Un espía nunca se jubila.

==========

Agente secreta y escritora.

Aline Griffith, condesa de Roma nones, se infiltra en la trama marroquí el último episodio para una saga, al estilo Indiana Jones, que rodará en España la factoría Spielberg. Siempre se pone de parte de los hombres, salvo cuando su esposo, el conde de Roma nones, le reprochó que los «Espías estaban mal vistos en España porque aquí espía suena a traición». Y le dio la razón, claro, pero también hizo lo que le dio la real gana. Efectivamente reconoce Aline Griffth-, pero no enseguida: Tras diez años de casada, sumisa y enamorada, una mujer hace lo quiere con su marido. Para entonces, ¿Quién iba a sospechar de una condesa española?. Regresó al mundo de los agentes secretos del que me confiesa, a sus magníficos, bellos y sobre todo admirables 82 años, que nunca, nunca, volvió a salir.

Pregunta.-Cuando me hablaron de «La trama marroquí» pensé que iba del 11-M.

Respuesta.-Me lo imaginaba, por la conexión con Marruecos, puesto que los terroristas eran de aquel país. Sospeché desde el primer momento que hubiera algunos árabes metidos en ese desastre porque, aunque pareció a todas luces que tenía que ser ETA, mis estudios sobre cómo trabajan todos juntos los terroristas, porque la ETA y los otros grupos están muy unidos, tanto en su preparación y su entrenamiento como en el trasiego de armas, naturalmente me llevaron a plantearme otras hipótesis que luego resultaron ciertas.

P.-¿Por qué rescata precisamente el atentado contra Hassan II?

R.-Porque era un momento histórico muy importante. Además, se presta mucho al interés humano porque se ve el drama y la trama de que la persona en quien el Rey Hassan tenía puesta la máxima confianza y colocó en los puestos más elevados resultó ser su enemigo y el gran traidor que quiso acabar con él. Una historia donde se mezcla la posibilidad del terrorismo con la historia de una traición, un hecho real que pasó en 1971 y del que fui testigo directo.

P.-En su libro narra los entresijos de una conspiración libia contra la monarquía alauita; pero desde entonces las cosas han cambiado mucho y Gadafi es ahora «amigo». ¿Usted se fía?

R.-Imagínese, éste cambia según le convenga. No me fío, en absoluto. ¡Cómo iba a creerme nada de esto si conozco el tema del terrorismo tan a fondo! Trabajé para la CIA cuarenta años, hasta el año 1986, y ahora formo parte de un grupo constituido por antiguos agentes de los servicios de inteligencia procedentes de doce países, y entre los que yo soy la única señora, y que desde hace mucho tiempo venimos estudiando la cuestión terrorista. Por eso pude escribir mi libro sobre Carlos «El Chacal», que estuvo trabajando con nombre falso en una compañía de mi marido; pero ésta es otra historia.

P.-Dice que pertenece a un grupo de ex espías, ¿quiénes son y cuál es su misión?

R.-Es un grupo, aunque no descarto que existan otros, donde personas procedentes de una docena de países entre los que están Francia, Alemania, Inglaterra, España y EE.UU., nos reunimos dos veces al año para estudiar y analizar los problemas más graves internacionales de los que hemos tenidos noticias. Con esa información intentamos ayudar e informar a nuestros propios países aportando a los Gobiernos cuestiones de las que nos hayamos podido enterar y que sean de interés. Somos personas que hemos estado toda la vida en centrales de inteligencia y las reuniones, de tres o cuatro días, se celebran en sitios diferentes del mundo, aunque siempre una de ellas es en Washington, y a las que también asisten representantes de países árabes.

P.-De manera que un espía no se jubila nunca.

R.-Nunca.

P.-¿No le tienta investigar los tentáculos de Bin Laden en España?

R.-Naturalmente. Pero si lo estuviera haciendo no lo diría.

P.-¿Por qué, al contrario de lo que sucede en EE.UU., en España no se la toma en serio?

R.-Es algo que está ahí y que no me gusta. Cuando me casé noté que al adquirir un título y ser una señora que va a fiestas con trajes de alta costura te asignan el papel de frívola y tonta. Siempre he tratado de combatir esa imagen que, sin embargo, en América no es así: allí les encantan los títulos

nobiliarios, algo que me ha facilitado muchísimo la obtención de información en Francia, Marruecos, Alemania... En América nunca nadie me ha puesto en tela de juicio. Pero le diré que esto no ha afectado ni un ápice mi enorme amor a España.

P.-¿Una cualidad imprescindible para ser espía?

