ieee.es
Instituto Español de Estudios Estratégicos

Documento
Opinión

81/2014 24 de julio de 2014

*Fernando Ruiz Domínguez**

NEO-GEOESTRATEGIA SIN GNSS

NEO-GEOESTRATEGIA SIN GNSS

Resumen:

Dos décadas después de estar disponible la señal civil del *U.S. Global Positioning System* (GPS) conviene hacer una rápida evaluación de lo que ha supuesto en algunos aspectos su implantación. De esta manera se puede ver junto con la aparición en escena de GALILEO, BEIDOU/COMPASS, GLONASS, IRNS, etc., hacia dónde evoluciona la geolocalización y navegación por satélite y lo que ello puede implicar en cada momento.

Abstract:

Two decades after the civil signal available from U.S. Global Positioning System (GPS) should make a quick assessment of what has been assumed in some respects its implementation. This way you can see along with the appearance on the scene of GALILEO, BEIDOU / COMPASS, GLONASS, IRNSS, etc., where evolving geolocation and satellite navigation and this may involve at all times.

Palabras clave:

Global Navigation Satellite System (GNSS), *U.S. Global Positioning System* (GPS), GALILEO, BEIDOU/COMPASS, GLONASS, Indian Regional Navigation Satellite System (IRNSS), informe Volpe, sectores estratégicos, vulnerabilidades, jamming, meaconing, spoofing.

Keywords:

Global Navigation Satellite System (GNSS), U.S. Global Positioning System (GPS), GALILEO, BEIDOU / COMPASS, GLONASS, Indian Regional Navigation Satellite System (IRNSS), Volpe report, strategic sectors, vulnerabilities, jamming, meaconing, spoofing.

INTRODUCCIÓN

El *Global Navigation Satellite System* (GNSS) constituye un sistema con cobertura global que proporciona información precisa y fiable sobre el tiempo y la localización espacial (longitud, latitud y altitud) al dispositivo receptor de las señales emitidas por un grupo de satélites en órbita alrededor de la Tierra.

Los elementos clave de todo el sistema son: Los satélites que emiten las señales de radio-frecuencia; las estaciones ubicadas en diferentes puntos del planeta para el seguimiento y control de esas señales; y los dispositivos receptores de las mismas.

De esta manera el conjunto constituye una clara ayuda para:

La navegación por tierra, mar y aire;

La búsqueda y el rescate por servicios de emergencias;

La sincronización de las operaciones financieras y bancarias;

El correcto control de la producción energética;

El funcionamiento de Internet;

La agricultura y pesca de precisión;

El guiado de misiles; Etc.

En definitiva, todo tipo de actividades que, con el único límite de la imaginación humana, han afectado y afectarán a la forma en que vivimos, nos comunicamos y viajamos.

Algunos sistemas de posicionamiento vía satélite solo tienen cobertura regional y por lo tanto no son GNSS pero, dado el interés estratégico que suponen, también conviene tenerlos en cuenta.

Habría que añadir como eje del asunto que, a diferencia de lo que ocurre con las señales militares de los GNSS (fuertemente encriptadas y de uso restringido), con las señales civiles de los GNSS resulta todo lo contrario, lo cual genera una serie de cuestiones con sus correspondientes puntos de encuentro y desencuentro entre las grandes potencias actoras.

Es obvio que cada uno lucha y luchará por sus propios intereses pero al final - dado que vivimos en un mundo en el que el fenómeno de la globalización trasciende fronteras y las sinergias y/o el efecto mariposa están a la orden del día – no habrá que perder de vista antes de que sea demasiado tarde, lo que los demás están haciendo, cómo lo están desarrollando y para qué lo quieren.

POSICIÓN ACTUAL DE LOS ACTORES GUBERNAMENTALES IMPLICADOS

EE.UU. (GPS)

Como en tantos otros proyectos, el *Department of Defense* (DoD) de EE.UU. fue el primero en desarrollar en 1973 con 24 satélites un GNSS que se conoce como *US Global Positioning System* o simplemente GPS. Dicho sistema estuvo totalmente operativo en 1994 y con sus correspondientes actualizaciones y mejoras es el que a día de hoy se utiliza y mantiene como tal, aunque en un futuro el número de satélites se podría aumentar hasta 30[1].

Es el que más implantado se encuentra y por lo tanto el más expuesto a vulnerabilidades dada además su longevidad y amplio conocimiento público de su arquitectura técnica.

