

Tecnología rebelde

RAFAEL L. BARDAJI

Director del Grupo de Estudios Estratégicos (GEES)

UNA de las características que más distinguen al hombre del resto de los animales es la utilización intensiva de instrumentos para conseguir sus fines. Ya para realizar mejor una vieja tarea, ya para conseguir hacer algo nuevo, la tecnología no ha dejado de sofisticarse en nuestras manos con el paso de los años.

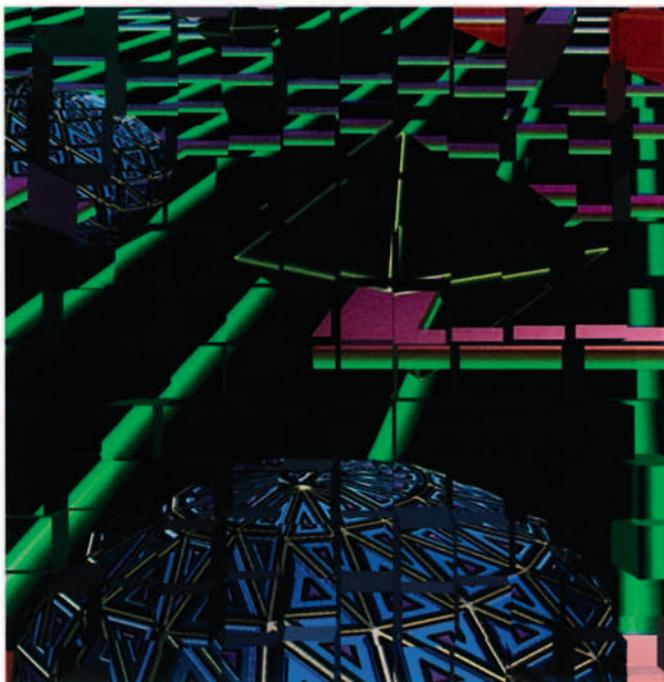
¿Alguien puede imaginar viajar con un ordenador de los años 50, que ocupaban una habitación mediana, pesaban toneladas y exigían auténticos científicos para entrar y salir de ellos? En poco más de tres décadas la miniaturización, mejores componentes y nuevas arquitecturas permiten llevar en un bolsillo más información que en la Enciclopedia Británica.

Ahora bien, el adelanto tecnológico no es inocuo. Conlleva cambios a veces insospechados. Piensese, simplemente, en el cambio de los hábitos culinarios con la introducción del microondas en sociedades relativamente tradicionales. Es más, la tecnología altamente sofisticada, a la vez que promesa y esperanza de un mundo mejor, también ha generado ancestrales temores y miedos. ¿Quién no recuerda al ordenador HAL de la película "2001, Una Odisea del Espacio", rebelándose contra sus creadores y planeando el asesinato de sus usuarios?

Ciertamente, estamos aún muy lejos del espantoso escenario de un mundo dominado por las máquinas, por muy inteligentes que puedan ser. Pero es innegable que el uso y la ex-

plotación masiva de la microinformática, de las comunicaciones electrónicas y de otros inventos, plantean problemas de seguridad al mismo tiempo que mejoran la vida de sus usuarios, paradójicamente.

Tal vez por ello, el Departamento de Defensa norteamericano iniciase este año la revisión del concepto de



guerra electrónica comunmente admitido, a saber, una agresión física contra los centros de Comunicaciones, Mando y Control, el famoso C3.

El grupo de trabajo organizado por la Junta de Jefes de Estado MAYor acabó ampliando el concepto a varias actividades, que podemos resumir básicamente en tres grandes apartados: 1) Guerra electrónica contra el C3; 2) Guerra basada en la inteligencia (todo tipo de operaciones basadas en el uso de los sistemas de información); y 3) Guerra psicológica (basada en

las comunicaciones y en la información con el objeto de modificar la percepción de los hechos).

Visto así, es cierto, nada parece nuevo, puesto que la guerra de la información es tan vieja como la guerra misma. Sin embargo, la novedad la aporta la tecnología hoy al uso y su progresiva diseminación.

LOS PELIGROS DEL GPS

El Sistema de Posicionamiento Global o GPS es un sistema, como todos sabemos, de navegación basado en una red espacial de satélites. Cuando el Pentágono lo hizo operativo en 1973 nunca pudo imaginar ni la popularidad que llegaría a alcanzar entre militares y civiles ni las connotaciones no deseadas que se avecinan.