R.-Ofrecer confianza. A mí me vigilaron muchísimo. Me habían entrenado a fondo en la escuela de espías y me ofrecí para realizar tareas que entrañaban peligros sin saber que me iban a pagar doble, lo que al final resultó una sorpresa muy agradable. Hablando de la confianza recuerdo que durante la guerra, en Portugal, una secretaria de la oficina de la OSS, que fue el precursor de la CIA, se había enamorado de un portugués que estaba trabajando para los alemanes; la pobre no sabía que él la estaba usando para sacar información y ella, sin querer, le dio datos muy peligrosos y dañinos para los aliados; acabó suicidándose con la cabeza metida en el horno de gas de la cocina de su casa.

P.-¿Qué diferencia a los espías de ahora con los de antes?

R.-Durante muchos años, los servicios de inteligencia y las organizaciones pensaban que tenían que utilizar la más alta tecnología, como cámaras por satélite, para lograr información, pero ahora se han dado cuenta de que lo más importante es la herramienta humana. Hoy en día eso se complica porque necesitas como espías a personas del propio país, con conocimientos íntimos del lugar, y en los que puedas confiar plenamente.

P.-¿Y a los de sus libros con los de verdad?

R.-En que, sin duda, son mucho más divertidos.

P.-Después del chasco de las armas de destrucción masiva en Irak, ¿aconsejaría a la CIA algún curso de reciclaje antes de meterse en Irán?

R.-Se equivocaron y esperemos que la próxima vez lo hagan mejor. Un amigo mío, que fue jefe de la CIA durante los años ochenta, y con el que trabajé en su oficina de Langley donde tantas veces almorzábamos por falta de tiempo un simple bocadillo, aseguraba, sin pensárselo dos veces, que el mejor servicio de inteligencia es el Mossad porque puede hacer lo que le dé la gana sin pedir permiso a nadie. Yo, sin embargo, no podía hacer servicios muy buenos, le hablo de los primeros años ochenta, porque tenemos comisiones en el Senado con distintos grupos que controlan la inteligencia. Así es muy difícil hacer algo útil y eficaz.

P.-Dedica el libro a los servicios de inteligencia españoles. ¿Qué pudo ocurrir para que se gestaran los ataques de marzo y ni siquiera los olieran?

R.-Que los terroristas son muy inteligentes, están muy bien preparados y entrenados desde hace mucho tiempo y nada está hecho al tuntún. Creo que aún hay mucho más detrás de lo que hemos podido averiguar. Además, en España este peligro no se tomó nunca en serio, a pesar de tener desde hace tantos años a una banda como ETA. Los españoles han tenido siempre un buen servicio de inteligencia y así se demostró durante la segunda guerra mundial, como desde luego reconocieron los americanos, que éramos un desastre. El general Emilio Alonso Manglano fue un jefe de inteligencia magnífico y desde otros países se le reconocía como uno de los mejores, un hombre muy discreto...

P.-Pues ya ve cómo cayó.

R.-Claro, porque tenía un empleado que le traicionó.

P.-¿Su olfato qué le dice del estado actual de España?

R.-No me quiero meter en la situación política, pero en lo que se refiere a la inteligencia, aunque ahora no tengo contacto con la agencia, me imagino que están muy bien, porque han pasado por una lección muy dura. Han fallado en una cosa muy grave, pero también fallaron países mucho más grandes y más poderosos.

P.-¿Qué le inspira el «hola amigo» de Bush a Zapatero?

R. ¡Quería presumir de su buen español! A mí, naturalmente, el antiamericanismo me molesta; conozco las muchas faltas de los EE.UU. pero es muy difícil comprender hasta el fondo lo que ese país sintió cuando, sin provocación previa, atacaron sus dos torres. Mi nieto estaba en el edificio contiguo y escapó viendo cómo compañeros morían en el atentado. ¿Se imagina cómo nos sentimos aquí? Los americanos nunca habían sido atacados por ningún país extranjero en su propio territorio en la poca historia que tienen, y recibieron un golpe muy difícil de absorber.

P.-¿Preparada para dar el salto a Hollywood?

R.-En EE.UU. soy la mujer de la inteligencia americana más conocida. Tengo muchos libros sobre los servicios americanos y «La trama marroquí» es sólo un episodio más de mi trabajo como espía. Los estudios Universal y Kennedy

Marshall, que trabajan siempre con Steven Spielberg, han comprado mis cinco libros y quieren convertirlos en súper producciones. Están buscando un guionista y quieren rodar ya este verano en España.

P.-¿Qué actriz ha pensado para condesa de Roma nones?

R.-Catherine Zeta Jones, pero me han dicho que es demasiado mayor ya que para la primera película yo tengo muy pocos años y quieren una actriz muy joven. Su idea es hacer una serie, como la de Indiana Jones, donde el protagonista vaya cambiando de edad.

P.-¿Y quién la vestirá?

