentización del desarrollo neuronal. Este último proceso se podría catalogar dentro de lo que los expertos en embriología han denominado neotenia, término acuñado por Arthur Kollmann en 1885 y desarrollado en los setenta por científicos tan brillantes como Stephen Jay Gould.

La investigadora Victoria Wobber y su equipo de la Universidad de Harvard se han preguntado las razones de la mayor tolerancia social de los

Parte de nuestra inteligencia se debe al desarrollo neuronal lento

bonobos (*Pan paniscus*) con respecto a la del chimpancé común (*Pan troglodytes*). Estos últimos pierden la tolerancia para compartir el alimento una vez alcanzan la edad adulta. Los bonobos, por el contrario, retienen esa capacidad juvenil durante su vida adulta, a la vez que su grado de sociabilidad es mayor. Wobber y su equipo encuentran la respuesta en la ralentización de la conectividad neuronal de los bonobos con respecto a los chimpancés. Los bonobos son muy inteligentes y por ello se utilizan en las investigaciones sobre las capacidades cognitivas de los chimpancés. Parece que este carácter adaptativo no es exclusivo de nuestra especie y puede haberse producido en más de una ocasión en la evolución de los simios antropoideos.

PARA COMENTAR EL ARTÍCULO:
blogs.publico.es/ciencias

La tormenta no pasará por la zona del vertido

MIAMI// La tormenta tropical *Alex*, que inaugura la temporada de huracanes del Atlántico, no pasará finalmente por el área, según declaró ayer el almirante de los guardacostas estadounidenses, Tim Allen. Los datos del Centro Nacional de Huracanes de Estados Unidos hacían temer ayer por la mañana que *Alex* llegaría a la zona del Golfo de México donde se está intentando detener el derrame masivo de crudo. En tal caso, los trabajos que, según *The Wall Street Journal,* han mejorado sus resultados, se habrían tenido que detener. ✱