El GPS estuvo operativo exclusivamente en manos de las fuerzas armadas durante 20 años, hasta que, en 1983, el Presidente Reagan, conmovido por el derribo del avión Coreano tristemente famoso, el KL007, decidiese ponerlo al alcance de usuarios civiles a través del Ministerio de Transporte.

Desde entonces, multitud de empresas tienen su negocio en torno a los receptores GPS. De hecho, los civiles superan con mucho al número de militares que lo utilizan.

Ahora bien, temerosos de dar a un enemigo un instrumento de precisión con el que apuntar a objetivos americanos, el pentágono ideó

dos sistemas en uno: un GPS codificado y de precisión (modelo P) y uno al que se le introducía un error arbitrario (modelo C/A) que redujera su fiabilidad a unos 100 metros en horizontal y unos 140 en vertical, frente a los 20 que era capaz de lograr.

El problema que no podían prever, es el afán de lograr más y la vertiginosa dinámica de la tecnología civil a partir de los años 80. Diversas compañías venden hoy una versión modificada del sistema estándar civil, bajo

la denominación DGPS, que permite a los usuarios conseguir altísimas precisiones (se anuncian errores de tan solo 5 metros) gracias a un complejo sistema de delimitar el error arbitrario. Incluso en los propios EEUU una compañía mantiene hoy operativo lo que llama el WADGPS, un sistema que mejora las prestaciones del DGPS.

Ni que decir tiene que en plena era de la proliferación de misiles de todo tipo y de atentados terroristas, el GPS permite incrementar la letalidad de cualquier acción. Si recordamos la precisa movilidad que le dio a las tropas en el desierto del Golfo, entenderemos como el GPS favorece, con mucho, a la ofensiva.

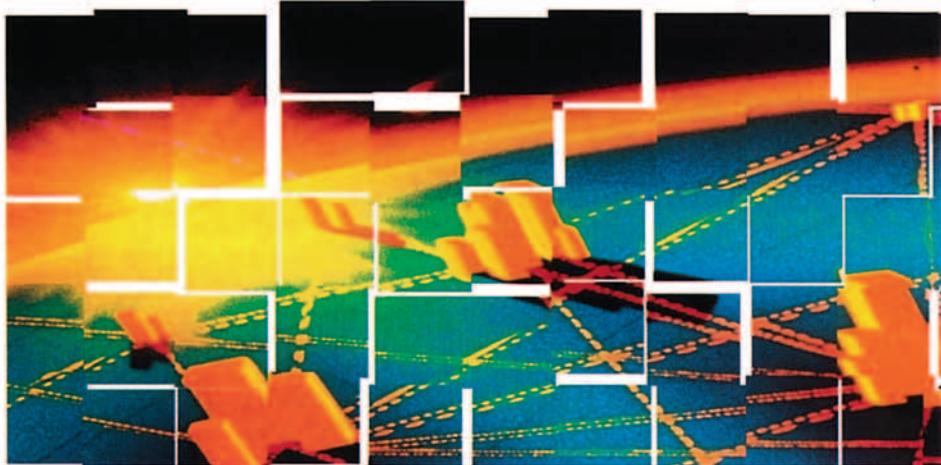
Es más, muchos expertos piensan que países de mediana capacidad pueden optar por usar el DGPS como sistema de guía de misiles de medio y largo alcance, particularmente los cruceros, a falta de un caro y complejo sistema como el Tercom empleado todavía en los Tomahawks.

El dilema actual para los Estados Unidos es enorme: El apetito empresarial obliga a mantener el libre acceso al GPS. Incluso hay quien recomienda la desaparición del modelo de Precisión en manos militares. Pero eso aumentaría la vulnerabilidad de sus instalaciones.

Por otro lado, la tecnología sobre la que se construye la red (satélites, estaciones en tierra y terminales) no es ya un monopolio americano. Varios países, incluido Japón pueden ponerla en marcha. Esto es, cualquier decisión contraria a las leyes del mercado (donde hay una gran avidez por los GPS) sería futil sin un acuerdo internacional previo.