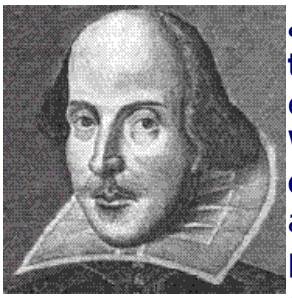
R.-He tenido que ver mucho con la alta costura y muchas veces he estado en las listas de las mejor vestidas gracia a los modistas españoles, personas como Balenciaga y Pedro Rodríguez, que era una maravilla. Ahora, tal vez, Elyo Berhanyer sería el más adecuado, y si no, que, por supuesto, sea un diseñador español.

Fuente: ABC/2005

Los espías británicos leen a Shakespeare

==========

Los servicios secretos británicos están introduciendo reformas para mejorar su eficacia, después del fiasco sobre las armas de destrucción masiva de Irak.



¿Cómo tener más influencia en las personas que uno tiene alrededor? ¿Cómo influir en ellas con mayor efectividad? La respuesta está en **«Julio César», de William Shakespeare**, o al menos eso considera la **dirección de los servicios secretos británicos**, que acaba de organizar una sesión de trabajo para parte de su plantilla de investigadores sobre los personajes de Marco Antonio, Casio, Bruto y Julio César. La pieza de teatro enseña que para influir en los demás no basta la lógica sino que hace falta la inteligencia emocional.

La iniciativa se inscribe en las **medidas** que están adoptando los **servicios de espionaje del Reino Unido** para **mejorar su eficacia y salvar el descrédito que ha supuesto su información de que el régimen de Saddam Husein contaba con armas de destrucción masiva,** dispuestas a ser usadas en un breve plazo de tiempo. El informe Butler presentado en julio estableció que los trabajos de inteligencia habían sido seriamente defectuosos, basados en fuentes de poca confianza, y aconsejó una serie de cambios.

Un hombre de negocios en el MI6

Una de esas reformas ha sido el anuncio esta semana de **crear en el MI6 (Espionaje exterior) dos nuevos puestos directivos,** uno dedicado a **controlar la calidad de** la **información que se procesa y la validez de los informes que se elaboran,** y otro -alguien procedente del mundo de los negocios del sector privado para **velar por la eficiencia de la organización.** Pero no todo es cuestión de organigrama. Lo mejor puede venir por el teatro, sobre todo si se tiene en cuenta que el **trabajo de Espía tiene mucho que ver con el arte de la representación.**

Por eso el (GCHQ), la gran central dedicada a las escuchas, que junto con el MI6, el MI5 (Espionaje interior) y el DIS (Inteligencia militar) constituye los servicios secretos británicos, ha organizado varias sesiones para sus empleados centradas en piezas de Shakespeare, la última sobre: Julio César.

Según el conocido director teatral Richard Olivier, promotor de la experiencia, a la que asistieron doscientos agentes, la obra enseña a valorar la inteligencia emocional. Normalmente se confía a la lógica el deseo de influir en los demás, pero eso lleva su tiempo y en ocasiones no funciona. Nosotros sugerimos que ese tiempo se puede acortar si a la energía mental se añade la energía emocional. Uno puede atrancarse en el nivel lógico y en el uso de argumentos, asegura Olivier, que pone como ejemplo a seguir el personaje de Marco Antonio, cuyo triunfo sobre sus rivales se debe a una inteligencia emocional que le permite entender las necesidades de los que le rodean. Por el contrario, Bruto, que confía en la lógica del honor y en el intelecto, se ve llevado a la muerte.

Fuentes: ABC/2005

Trabajos disponibles para Investigadores

==========

Londres reclutará mil espías más para reforzar la lucha contra el terrorismo en el Reino Unido

En la mayor contratación desde el fin de la Segunda Guerra Mundial, el Gobierno británico va a incorporar nada menos que a mil nuevos espías para combatir el terrorismo en el Reino Unido, donde existen células de extremistas islámicos dispuestos a perpetrar atentados, según insisten los servicios de seguridad.

El reclutamiento se hará especialmente entre las minorías raciales, con prioridad por los conocedores de la lengua árabe, con el fin de lograr una eficaz infiltración y un adecuado procesamiento de la información.

El plan será anunciado el miércoles por el ministro del Interior, David Blunkett, que ante el Parlamento solicitará un importante crecimiento de la partida destinada a la financiación de los servicios secretos. Según adelantaba ayer la Prensa británica, Blunkett planteará incrementar un 50 por ciento el gasto dedicado a espionaje, que llegará a ser de 2.143 millones de euros.

Gran parte del aumento será absorbido por la ampliación de plantilla del MI5, el departamento dedicado al espionaje en el interior del país. Las otras dos principales agencias de los servicios secretos británicos -el MI6, dedicados al espionaje exterior, y el GCHQ, ocupado sobre todo de las escuchas- únicamente tendrán un aumento presupuestario paralelo al incremento de la inflación.

Record

Al MI5 estarán adscritos los nuevos mil agentes, con lo que experimentará un notable crecimiento, ya que pasará de sus actuales 2.100 empleados a superar los 3.000. Esta cifra sólo se había alcanzado en la II Guerra Mundial.