Los principales problemas que ha planteado su uso por el resto de países son:

La dependencia: Las potencias amigas o enemigas que no han sido capaces de desarrollar una tecnología similar y explotarla, dependen totalmente de su GPS y por lo tanto están expuestas a sus vulnerabilidades;

La precisión: Ya que su versión abierta para uso civil es mucho menos precisa[2] que la de uso militar.

Unión Europea (UE): GALILEO

Por su parte, la UE pretende poner en funcionamiento durante 2014 su propio GNSS llamado GALILEO. Un sistema operado a nivel civil que contará con 30 satélites (27 principales y 3 de repuesto) y que - entre otras cuestiones - por su distribución y órbita proporcionarán una mejor cobertura y fiabilidad que el operado por EE.UU.

Su implantación está siendo más problemática de lo esperado[3] debido a la burocracia, la coordinación presupuestaria y los diferentes puntos de vista de los miembros de la UE que ha habido que consensuar en numerosas ocasiones.

Contará con cuatro servicios distintos como:

Un servicio abierto, libre y gratuito para el público en general;

Un servicio con verificación de usuario, para funciones de rescate y salvamento;

Dos servicios encriptados siendo uno de ellos para usos gubernamentales y el otro para usos comerciales.

Por otra parte, uno de los aspectos más significativos de la apuesta europea se encuentra en el campo del desarrollo de las aplicaciones informáticas para dispositivos móviles –conocidas

---

1 United States Government Accountability Office (GAO), *Global Positioning System: A Comprehensive Assessment of Potential Options and Related Costs is Needed*, September 2013. Disponible en http://www.gao.gov/assets/660/657507.pdf Fecha de consulta 04.11.2013.

2 Unos 20 metros de diferencia para el uso civil.

3 Se esperaba que hubiera estado operativo en 2008 pero ha sido pospuesto hasta 2014.

como Apps- que tengan como base el uso de la señal GNSS, ya que el pasado mes de abril terminó el plazo para presentar los diferentes proyectos del *EGNSS Applications*[4]. Se trata de un subproyecto del Programa *Horizon 2020* que cuenta con un presupuesto inicial de 38 millones de euros y que se incrementará hasta los 70 millones durante el periodo 2014-2020.

República Popular de China: BEIDOU y COMPASS

BEIDOU.

Es un sistema regional que proporciona cobertura a China y países limítrofes o próximos.

Durante 2013 China consiguió firmar acuerdos públicos con al menos Pakistán, Tailandia, Laos y Brunei para instalar en dichos países estaciones de seguimiento de sus satélites lo que la asegura una posición estratégica en la zona de Asia-Pacífico[5].

COMPASS.

Dará cobertura global (GNSS) cuando al parecer en 2020 esté operativo. Ofertará dos tipos de servicios: uno militar y otro civil, por lo que en los próximos años China posiblemente buscará socios en Latinoamérica y África donde poder instalar algunas estaciones adicionales de seguimiento y control de las señales de sus satélites.

Federación Rusa: GLONASS

De origen militar, este GNSS fue desarrollado en 1976 en la URSS llegando a estar plenamente operativo en 1995. Aunque inicialmente su cobertura fue a nivel regional y durante algún tiempo no estuvo operativo por motivos políticos[6], en la actualidad es -junto al de EE.UU.-, uno de los dos únicos sistemas globales en servicio.

Está operado militarmente por la Federación Rusa, de la que pasó a depender en el año 2000.

En los dos últimos años ha recibido un fuerte apoyo gubernamental para que dos importantes sectores comerciales como son la telefonía móvil[7] y la automoción fabriquen productos que sean compatibles además de con el GPS con su GLONASS.

---

[4] En campos relacionados con el transporte, marítimo, agricultura, energía y cambio climático. European GNSS Service Centre. Horizon 2020 - *Call for "Applications in Satellite Navigation - Galileo".* Disponible en http://www.gsc-europa.eu/gnss-markets/rd/horizon-2020

[5] China Daily, Beidou set to spread its wings in region, 18.05.2013. Disponible en http://usa.chinadaily.com.cn/china/2013-05/18/content_16508494.htm Fecha de consulta 04.11.2013.

[6] Desaparición de la URSS.

[7] 152 modelos de *smartphones* de los principales fabricantes mundiales (Apple, Sony, Samsung, Nokia, Motorola, etc.) -a fecha 04.11.2013- soportaban el sistema GLONASS. Disponible en http://www.phonearena.com/phones/full/page/2/?ft=2&f#/phones/full/?f[397][]=1659

India: Indian Regional Navigation Satellite System (IRNSS)

Se trata de un sistema regional de posicionamiento que India ha decidido poner en funcionamiento para 2015 debido, principalmente, a su status geopolítico en la zona y a su conocido interés por no quedarse aislada en caso de hostilidades.