IMAGENES DE ALTA RESOLUCION

El dilema del GPS es solo uno. El segundo viene dado por la difusión de imágenes por satélite de alta resolución. La observación militar del enemigo vía espacial no es un secreto desde finales de los 50. Ni tampoco es nuevo que el mercado civil e industrial utilizase sus propios satélites de observación: La NASA puso en órbita en 1972 su Landsat-1 y desde



entonces no ha dejado de mejorarse la resolución de la que era capaz ni ha dejado de crecer el parque de países con capacidades espaciales. La prueba es el Spot-2 con una resolución de 10 metros GSD desde principios de los 90.

Sin embargo lo que si era desconocido hasta fechas muy recientes era el acceso público a imágenes de alta resolución (máximo de 2 metros GSD) que permiten un análisis detallado y, en conjunción con otros medios (como el GPS) de sistemas de guía inquévocos.

La aparición en el mercado de imágenes normalmente limitadas en su uso a la inteligencia comenzó en 1992 cuando el gobierno de Rusia autorizase a dos de sus empresas (Sovinsputnik y Piroda) a vender imágenes de una resolución de 2 metros tomadas por el satélite KVR-1000. Desde entonces, es verdad, debido a causas y rivalidades internas, Rusia no ha saturado el mercado con sus fotos, pero sí ha conseguido algo inesperado: la constitución de un auténtico mercado de la imagen de alta resolución.

De hecho, el Presidente americano Bill Clinton decidiría en 1994 un cambio de política y con su directiva presidencial 23 apoyaría a los grupos industriales civiles americanos a participar en la obtención y manejo de imágenes de alta resolución. Su idea era que se trataba de un mercado comercial de potenciales beneficios de los que no debían hurtarse los industriales estadounidenses.

Por su parte Francia tampoco pare-

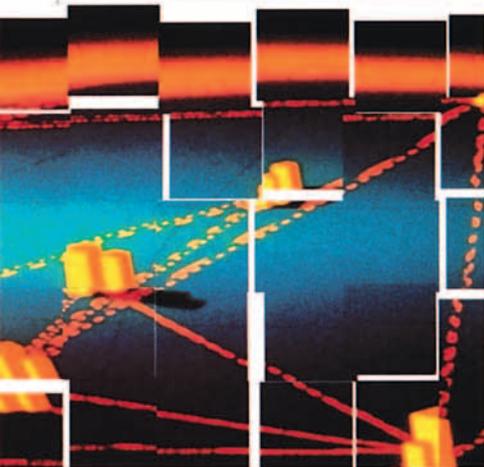
ce querer quedarse al margen de este lucrativo negocio. A sus recelos tradicionales le ha venido a sustituir la política de un nuevo presidente, inclinado a entrar en el mercado de la imagen. En cualquier caso, incapaz financieramente de dar el salto de la presente generación del Helios al Helios 2 y, sobre todo, al Osiris, lo que en realidad le interesa a Francia es la posibilidad de exportar no sus imágenes, sino sus satélites.

Israel y Japón aún no se han decidido a seguir esta carrera y observan simplemente el fenómeno, pero qué duda cabe de que lo harán si ven intereses en ello.

Que la difusión de imágenes tenga efectos positivos o perjudiciales dependerá de varios factores circunstanciales. Conocer los despliegues, las instalaciones, etc. de un vecino es conocer sus puntos fuertes y sus debilidades, lo cual puede servir tanto como para mejorar la defensa propia como para lanzar una ofensiva más eficaz. Pero claramente vuelve al mundo más expuesto, sobre todo en regiones y zonas con disputas territoriales abiertas.

EL LABERINTO DE INTERNET

Pero tal vez no haya nada más revolucionario estratégicamente en estos momentos que ese mundo incomprendible y sin centro que es el Internet. Creado también por el pentágono a finales de los 70 a fin de evitar que sus C2 fuesen decapitados en un ataque nuclear sorpresa por parte de la



URSS, hoy en día la red ha escapado totalmente de sus manos y se expande como el universo, permeando todo tipo de instituciones. La Moncloa tiene abierta una ventana informativa y la Generalitat ofrece a quien lo quiera la historia de las instituciones catalanas y comentarios de la política autonómica actual.

Internet cambia radicalmente el mundo y sus servicios, abriéndolo a

las manos del usuario, cómodamente sentado frente a la pantalla de su ordenador personal.

Ya hemos visto en películas, como Juegos de Guerra, lo que un Hacker, un pirata informático, puede hacer voluntaria o involuntariamente, penetrar en las redes informáticas mejor guardadas del mundo. No hace mucho un periodista pudo infiltrarse a su vez en los ordenadores de los servicios secretos británicos, robando innumerables teléfonos.