El nuevo personal se incorporará en su mayor parte a tareas de seguimiento y observación de sospechosos las 24 horas del día. Otro grupo estará destinado a reforzar la seguridad de personas o centros que pueden ser objetivos de ataques terroristas.

Una de las principales misiones encargadas al MI5 es la interceptación de mensajes entre la cúpula de Al-Qaeda y los correos que esta organización pueda tener en el Reino Unido. Para ello se considera prioritario el reclutamiento de personas procedentes de minorías raciales, principalmente de origen árabe, con conocimiento de ese idioma, porque pueden infiltrarse con mayor facilidad entre grupos sociales muchas veces cerrados.

El riesgo de atentados perpetrados por extremistas islámicos ha llevado a la continua cancelación del vuelo 223 de British Airways, que cubre la ruta Londres-Washington, ya que información secreta apuntaba a una posible acción terrorista. En un intento de superar la situación.

Fuentes: ABC/2004

La CIA prepara un videojuego para entrenar a sus analistas en la lucha contra el terrorismo

==========

La Agencia Central de Inteligencia (CIA) está trabajando en un proyecto que consiste en crear un videojuego para entrenar a sus empleados en la lucha antiterrorista. El juego forma parte de un proyecto, financiado con 10 millones de dólares, para mejorar la formación de los analistas del Centro Contraterrorista de la CIA, un área de trabajo que cuenta con unos 1.000 empleados.

Según el diario estadounidense *The Washington Times*, el Centro Contraterrorista de la CIA ha encargado la creación de un videojuego para que sus analistas puedan entrenarse en la lucha contra el terrorismo internacional. El Instituto para las Tecnologías Creativas de Los Ángeles, que depende de la Universidad del Sur de California, está elaborando el proyecto con ayuda de expertos de Hollywood y especialistas en videojuegos.

Los defensores del proyecto, como el portavoz de la CIA, Mark Mansfield, consideran que el videojuego será una herramienta "Innovadora" para la lucha antiterrorista porque servirá a los analistas para introducirse virtualmente en una organización criminal, convirtiéndose en un terrorista, o en un responsable financiero, o incluso en un agente de la CIA. Los portavoces de la Agencia Central de Inteligencia justifican la puesta en marcha de este proyecto afirmando:

=====

"Si sirve para ayudarnos a prevenir un ataque terrorista, bienvenido sea".

======

Sin embargo, desde el Pentágono se alzan voces críticas que afirman que la CIA se entretiene con estas "Ideas absurdas" que demuestran que el Centro Contraterrorista, que cuenta actualmente con unos 1.000 empleados.

"No sabe lo que hace".

Las mismas fuentes afirman, en declaraciones a *The Washington Times*, que el vicealmirante retirado John Poindexter, que dirigía el proyecto TIA (Terrorist Information Awareness), se vio obligado a renunciar tras la cancelación de un programa desarrollado por su departamento que simulaba un mercado virtual de futuros en el que pudieran valorar riesgos de carácter terrorista**.**

El director del Instituto para las Tecnologías Creativas, Richard Lindheim, ha declarado por su parte:

"Los juegos son un magnífico camino para impartir formación" y que "nosotros no le llamamos juegos, sino simuladores informáticos de apoyo formativo".

Con respecto a las críticas del Pentágono, Lindheim ha recordado los numerosos galardones que ha recibido "Full Spectrum Warrior", un juego desarrollado por este mismo instituto para el Departamento de Defensa que fue diseñado para formar a los soldados en operaciones de pacificación.

Fuentes: ABC/2004

Semilleros de información

A) Los almacenes de datos de las organizaciones de salud (Hospitales) superan a los de otros tipos establecimientos.

B) Según expertos en Espionaje Internacional, en lo que va del año 2009 las organizaciones de salud han permitido 119 alerta de escape importante dentro de sus computadoras, en comparación con las 39 que ha sufrido la industria de servicios financieros.

C) La industria de los servicios financieros siempre ha estado protegiendo activos valiosos, como dinero, oro, joyas y documentos. Pero el enfoque tradicional de la salud es el paciente. Asegurar la información de los pacientes es un imperativo relativamente nuevo

¿Están fracasando estas regulaciones en la industria de la **salud**?

D) Sí, los criminales de hoy son muy ingeniosos y actúan rápidamente utilizando tácticas innovadoras y en constante cambio que las regulaciones simplemente no pueden cubrir. Cuando se identifica una nueva amenaza a la seguridad y se incorpora al cumplimiento obligatorio, ya ha sido explotada, se han perdido datos y se ha causado daño.

E) El cumplimiento en la seguridad dentro de los Hospitales que es un paso necesario para reducir las brechas de la información confidencial de los pacientes debe ser parte de un plan de seguridad proactivo que incluya políticas efectivas, educación para los empleados, y las tecnologías adecuadas.

