

Internet y nuevas tecnologías

ROBERTO PLÁ
Teniente coronel de Aviación
<http://robertopla.net/>



CIBERGUERRA PRIMER JEFE DEL MANDO DE CIBERDEFENSA

La Estrategia Española de Seguridad de 2011 considera los ciberataques como una amenaza actual, real y en crecimiento para los intereses nacionales, y hace hincapié en la necesidad de garantizar el uso seguro del ciberespacio.

La Directiva de Defensa Nacional de 2012 establece que la disuasión es el resultado de disponer de unas capacidades y de la determinación de utilizarlas si fuera necesario.

Para encuadrar la actuación de las Fuerzas Armadas en este importante campo de la Defensa, se creó el pasado 19 de febrero el Mando Conjunto de Ciber Defensa (MCCD), dependiente del JEMAD, almirante general Fernando García Sánchez; su ámbito de actuación son las redes y los sistemas de información y telecomunicaciones de las Fuerzas Armadas, así como aquellas otras redes y sistemas que específicamente se le encomiendan y que afecten a la Defensa Nacional.

La dirección de esta gran unidad de elite en la defensa moderna ha sido encomendada al general de brigada del Ejército del Aire Carlos Gómez López de Medina.

Se encargará, entre otros cometidos, de garantizar el libre acceso al ciberespacio, de responder en el mismo a las amenazas o agresiones que puedan afectar a la Defensa Nacional y también deberá cooperar con los centros nacionales de respuesta a incidentes de seguridad de la información (CERT), de acuerdo con lo que determinen las estrategias y políticas nacionales de 'ciberseguridad' en vigor.

Si desde Revista de Aeronáutica saludábamos con alegría la creación de las primeras unidades de Ciberdefensa del Ejército del Aire, es un auténtico placer celebrar el nombramiento de un presti-

gioso oficial de nuestro ejército como primer jefe del MCCD.

El general de brigada del Ejército del Aire Carlos Enrique Gómez López de Medina, es miembro de la XXXIII promoción de la AGA y mandó como coronel el Grupo Central de Mando y Control -unidad pionera de la informática operativa del Ejército del Aire.- desde mayo de 2009 hasta agosto de 2011, cuando fue ascendido a general de brigada pasando destinado al Mando de Apoyo Logístico del Ejército del Aire. A lo largo de estos últimos meses ha trabajado en el Estado Mayor de la Defensa para poner en marcha el MCCD.

Está previsto que el Mando Conjunto de Ciberdefensa se traslade a las instalaciones que ha dejado libre el Mando de las Fuerzas Aliadas de la OTAN en Retamares, donde alcanzará la Capacidad Operativa Inicial después de verano.

 <http://delicious.com/rpla/raa826a>

SEGURIDAD

¿ES POSIBLE “HACKEAR” AVIONES CON UN TELÉFONO?

Cuando nos subimos a un avión comercial se nos indica que debemos apagar los teléfonos. Los profanos no se explican cómo se puede pedir al pasaje que apague completamente sus móviles, prescindiendo incluso del 'modo avión' cuando, según comentaba alguien en una red social, al subir al aparato pudo ver a los pilotos utilizando una tableta gráfica.

Los profesionales sabemos que en un entorno crítico y complejo, como es la instrumentación de un avión, uno de los mayores peligros son las sorpresas. Se podría decir que todos los fallos posibles de la aeronave han sido estudiados y las medidas para afrontarlos se describen de forma detallada en los manuales de operaciones. El problema de una interferencia extraña no es tanto lo que hace o puede hacer, sino la forma inesperada de hacerlo. Por esa razón las normas de las

compañías intentan evitar a sus tripulaciones esas 'sorpresas' indeseadas e innecesarias.

La habilitación de conexiones a internet para dispositivos móviles que han iniciado algunas compañías demuestra que estos dispositivos no son incompatibles con el vuelo, si se encuentran dentro del entorno de funcionamiento previsto por el diseño del aparato.

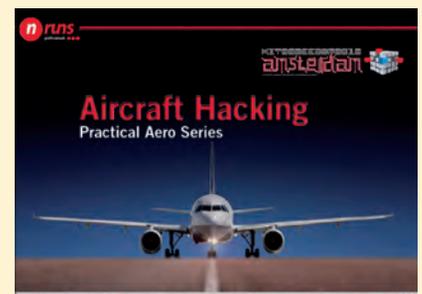
Pero el uso de teléfonos 'inteligentes' u otros dispositivos similares, ¿Puede hacer peligrar de otra forma la seguridad de la aeronave?.

El experto en seguridad informática y piloto comercial Hugo Teso presentó en el congreso 'Hack in the Box' de Amsterdam una ponencia sobre las posibles vulnerabilidades informáticas que afectarían a los modernos sistemas relacionados con la circulación aérea.

Todos sabemos el delirio que tienen los periodistas por los titulares llamativos y a través de ese prisma podemos desechar casi todos los que ha generado este hecho, que nos presentan una imagen caricaturesca de un *hacker* controlando mediante su teléfono un avión comercial como lo haría un aeromodelista con su modelo de radiocontrol.

Hay que desechar también las declaraciones oficiales de las compañías relacionadas con la industria aeronáutica negando la mayor.