Ahora bien, hasta ahora el fantasma se reducía a un niño o loco por la informática que se devanaba los sesos para romper un código. Ninguna otra consecuencia se había extraído. Sin embargo, en la actualidad, los expertos temen una auténtica guerra en la red, para empezar el uso de técnicas, como virus, para degradar o destruir información de los sistemas militares o civiles que afecten a la seguridad nacional. Recordemos el rumor sostenido durante la guerra del Golfo de que un ordenador aparentemente robado a un oficial inglés, en realidad

portaba un virus que ralentizaba los procesos de los ordenadores iraquíes. Lo contrario también se vuelve factible.

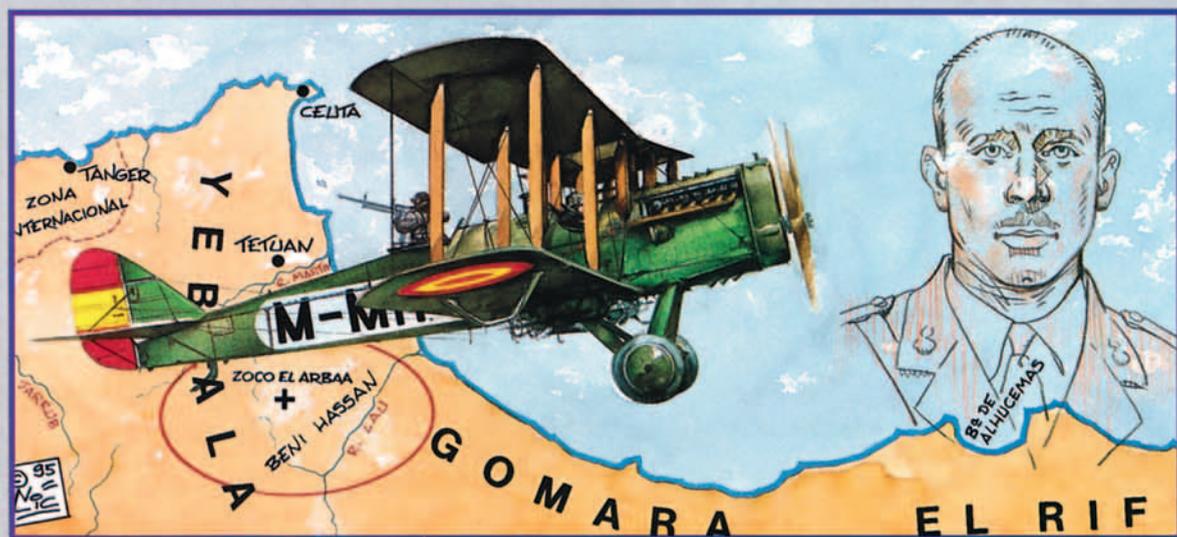
Pero además, Internet, la red, es un espacio virtual donde fluyen millones de informaciones y que se puede convertir facilísimamente en el terreno de batalla de una guerra de propaganda y desinformación. Y no se trata de imaginar campaña de desprestigio, sino una hábil manipulación de los indicadores económicos de una empresa clave de un país. ¿Por qué no?

A finales del año pasado, el Pentágono patrocinó un juego de guerra de la información. El escenario era un plan estratégico de agresión informativa e informática contra los EEUU por parte de un país tecnológicamente avanzado. Los miembros del equipo de Estados Unidos idearon una defensa contra millones de piratas informáticos, pero su plan fracasó: el agresor había decidido por una manipulación informativa vía Internet con destino a todos los servicios de información del país. ■

Efemérides aeronáuticas

SEPTIEMBRE. El día 25 de este mes del año 1924, moría uno de los más prometedores aviadores militares españoles.

Con muy mal tiempo, y ante la urgente necesidad de apoyo a las columnas que en Zoco el Arbáa de Beni Hasán trataban de retirar las guarniciones de varias posiciones, el capitán José Carrillo Durán, Jefe del 3º Grupo De



Havilland, decidió la salida de éste, realizándose el servicio por parejas, haciéndolo él solo.

Próximo a la posición de El Fondalillo, resultó herido por el fuego de fusilería de los moros, y derribado, estallando las bombas y muriendo él y su bombardero, suboficial José Amat Amat.

Larus Barbatus