Tendrá dos servicios: uno de tipo militar y otro civil.

DIFICULTADES ECONÓMICAS[8]

Cualquier retraso en el desarrollo, implantación o mantenimiento de una red GNSS - o de posicionamiento a nivel regional- supone, por regla general, un incremento presupuestario. El problema viene cuando estos costes se disparan durante un largo periodo de tiempo – como en el programa GALILEO - .

En el caso de EE.UU., y teniendo en cuenta solo las cifras del año 2012, esto supuso un incremento del 15% (70 millones de $). Para paliar dicho problema y reducir de forma significativa las progresivas subidas extra-presupuestarias a tan solo un incremento de un 7% sobre el presupuesto del 2013 se han planteado en EE.UU. diversas soluciones tales como:

No dotar a los nuevos satélites de la red GPS con los costosos sensores de detonación nuclear;

Firmar contratos para el lanzamiento de varios satélites y no de uno solo;

Firmar acuerdos con empresas civiles para que ellos pongan en órbita nuevos satélites propios y que sea el *DoD* el que pueda usarlos en régimen de *leasing;*

Reducir peso y volumen de los satélites para maximizar el espacio de carga útil en los lanzamientos espaciales.

Es decir, toda una carrera contra-reloj para posicionarse firmemente en un mercado que evoluciona constantemente y en el que cualquier error de cálculo supone no solo un daño emergente para las arcas estatales sino un lucro cesante para la de los ciudadanos y, por ende, para el propio gobierno.

[8] Aviation Week citando a la agencia Reuters, *US Forces Eyes Changes to National Security Satellite Programs*, 18.01.2013. Disponible en http://www.aviationweek.com/Article.aspx?id=/article-xml/awx_01_18_2013_p0-538541.xml&p=1 Fecha de consulta 04.11.2013.

EL CÚMULO DE FACTORES ASOCIADOS QUE AFECTAN A LOS GNSS

Punto de partida

Dos son los hechos claves que marcan el punto de partida para empezar a tomar medidas sobre las vulnerabilidades y el uso contrario a los intereses, de la señal de posicionamiento por satélite:

- Las vulnerabilidades: El 10 de septiembre de 2001 se publica el conocido como Informe Volpe[9] que evalúa la vulnerabilidad de la infraestructura de transporte que se basa en la señal y dispositivos GPS;

- El uso contrario a los intereses: El 11 de septiembre de 2001 dos aviones de transporte de pasajeros son estrellados contra el *World Trade Center* de Nueva York; otro contra el Pentágono en Washington D.C; y otro más contra el suelo en Pennsylvania al fallar su objetivo. Un quinto avión debería haberse estrellado contra la Casa Blanca en Washington D.C. - la cual se habría localizado por los terroristas mediante señal GPS[10] dada la dificultad de visualizarlo desde el aire, según declaró otro de ellos, Abu Zubaydah -.

Problemas climatológicos

Limitaciones del sistema.

Los problemas a nivel terrestre que se pueden producir y que afectan al retraso de la recepción de las microondas emitidas por los satélites son los siguientes:

Por un lado tenemos el generado en la ionosfera (la dispersión[11] [12]);

Y por el otro el generado en la troposfera (la humedad).

Ambos originan constantes líneas de investigación – al igual que lo que sucede con el estudio de los efectos de las explosiones en la corona solar sobre las señales de los satélites[13] - por lo que la comunidad científica tiene en todo lo que rodea técnicamente a los GNSS, uno de los grandes pilares de financiación económica, así como de desarrollo y promoción a nivel profesional.

---

9 VOLPE, John A, *Vulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning System*, Final Report, 29.08.2001, National Transportation Systems Center. Página 5. Disponible en http://www.navcen.uscg.gov/pdf/vulnerability_assess_2001.pdf Fecha de consulta 04.11.2013.

10 U.S. Department of Justice. *United States of America versus Zacarias Moussaoui*, Overt Acts 77. Disponible en http://www.justice.gov/ag/moussaouiindictment.htm Fecha de consulta 04.11.2013.

11 Cambia de forma lenta y se puede prever con antelación.

12 Error corregido en la versión militar.

13 IIP Digital, *NASA Heading Straight for Sun*, junio 2013. Disponible en http://iipdigital.usembassy.gov/st/english/inbrief/2013/06/20130611275917.html#axzz2jPXDL400 Fecha de consulta 04-11-13.