F) Cuando se desarrolla un plan de seguridad, hay que comenzar desde sus fundamentos. Todas las organizaciones tienen contenido que es creado, consumido y comunicado.

G) Desafortunadamente, las tecnologías tradicionales para proteger el contenido operan por separado dentro de sistemas descoordinados que son difíciles de mantener actualizados, son costosos, difíciles de administrar y poco efectivos contra las amenazas más insidiosas.

Tres pasos que llevan la seguridad más allá del cumplimiento

- **Crear políticas de seguridad de contenido realistas:** Es importante saber cómo se mueve la información confidencial dentro de su organización, al tiempo de asegurar que usted esté protegido contra amenazas Web maliciosas. Esa es la primera parte de este paso. Enseguida, necesita políticas que controlen quién está teniendo acceso a los datos, cómo los está usando y dónde están siendo transferidos. Finalmente, determine con qué tecnologías cuenta para evitar la pérdida de datos en tiempo real.

- **Educar, educar, educar:** Adoptar políticas y programas educativos ayuda a reparar procesos de negocio riesgosos. Además, ofrecer capacitación a los empleados puede ayudar a educarlos sobre las políticas establecidas y realzar la práctica de seguridad general. Si existen dudas, siga repitiendo las mejores prácticas a sus empleados. Realice un seminario de asistencia obligatoria para sus empleados por lo menos dos veces al año para hablar sobre las ramificaciones de las brechas de datos y las mejores prácticas más recientes.

- **Integrar tecnología de seguridad de contenido en tiempo real:** Integre tecnología innovadora que proteja proactivamente a su organización contra los métodos más recientes empleados por los criminales. Para contar con protección efectiva y una administración más sencilla, utilice productos de seguridad de contenido que estén integrados con análisis unificado de amenazas, consolas unificadas de administración y tecnologías de implementación flexibles (software que usted instala en sus servidores, dispositivos para el desempeño o servicios en la nube que no requieren hardware en sus instalaciones.

Las amenazas internas y externas están en constante cambio; su tecnología de seguridad también necesita analizar el tráfico Web en tiempo real, categorizar el contenido dinámico, al tiempo de bloquear malware de día cero y prevenir la pérdida de datos confidenciales. Asimismo, asegúrese de que la tecnología seleccionada cumpla con las regulaciones y genere los reportes adecuados.

El resultado es claro: las regulaciones son necesarias desafortunadamente el costo de las brechas de datos, ya sea de un intruso malicioso, un empleado inconforme o un simple error, puede tener repercusiones a largo plazo en la reputación de una institución que se construyó sobre años de prestar excelente atención a los pacientes. (Fuentes: ABC/2004)

Stuxnet, primera arma cibernética militar

==========

Un virus desarrollado por Estados Unidos e Israel habría dañado de manera irreversible la central nuclear iraní de (Busher) y retrasado su plan para conseguir el arma atómica

La primera batalla de la guerra del futuro tuvo lugar en agosto 2010. No habrán visto fuego, humo ni habrán escuchado el ruido de las explosiones en los telediarios.

¿El escenario?

Una red de ordenadores repartida por el mundo. ¿El arma? Un virus informático creado, según informaciones periodísticas británicas, por una coalición de naciones liderada por Estados Unidos e Israel.

¿El objetivo?

La central nuclear iraní de (Busher).

¿Su nombre? Stuxnet.

Se trata de un virus, del primer gusano informático que afecta a equipos con Windows, es capaz de espiar y reprogramar sistemas industriales, en concreto el sistema Scada de control y monitorización de procesos. El virus Stuxnet infectó a más de 30.000 ordenadores de Irán (un 60% de los que existen en el país). También se vieron afectados países como Indonesia, India y Pakistán. La conexión sería Siemens, la empresa alemana que ha desarrollado un sofware de control de grandes infraestructuras para su instalación en la central nuclear iraní y que emplea Windows 7.

«Stuxnet es algo nuevo. Hasta ahora no había un código dañino con esa capacidad de atacar a esta clase de sistemas. El virus no se ha transmitido en remoto, por correo o entrando a una web. No. Se empleó una llave USB. Y posee una capacidad para atacar sistemas operativos muy avanzados. Stuxnet representa un cambio de tendencia, concede el responsable del Centro Criptológico Nacional. Stuxnet nos alerta de que los ataques pueden ser muy complejos.

Aunque Irán ha anunciado hace unos días que ha empezado a realizar la carga de la central con uranio, el fracaso del ataque con Stuxnet habría obligado a la fuerza aérea israelí a bombardear Busher(casi inexpugnable por vía aérea, según el ministro israelí de Defensa) como ya hizo con las de Osirak y Tammuz (ambas en Irak).