La mejor vía de información es la propia fuente y en la *web* del propio Teso, 'Comander Cat', podemos encontrar el resultado de su trabajo. En un interesante análisis que detecta vulnerabilidades fá-



cilmente explotables en los sistemas Automatic Dependent Surveillance-Broadcast (ADS-B), que envía información acerca de cada aeronave (identificación, posición actual, altitud, etc) mediante el transmisor de a bordo, al sistema de control de tránsito aéreo y el Aircraft Communications Addressing and Reporting System (ACARS), sistema que proporciona automáticamente la información sobre cada fase de vuelo y permite intercambiar mensajes por radio o por satélite entre los aviones y el control terrestre.

Estos sistemas están basados en la confianza, y entre sus planteamientos de diseño no está la posibilidad de que se pueda introducir intencionadamente información falsa. El propio ACARS puede seguirse casi en tiempo real mediante un terminal en casa, y a través de la red en el propio teléfono móvil.

A partir de ahí el estudio investiga cómo se podrían explotar estas vulnerabilidades para inducir errores o variaciones en el desarrollo de un vuelo. Las investigaciones se han desarrollado sobre modelos simulados de los sistemas reales de los aviones, y las conclusiones de la exposición de Hugo Teso son que el concepto de seguridad en vuelo aplicado a los aviones comerciales es diferente de la seguridad necesaria para evitar un ciberataque, y que es necesario un nuevo concepto de seguridad que realice una auditoría de la seguridad informática de los sistemas a bordo. Una tarea que ha de afectar a los fabricantes, a los proveedores de servicios en tierra y a las aerolíneas.

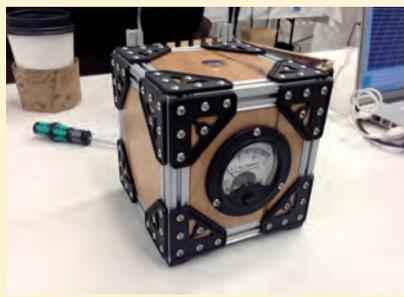
■ <http://delicious.com/rpla/raa826b>

TECNOLOGÍA

LA FERIA DE LOS HÁBILES INGENIOSOS

Maker es una nueva tendencia que arrasa en la red. Reúne a los amantes de la alta tecnología hecha en casa. El abaratamiento y disponibilidad de muchos elementos de alta tecnología ha hecho posible que pasemos del bricolaje clásico al tecnológico.

Como otros fenómenos de internet, puede ser pasajero o tratarse del primer paso en una importante transformación cultural. Probablemente tiene algo de ambas cosas, ya que nada es para siem-



pre y todos los cambios afectan a nuestro mundo, que con ellos evoluciona de forma continua.

En aviación, el medio más importante no es el aire, sino la tecnología. Al fin y al cabo, el aire siempre ha estado ahí, pero solo hemos podido navegar a través del mismo cuando hemos dominado la tecnología adecuada. Por esta razón, un aviador debería ser siempre sino un tecnólogo, cuando menos un tecnófilo.

Hace años los espíritus inquietos podían construir cometas o planeadores, radios de galena o telescopios en su propia casa. Había mucha diferencia entre la tecnología disponible para el público y la que solo era accesible a los laboratorios científicos o talleres de diseño de las grandes empresas.

Hoy en día, sin embargo, podemos acercarnos a la tienda de componentes y comprar elementos electrónicos de alta tecnología como microprocesadores, receptores de GPS, pantallas táctiles o cualquier otro elemento electrónico a precios económicos y listos para integrarlos en nuestro invento particular. A veces casi es mejor no tener una tienda de componentes a mano: en la red encuentras quien te lo envía desde la otra punta del mundo a portes pagados y mucho más barato.

La revista Make Magazine tiene como tema central la difusión de proyectos que amplían el conocido "hágalo usted mismo" al de "hágalo con otros". Se trata de difundir el conocimiento de proyectos técnicos, mecánicos, artísticos o científicos realizados por entretenimiento o por el puro placer de aprender.

Se podría decir que es la heredera moderna de la clásica "Mecánica Popular", y a sus seguidores se les llama 'Makers' (fabricantes). Son estudiantes o ingenieros, informáticos, artistas o modelistas y son curiosos, inquietos y habilidosos, con una gran capacidad para integrar la tecnología disponible en sus proyectos.

En 2006 se organizó por primera vez una Feria Maker en la ciudad de San Mateo (California, EE.UU.). En 2012, su séptima edición, la exhibición reunió alrededor de 800 makers y convocó a más de 110.000 visitantes durante un fin de semana. Este éxito ha permitido exportar el concepto y formato de Maker Faire que se ha extendido por el mundo bajo la marca Mini Maker Faire.

Los protagonistas de estas ferias son los makers, personas inquietas y apasionadas por la tecnología que no se conforman con imaginar, sino que deciden poner en práctica ideas nuevas sobre el uso de la tecnología. No se trata tanto de hacer grandes y nuevos descubrimientos como de aplicar de una forma original y siempre sorprendente la tecnología disponible, en un terreno entre el arte y la ciencia, con una actitud de gran creatividad.



Los objetos con los que frecuentemente tropezamos en ellas son impresoras 3D, cortadoras láser, microprocesadores Arduino usados de las formas más inverosímiles o robots de diferentes hechuras y tamaños.

En 2013, se han sumado a la iniciativa dos ciudades españolas: Barcelona (29 de junio) y Bilbao (20 y 21 julio). Estos eventos se celebraron en nuestro país con un gran éxito de público y han tenido un amplio eco en la prensa. Esperamos que este éxito anime no ya a su consolidación sino incluso a su ampliación para años venideros.

■ <http://delicious.com/rpla/raa826c>

Enlaces

■ Los enlaces relacionados con este artículo pueden encontrarse en las direcciones que figuran al final de cada texto