Desastres Naturales

En este apartado se debe tener en cuenta lo que puede suponer la destrucción -por fenómenos climatológicos extremos- de las infraestructuras que soportan y mantienen los GNSS. Tan solo hay que echar un vistazo -y por simple comparación- a los daños provocados por el huracán Katrina en tres estados de EE.UU.:

Tres millones de usuarios sin línea telefónica;

Treinta y ocho Centros de Servicios de Emergencias fuera de servicio;

Mil torres de telefonía móvil destruidas.

Fenómenos provocados intencionadamente

Indudablemente algunos fenómenos climatológicos también se pueden originar y en cierta medida controlar por la acción intencionada del ser humano. Su uso potencial está ahí y es otro factor más a tener en cuenta a la hora de diseñar las instalaciones donde se albergan los centros de control y mantenimiento de los GNSS.

Negligencias

No es ni el primer ni el último caso en el que, por ejemplo, los propietarios de vehículos deciden oscurecer las lunas de los mismos. La mayoría desconoce que algunas de las láminas adhesivas de *polyester* con las que se realiza esa operación contienen partículas metálicas[14] que pueden interferir las señales de los GNSS que se lleven a bordo. Esta cuestión puede generar, cuanto menos: constantes incomodidades; gastos por visitas innecesarias a talleres y servicios técnicos; y, en algún caso, incluso un accidente al tratar de manipular el conductor - con el vehículo en marcha - el receptor de señales GNSS que se encuentra fallando.

Atentados terroristas

Por su clara similitud, tenemos el caso de la destrucción de un centro de telecomunicaciones ubicado en el conocido *World Trade Center* neoyorkino durante los ataques del 11-S que afectó a cuatro millones de circuitos de datos. De esta o similares formas, los ataques sobre alguno de los diferentes centros terrestres de control o gestión de GNSS distribuidos por el planeta, pueden tener consecuencias no solo sobre dicho centro y sus operadores en sí, sino además sobre la monitorización y corrección de los datos enviados por los satélites[15]. A finales de 2011 el *Department of Homeland Securit*y (DHS) de EE.UU. examinó en detalle, de

[14] 3M, *Color Stable Automotive Window Films*. Disponible en http://solutions.3m.com/wps/portal/3M/en_US/Window_Film/Solutions/Markets-Products/Automotive/Color_Stable_Automotive_Films/ Fecha de consulta 04.11.2013.

[15] Si bien estos centros terrestres no son imprescindibles para el funcionamiento instantáneo del sistema.

entre todas las infraestructuras críticas del país, las siguientes cuatro[16] por su especial vulnerabilidad y en relación a su extrema dependencia de las señales de su GPS:

Comunicaciones;

Servicios de Emergencias;

Energía;

Sistemas de Transporte.

Por otra parte, resulta significativo que en EE.UU. la posesión de un dispositivo receptor de las señales GPS[17] sea considerado - en conjunción con otros elementos y factores - como un factor indiciario para que un individuo sea considerado como sospechoso de ser un terrorista. Así, por ejemplo, se entiende que se pueden marcar con precisión determinados objetivos, vías de ataque o escape, etc.

Tecnologías compartidas

El caso de la República Popular de China y la UE ha sido el más palmario ya que a finales de 2004 este país firmó un acuerdo con la UE para participar económicamente[18] en el sistema GALILEO. A continuación, en 2005, la UE expuso a varias empresas chinas su interés concreto por el desarrollo de diferentes aplicaciones comerciales para el programa GALILEO. Es en 2006 cuando el país asiático abandona el proyecto europeo - forzado por la política de seguridad e independencia tecnológica de la UE- e inicia en solitario el desarrollo de sus propios proyectos de geolocalización vía satélite (el regional -conocido como BEIDOU- y el global – conocido como COMPASS -).

Evidentemente esta situación generó no pocas disensiones en el seno de la UE entre los países que inicialmente abogaban por negar la trasferencia de tecnología a China y por los que se la quisieron facilitar sin ningún tipo de cortapisas a cambio de una financiación a corto plazo para el proyecto, de la que se carecía a nivel europeo.

¿Alianzas estratégicas?

En estos momentos en los que al parecer el prolongado espionaje entre países aliados parece estar otra vez de forma pública de moda, cobra interés la posición de dos de los grandes actores en el tema en cuestión. Así por un lado tenemos a EE.UU. con su dualidad de GNSS (el GPS militar/civil) y por otra a la UE con su GNSS operado civilmente (GALILEO). Si a esto le añadimos el peso específico de las fechas – todo 2014- , el papel concreto de

[16] Ibid, *National Risk Estimate: Risks to US. Critical Infrastructure from Global Positioning System Disruptions*. 2011. Disponible en http://www.gps.gov/news/2013/06/2013-06-NRE-fact-sheet.pdf Fecha de consulta 01.08.2013.