Los nuevos conceptos establecidos por la OTAN y el CNI participa en numerosos comités y grupos especializados de la organización prevén que los aliados puedan sufrir el ataque de un virus preparado para hacerse con el control de los sectores críticos de los países integrados en la Alianza (energía, transportes, comunicaciones, banca...) De hecho, Estados Unidos y otros países de la OTAN preparan un blindaje que proteja de un ataque cibernético al escudo antimisiles que se instalará en Europa.

Stuxnet, que fue detectado en Bielorrusia el pasado mes de junio por la empresa VirusBlokAda, ha demostrado que los blindajes informáticos actuales no sirven ante las nuevas armas cibernéticas, capaces de mutar y de disfrazarse para aparentar lo que no son. Es un prototipo funcional y aterrador de arma cibernética que conducirá a la creación de una nueva carrera armamentística mundial, alertan las compañías europeas de seguridad digital.

La proliferación de tecnología bélica cibernética escapa a todo control, escribe en su blog Daniel Kuehl, un teniente coronel especializado en guerra cibernética. Y ya empiezan a oírse voces en Estados Unidos que piden que las agencias gubernamentales que trabajan en la materia aúnen sus esfuerzos y la exigencia a las empresas privadas de informática para que hagan sus productos más resistentes a infecciones. (Fuentes: ABC/2004)

La ropa para hacernos invisibles.

==========

Físicos británicos crean un material flexible que consigue esquivar la luz y hace desaparecer los objetos al ojo humano

Investigadores de la Universidad de Saint Andrews en Escocia han desarrollado un material que da un paso más hacia la creación de prendas de invisibilidad capaces de manipular la luz para ocultar los objetos de la visión, **como la famosa capa de Harry Potter**. Los resultados de su trabajo se publican en la revista New Journal of Physics.

Una membrana del nuevo material Metaflex

Dos de los principales retos en el desarrollo de una prenda que pueda hacer invisibles los objetos que cubre son, por un lado, producir meta átomos lo suficientemente pequeños para interactuar con la luz visible y, por otro, que estos diminutos elementos sean lo suficientemente flexibles.

Los físicos han diseñado un nuevo material denominado **Metaflex** que puede superar ambos obstáculos. Este meta material, compuesto de meta-átomos capaces de desligarse de una superficie rígida, interactúa de forma especial con la luz. En vez de reflejarla, la curva, de manera que los rayos que lo rodean recuperan su trayectoria y siguen su camino. **Lo que se sitúa detrás de este material especial, simplemente, se esfuma en el aire**. Parece un truco de magia, pero tras este logro hay un complicadísimo estudio de la Física. Este efecto de invisibilidad ya se había conseguido otras veces, pero en esta ocasión da un paso más allá. Anteriormente, el efecto se

había conseguido con luz no visible (infrarojos y microondas).

Ahora, se ha conseguido dentro del rango de luz visible para el ojo humano. Cualquiera puede comprobarlo.

Un poro de Harry Potter

Además, los autores también han conseguido que el material sea flexible y lo suficientemente grande para que no se quede sólo en el ámbito experimental de la nanotecnología y pueda adoptarse para una variedad de aplicaciones. Su muestra mide 5x8 milímetros cuadrados. **No puede cubrir entero a Harry Potter, pero es un primer paso.**

El nuevo material podría utilizarse para crear ropa inteligente y en lentes de contacto desechables, explica Andrea Di Falco, director del proyecto.

«Es un gran paso adelante en muchos sentidos»

Ha añadido Ortwin Hess, físico del Imperial College.

«Está claro que no es una capa de invisibilidad aún, pero es el paso correcto hacia ella» (Fuentes: ABC/2004)

"No descarto un `Pearl Harbor` digital"

La proliferación de nuevos y más sofisticados ataques cibernéticos, sumado a una mayor avaricia e ingenio por parte de los delincuentes digitales, plantean un escenario de terror para el futuro que se podría traducir en una `guerra cibernética`.
Así lo confirma Patricia Titus, vicepresidente Global de Seguridad de Unisys, y anteriormente asesora en seguridad informática del Departamento de Estado de los Estados Unidos.

Esta inteligente mujer es una de las personas que más conoce en el mundo sobre el tema. En conversación con (Titus) alertó sobre la necesidad imperiosa de llevar la discusión sobre la seguridad a instancias internacionales como la ONU para evitar en el futuro una guerra digital que podría ocasionar un caos generalizado en todos los países del mundo.

¿Cómo vienen avanzando los ataques informáticos y quiénes los realizan?

En el entorno internacional lo que estamos viendo es un direccionamiento de los ataques hacia áreas específicas como instituciones financieras, fraudes a tarjetas de crédito, y cosas de alto valor. Los hackers se vuelven cada día más avaros, eso hace que sus golpes se vuelven cada vez más sofisticados y se focalicen principalmente en grandes infraestructuras y objetivos de alto valor. Como predicción, creo que en los próximos meses, en los Estados Unidos, se producirá un ataque importante contra una gran empresa ya sea en el sector de telecomunicaciones, energía o una institución financiera importante, que probablemente va a crear algún nivel de caos.