[17] Ejemplo: *New York State Law Enforcement Terrorism Indicators Reference Card*, Unusual items in vehicle/residence, Global Positioning Satellite (GPS) unit. Fecha de consulta 04.11.2013.

[18] Aportación china de 200 millones de euros sobre el total de 3.200 millones de euros que se supone costará el proyecto GALILEO.

Alemania[19] [20]dentro del proyecto europeo, así como las consabidas reticencias iniciales de EEUU[21] al desarrollo de dicho proyecto, entonces la tensión está servida.

La exactitud o inexactitud

Tan solo hay que recordar algunos incidentes ocurridos en cualquier lugar del planeta para darse cuenta de la importancia a este nivel que supone la exactitud o inexactitud del sistema de señales de GNSS utilizando todos el mismo sistema de uso generalizado hasta ahora (el GPS), así que si se pone en escena la combinación del resto de GNSS vistos anteriormente – o las versiones regionales - , la cuestión se puede complicar exponencialmente pese a la interoperabilidad o complementación de algunos de los sistemas con otros a nivel de usuario.

Y es que cuestiones como por ejemplo la altura máxima de una montaña limítrofe y su pertenencia a un país u otro pueden provocar todo tipo de reacciones -incluso de organismos públicos- ya sea el incidente real o ficticio[22] y siempre con consecuencias imprevisibles como se han visto en tantas ocasiones a lo largo de la historia.

Igualmente, veinte metros de error en una señal de GPS pueden ser más o menos importantes según para qué actividades. Esos metros pueden suponer una masa ingente de agua dulce la cual es crucial para -por ejemplo – el sector agrícola de un país, región, o particular. De esta manera, esa precisión y fiabilidad de la señal GNSS puede generar a su vez nuevos conflictos entre los que se amparan en las antiguas mediciones basadas en señales menos precisas y los que quieren recuperar sus derechos basados en las nuevas mediciones.

Además, la mayoría de la población desconoce que actualmente se dispone de la señal GPS para uso civil a raíz de un grave incidente durante la guerra fría. Se trata del avión de pasajeros 747-200 en su vuelo Korean Air 007 que fue derribado el 31-08-1983 por cazas de la Fuerza Aérea de la extinta URSS al haber entrado el primero - por error de posición - en el territorio de los segundos.

En enero de 1993 el *Department of Transport* (DOT) de EE.UU. y su DoD ya habían firmado un Memorando de Acuerdo[23] para el uso civil de la señal GPS designada, pero tras el grave

---

[19] Junto con Italia y la República Checa, Alemania cuenta con uno de los centros de control y gestión del sistema GALILEO.

[20] Múnich (Alemania) ha sido de forma habitual la ciudad sede de las reuniones de alto nivel en relación al proyecto GALILEO. Disponible en http://www.munich-satellite-navigation-summit.org/Summit2009/

[21] BBC News, *US warns against european satellite system*. 18.12.2001. Disponible en http://news.bbc.co.uk/2/hi/europe/1718125.stm Fecha de consulta 04.11.2013.

[22] Ösis klauen Zugspitze, Robo ficticio de 25 cm del pico más alto de Alemania a manos de cuatro austriacos que presuntamente accedieron a territorio alemán desde Austria -por un punto no autorizado-. El Zugspitze con sus 2962,06 metros es la montaña de los Alpes que separa Austria de Alemania. Video de una agencia de publicidad visto por 125.479 personas desde el 24.10.2013 hasta el 07.11.2013 y por el que tuvo que intervenir la policía de la región de Garmisch-Partenkirchen en el Estado Libre de Baviera (Alemania). Disponible en http://www.youtube.com/watch?v=e0Ds2lTItKM

[23] VOLPE, John A, *Vulnerability Assessment of the Transportation Infrastructure Relying on the Global*

conflicto diplomático del avión derribado y por decisión del entonces presidente del país, Ronald Reagan, fue en diciembre de ese mismo año cuando finalmente dicha señal estuvo operativa para todo el mundo y de forma gratuita.

Conflictos armados

Desconexión del GNSS.

Entre las capacidades estratégicas asociadas al GPS - que han contribuido al desarrollo de otras alternativas como el desarrollo de nuevos GNSS o sistemas regionales de posicionamiento por satélite- se encuentra el hecho de que dicho servicio puede ser desactivado por el proveedor en caso de conflicto armado[24], lo cual supone claramente la posibilidad de mermar seriamente - entre otras – las capacidades logísticas y de ataque[25] del enemigo.