¿Cuáles son los sectores preferidos de estos delincuentes para sus ataques?

Existe una fuerte actividad en el sector financiero, y posibilidades de ataque significativos en los sectores de energía y telecomunicaciones que podrían desestabilizar a estas empresas. Curiosamente el sector público ya no es un objetivo primordial, pero el riesgo está en que a través del acceso a información privilegiada de los proveedores de un Gobierno, ellos pueden en algún momento vulnerar los sistemas de entidades gubernamentales y causar estragos en esas plataformas.

¿Se rumora que la próxima guerra podría ser cibernética, está de acuerdo con esto?

Espero no estar viva para verlo. En caso de darse una guerra lo primero que podría suceder es que los terroristas usen la tecnología para causar daño físico a las instalaciones y a las personas para las cuales va dirigido el ataque. Ese sería su principal interés. En cuanto a una guerra 100% digital, eso aún no ha pasado pero estamos viendo manifestaciones. Yo creo que en unos años se podría dar un `Pearl Harbor` digital, con consecuencias desastrosas. De hecho, los impactos de un gran ataque cibernético serían inimaginables, pues podrían desestabilizar países enteros.

¿Qué se puede hacer para minimizar esa posibilidad?

Creo que hay que llevar la discusión a las altas instancias internacionales para poner el tema sobre la mesa, ya que los ciber delincuentes no se van a detener y cada día buscan nuevas formas de causar daño a través de sus ataques.

De hecho, en Estados Unidos se planteó la posibilidad de proponer que los países tuvieran `ciber embajadores`, y tratar este tema de una forma diplomática. La alta dependencia actual de las comunicaciones nos obliga a tomar acciones que protejan no solo a los gobiernos sino también a las empresas que se mueven a través de este medio. Esto se debería dar ya, la verdad no sé qué estamos esperando.

Si bien el solo hecho de pensar en un gran ataque causa zozobra, ¿qué recomendaciones se pueden dar al respecto?

Pensar en esa posibilidad hace que la gente descuide sus sistemas personales como las computadoras y los smartphones. Es importante que tanto usuarios como empresas sigan las recomendaciones correspondientes, como la actualización de los parches de los sistemas operativos, establecer contraseñas y contar con antivirus. Lo importante aquí es pensar siempre en su seguridad y actuar rápido para mantenerla.

Sistema financiero, un objetivo principal

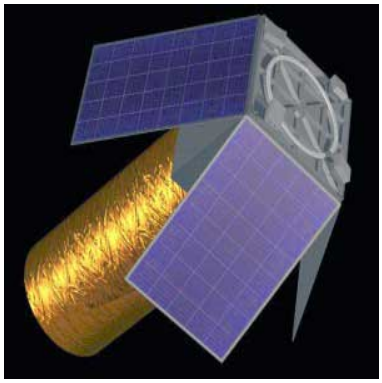
De acuerdo con Patricia Titus, el sector financiero es uno de los más atractivos para los criminales cibernéticos, no solo por el simple hecho de los réditos de atacar las plataformas de los bancos sino de obtener información de las cuentas de los usuarios para realizar transacciones fraudulentas. Los movimientos electrónicos del sistema financiero internacional podrían ser un blanco favorable para estos delincuentes y crearían un serio temor en los mercados internacionales, con los efectos que estos pueden tener sobre las economías de todo el mundo. (Fuentes: ABC/2004)

Satélites espías para ayudar a las unidades militares de tierra

Imagina una unidad militar en situación de combate en una zona montañosa al este de Afganistán, tratando de controlar a un grupo insurgentes que ha estado operando desde arriba en las montañas. Sería estratégicamente ventajoso saber exactamente quién y qué le espera al otro lado, sin embargo, el avión teledirigido *Predator* está ocupado en la supervisión en un paso clave en la frontera a kilómetros de distancia. En este caso, lo que realmente necesitarían las unidades militares es un satélite para obtener algunas imágenes en tiempo real del paisaje circundante. Para poder satisfacer esta necesidad, un equipo de ingenieros de la empresa *IntelliTech Microsystems* ha desarrollado el *Kestrel Eye*, un sistema de satélites espías de bajo costo que pueden ser reposicionados en el campo de batalla con gran rapidez y precisión.