Por lo tanto, algo que originariamente tenía un gran valor defensivo para EEUU se puede convertir - y va camino de serlo – en el ocaso de un monopolio de las señales GNSS.

Destrucción de satélites o estaciones de seguimiento y control de la señal GNSS.

Queda lejos el programa de la Strategic Defense Iniciative conocido como «Guerra de las Galaxias» que durante el mandato del presidente de EE.UU., Ronald Reagan, estuvo tan en boga. Aunque éste se centraba más en la destrucción de misiles, igualmente contemplaba la eliminación expeditiva de satélites en caso de ser necesario. A día de hoy esto último sigue siendo factible pero, seguramente, puede resultar más sutil - en los tiempos que corren- la estrategia de, o bien bloquear en el espacio las señales de los satélites enemigos que facilitan el posicionamiento global de los interesados, o bien la de inutilizar las estaciones en tierra de seguimiento y control de la señal GNSS.

Para ello se podrían emplear armas del tipo *Electromagnetic Pulse* (EMP) *Weapon* y *High-Powered Microwave* (HPM) *Weapon*. Tanto las armas de pulso electromagnético como las de microondas de alta potencia inutilizan los equipos electrónicos y su desarrollo secreto no permite determinar con precisión el estado actual y capacidades operativas de los actores gubernamentales. Basta decir que en el informe desclasificado en el año 2010 por el DoD[26] queda claro que al menos EE.UU., Rusia, China y Alemania tienen dichas capacidades y que uno de los posibles escenarios de uso estaría en Taiwán.

Positioning System, Final Report, 29.08.2001, National Transportation Systems Center. Página 5. Disponible en http://www.navcen.uscg.gov/pdf/vulnerability_assess_2001.pdf Fecha de consulta 04.11.2013.

[24] Se ha hablado ampliamente de que durante las guerras de Kuwait e Iraq se produjeron estos hechos, pero oficialmente EE.UU. no lo ha reconocido.

GPS.gov, *Has the United States ever turned off GPS for military purposes?* 2013. Disponible en http://www.gps.gov/support/faq/#jamming Fecha de consulta 04.01.2013,

[25] Para evitar el uso de estos dispositivos receptores como sistemas precisos de guiado de armas.

[26] National Ground Intelligence Center, *China: Medical research on Bio-Effects on Electromagnetic Pulse and High-Power Micro-Wave Radiation.* 17.08.2005. Disponible en http://media.washtimes.com/media/misc/2011/07/22/ngic-emp.pdf Fecha de consulta 04.11.2013.

El atractivo económico

Resulta obvia la porción del mercado comercial que se encuentra en juego pues existen ingentes cantidades de dinero que circulan entorno a los GNSS, ya sea –entre otras- durante las fases de diseño, desarrollo, fabricación, distribución, almacenamiento o venta de:

Dispositivos de captación de las señales (comercializados individualmente o como parte integrante de otros);

Componentes para dichos dispositivos;

Aplicaciones comerciales;

Actividades y empresas que no existirían sin los mismos; Etc.

El bajo costo de los dispositivos receptores y la amplia disponibilidad de la cobertura de la señal a cielo abierto hacen que no se haya encontrado techo al desarrollo de las aplicaciones civiles de esta tecnología de origen militar.

Una cifra que puede dar una idea del volumen de negocio de los GNSS es que por ejemplo BEIDOU -pese a que solo funcionará a nivel regional-, puede suponer en 2015 y tan solo en China, 37 billones de dólares[27].

Por si fuera ya poco y a la vista de los nuevos desarrollos de los diferentes sistemas de posicionamiento -regionales o globales- el nerviosismo crece en función del nivel del flujo de información y dirección de esta – la que se facilita por parte de los operadores de GNSS a los fabricantes de dispositivos y aplicaciones-. En el caso de EE.UU. ha habido una clara y creciente preocupación gubernamental por dichos motivos al entender que los retrasos en proporcionar información sobre determinadas características de GALILEO -por parte de la *European Commission* (EC)- podrían suponer un trato discriminatorio para las empresas norteamericanas y en favor de las de otros países[28].

De todo este planteamiento económico queda clara la tendencia entre unos y otros a ir recortando poco a poco el volumen de negocio del monopolio norteamericano.

Los servicios inalámbricos de telefonía 4G y transmisión de datos y la navegación aérea

La saturación producida por el número de radio-frecuencias comerciales en uso y la proximidad de unas con otras y sus posible interferencias está generando un problema desconocido hasta ahora y que tiene su origen en EE.UU.

La empresa *LightSquared* estaba instalando una red terrestre inalámbrica para la comercialización a particulares de los más avanzados servicios de telefonía 4G y transmisión

[27] The Economic Times, *Pakistan may opt for Chinese navigation system*. 18.05.2013. Disponible en http://articles.economictimes.indiatimes.com/2013-05-18/news/39354765_1_beidou-china-satellite-navigation-office-navigation-system Fecha de consulta 04.11.2013.

[28] USTR Report to Congress on U.S. Equipment Industry Access to the Galileo Program and Markets. 2009. Disponible en http://www.ustr.gov/webfm_send/1209 Fecha de consulta 04.11.2013.

de datos. Dicha red estaría en contacto -mediante radio-frecuencia – con sus propios satélites de comunicaciones. Sin embargo y a raíz de las diversas denuncias recibidas por la *Federal Communication Commision* (FCC) ésta ha llegado a revocar temporalmente la licencia para el uso terrestre de la frecuencia asignada hasta que se realicen diferentes estudios. Entre los mismos se encuentran los de la propia interesada que ha llegado a reconocer -aunque sea de manera remota- que existe dicha posibilidad de interferencias en determinados casos[29]. De esta manera y junto con los datos obtenidos tras las consultas públicas[30] pertinentes se tomará una decisión al respecto.

Las implicaciones son serias y claras pues debido a lo débil que es la señal civil del GPS y la proximidad de la misma a la frecuencia que pretende seguir utilizando *LightSquared*, los receptores civiles de GPS podrían captar solo la más fuerte -y utilizada por *LightSquared*- y por consiguiente llegarse a sobrecargar o saturar. Es decir, en definitiva, y para evitar dicho problema, se estaría obligando a los particulares a actualizar sus dispositivos receptores de señales GPS -con el consiguiente coste económico- o a prescindir de algunas de sus características.

Por otra parte, el asunto de las interferencias se puede complicar exponencialmente si el elemento afectado se encuentra abordo de un avión civil en vuelo. En este sentido hay trabajos de investigación[31] que muestran que las primeras versiones de los futuros sistemas de ayuda a la navegación aérea basados en señales GNSS – en este caso de la versión civil del GPS y del servicio de emisión en abierto, libre y gratuito de GALILEO –, podrían verse afectadas por otros sistemas de radio-navegación aeronáutica (ARNS). Así, tanto el Equipo de Medición de Distancia (MDE), como el de uso militar para la Navegación Aérea Táctica (TACAN) – los cuales operan con transpondedores, ubicados generalmente en las cercanías de los aeropuertos-, al emitir las señales desde sus estaciones -para ser captadas por sus receptores instalados en las aeronaves correspondientes-, podrían dañar al mismo tiempo los receptores de las mencionadas señales GNSS de otros aparatos en vuelo[32].

---

[29] Federal Communications Commission, *LightSquared Assessment of Uplinks in the 1626.5-1660.5 MHz band,* 15.07.2013. Disponible en http://apps.fcc.gov/ecfs/comment/view?id=6017458747 Fecha de consulta 04.11.2013.

[30] Ibid, *Comment Sought on LightSquared Subsidiary LLC Ex Parte Filing*. 07.08.2013. Disponible en http://transition.fcc.gov/Daily_Releases/Daily_Business/2013/db0807/DA-13-1717A1.pdf Fecha de consulta 04.11.2013.

[31] MUSUMECI, Luciano, DOVIS, Fabio, *Use of the Wavelet Transform for Interference Detection and Mitigation in Global Navigation Satellite Systems*, Hindawi Publishing Corporation, International Journal of Navigation and Observation, Volume 2014, Article ID 262186, página 2.

[32] En las últimas pruebas realizadas se demostró que esto puede ocurrirle a una aeronave que sobrevuele a 40.000 pies de altura, el área del aeropuerto de Frankfurt.

ATACAR LA SEÑAL GNSS

Interferencias electromagnéticas[33]

A veces y con elementos tan simples como los pre-amplificadores de una antena de televisión se puede lograr interrumpir la captación de la señal civil de un GNSS, lo que supone graves problemas en ciudades densamente pobladas y en las que es prácticamente imposible controlar de forma eficaz la correcta instalación de este tipo de aparatos o similares.

Jamming

Los dispositivos específicos que bloquean la captación de la señal emitida por los satélites de un sistema GNSS están a la orden del día y la actividad que realizan es conocida como *jamming*.