Kestrel Eye consiste en una red de 30 pequeños satélites transmitiendo imágenes directamente a las tropas sobre el terreno indicado. A través de un dispositivo móvil de reducido tamaño, permite conectarse con los satélites en tiempo real, pudiendo descargar hasta dos imágenes por segundo, que abarcan hasta 8 kilómetros cuadrados en cada fotografía. Además, estas fotos se almacenan en un servidor central para que otras unidades que operen en la zona puedan echar un vistazo del entorno

El telescopio de 254 milímetros implementado en el sistema, no es capaz de obtener las mismas imágenes en alta resolución que los satélites empleados por los servicios de inteligencia. Sin embargo, una resolución entre 1,5 metros a más de 8 kilómetros cuadrados es más que suficiente como para identificar al enemigo, localizar un lugar o conocer el desplazamiento de un convoy del enemigo. Pero quizás la mayor ventaja de *Kestrel Eye* es que cada satélite cuesta tan sólo 665.000 euros, un precio muy económico de venta en comparación con los grandes satélites de espionaje. Puesto que el costo es el mayor asesino de un sinfín de ideas brillantes en el ámbito militar, el bajo precio de *Kestrel Eye* significa que se encuentra en una buena posición para estar en órbita a partir del 2011 al servicio del ejército de los Estados Unidos. (Fuente: Feria de la Ingeniería)



EE.UU. anuncia el mayor acuerdo militar de su historia con Arabia Saudí

==========

Si se ejecuta el completo, supondrá la venta de armas a Riad por valor de $60.000 millones de dólares Se ha diseñado como eventual escudo ante la amenaza de Irán

El Gobierno de Estados Unidos ha presentado este miércoles al Congreso un plan para vender 60.000 millones de dólares en aviones a Arabia Saudí durante los próximos 10 años, que -si se ejecuta en su totalidad supondría el mayor acuerdo militar bilateral de su historia, ha informado el Departamento de Estado.

El subsecretario de Estado para Asuntos Militares, Andrew Shapiro, ha indicado en una rueda de prensa que la Administración Obama no espera que haya trabas por parte de Israel, a pesar de que en los últimos meses ha mostrado objeciones al plan.

El Congreso tiene 30 días -hasta el 20 de noviembre del 2010 para decidir si detiene la venta antes de que el Departamento de Defensa ponga a disposición del Gobierno saudí los contratos.

El acuerdo inicial prevé la venta de 84 nuevos aviones de combate F-15, la actualización de otras 70 de estas aeronaves y la oferta de tres tipos de helicópteros: 70 Apaches, 72 *Black Hawks* y 36 *Little Birds*.

Los contratos, divididos en cuatro paquetes, contemplan también el envío de radares avanzados y de bombas guiadas por satélite, además de la creación de programas de entrenamiento.

Un escudo ante la amenaza iraní

El Gobierno estadounidense considera que el plan aumentará la capacidad de las Fuerzas Armadas saudíes para crear un escudo ante las amenazas en la región, especialmente la irán. Sin embargo, el acuerdo no se ha cerrado únicamente por Irán, sino que pretende "ayudar a los saudíes con sus necesidades legítimas de seguridad, que son bastantes.

Según el funcionario, es posible que el reino de Abdulá bin Abdulaziz decida no aportar todos los fondos para los cuatro programas, debido a los requisitos de defensa que ha establecido el país.

La suma final de la venta podría ser inferior a la estimada $60.000 millones de dólares, ya que dependerá de lo que el Gobierno saudí decida comprar, y del resultado de las negociaciones con la industria.

Shapiro no ha realizado declaraciones sobre una posible segunda fase del plan que sí daba por hecha en septiembre The Wall Street Journal, según la cual Estados Unidos prestaría al país $30.000 millones de dólares más para modernizar las fuerzas navales saudíes. De acuerdo con el diario económico, esa fase podría incluir el despliegue en el litoral saudí de naves de combate y el uso de cargueros para operaciones cercanas a la costa.

Sin veto de Israel

Un tercer paso consistiría en reforzar la defensa de Riad contra misiles balísticos iraníes, mediante la venta de sistemas THAAD y la actualización de misiles *Patriot*, en una táctica similar a la empleada en los Emiratos Árabes Unidos. Shapiro ha subrayado que el acuerdo no afectará negativamente a los intereses de seguridad de Israel o a la calidad de sus fuerzas armadas, en referencia a las presiones de ese país para evitar que la venta incluyera armamento de largo alcance.

El compromiso de la Administración estadounidense de que no enviará ese tipo de equipamiento, y el acuerdo por el que **Washington venderá a Jerusalén una partida de aviones F-35, más avanzados** que los de los saudíes, parecen haber acallado las quejas israelíes. El Gobierno de EE.UU. se muestra optimista respecto a sus opciones de que el plan salga adelante en el Congreso, donde espera que el potencial del acuerdo para **crear empleos dentro del país** juegue a su favor. Según Boeing, la empresa que fabrica gran parte de las aeronaves, el plan podría sustentar $**77.000 nuevos puestos de trabajo** distribuidos en 44 estados diferentes.

(Fuente: Feria de la Ingeniería)