No hay más que navegar por Internet para darse cuenta de la cantidad de modelos que enmascaran la señal y sus usos posibles, estando entre los mismos los más generalizados que consisten en:

Impedir que una empresa localice a un determinado vehículo de su flota mediante el dispositivo GNSS instalado a bordo – entre otros – como una forma de camuflar el absentismo laboral por la presencia o ausencia del conductor autorizado en una determinada zona;

Detectar el uso ilegal del citado vehículo;

Evitar la localización de un vehículo de alta gama sustraído, antes de que sea sacado del país o desguazado en un taller ilegal para su venta por piezas;

Impedir la activación del sistema de alarma cuando un delincuente -al que se le ha instalado en su muñeca o tobillo una pulsera de geolocalización- entre o salga de una determinada zona preestablecida; Etc.

Muchos de estos dispositivos *jammer* son de reducido tamaño[34] y bajo costo, por lo que es obvio que el mercado ha ido evolucionando y creciendo al mismo ritmo que el de los receptores civiles de GNSS que se han implantado masivamente.

Los *jammer* más peligrosos son los de una potencia inferior a los 100 W porque son más difíciles de detectar cuando están operativos. Para hacerse una idea diáfana del poder que tiene uno solo de ellos basta decir que con un *jammer* del tamaño de un paquete de

[33] En 2001 el puerto entero de Moss Landing (California) tuvo inutilizados sus receptores de GPS durante semanas debido a un pre-amplificador de una antena de televisión instalada en un barco allí fondeado.

[34] Un dispositivo *jammer* de 1 W puede tener fácilmente un tamaño menor al de una lata de refresco de 33 cl. por lo que resulta sencillo su transporte y ocultación.

cigarrillos, que tenga una potencia de 1 W y una batería del tamaño de un cigarrillo, se puede cubrir un área de 20 km^2 durante al menos 10 horas.

Los dispositivos en cuestión son ilegales y en muchos países se persigue su comercialización con dureza[35], pero a nivel gubernamental son también muchos los países que prueban nuevos aparatos de ataque electrónico al igual que entrenan habitualmente a su personal en su uso.

No hay más que echar un vistazo al estricto protocolo del DoD de EEUU[36] para darse cuenta de que dichas prácticas llevan años realizándose -incluso con la colaboración de otros países- o cómo la Federación Rusa identifica esta actividad como una de las grandes vulnerabilidades de su país[37] para la que debe estar preparada.

A nivel defensivo en EE.UU. se ha llegado a plantear en 2009 por parte del DHS el instalar una red de sensores distribuidos por todo el país que serían capaces de detectar, identificar y localizar las fuentes de interferencia provocadas por el *jamming* y actuar en consecuencia. Es lo que se conoce como el programa *Patriot Watch*[38], y sus siguientes fases de respuesta, los programas *Shield Watch (*protección con contra-medidas *anti-jamming)* y *Sword Watch* (ataque electrónico contra las fuentes de *jamming*).

Hoy por hoy y debido sin duda al de momento escaso número de incidentes graves[39] investigados, el proyecto del DHS carece de financiación - aunque ni mucho menos se ha olvidado -.

Que la lucha contra el *jamming* a nivel oficial es importante es indudable, pero que además va de la mano del factor comercial anteriormente expuesto también se puede ver de manera evidente con los proyectos de la *Defense Advanced Research Projects Agency* (DARPA) de EE.UU. En concreto dos de ellos -desarrollados por la empresa Navsys Corporation[40]-, uno

---

35 Federal Communications Commission, *FCC Enforcement Bureau Steps Up Education and Enforcement Efforts Against Cellphone and GPS Jamming*, 09.02.2011. Disponible en http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-304575A1.pdf Fecha de consulta 04.11.2013.

36 U.S. Chairman of the Joint Chiefs of Staff Manual, *Performing tests training and exercises impacting the Global Positoning System (GPS) in the United States and Canada*, Directiva en vigor a partir del 28.02.2012.

37 Ministerio de Defensa de la Federación Rusa, КОНЦЕПТУАЛЬНЫЕ ВЗГЛЯДЫ НА ДЕЯТЕЛЬНОСТЬ ВООРУЖЕННЫХ СИЛ РОССИЙСКОЙ ФЕДЕРАЦИИ В ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ, páginas 3-4. Disponible en http://ens.mil.ru/science/publications/more.htm?id=10845074@cmsArticle Fecha de consulta 04.11.2013.

38 Department of Homeland Security, *Patriot Watch*, 2011, disponible en http://www.gps.gov/multimedia/presentations/2012/03/WSTS/merrill.pdf Fecha de consulta 04.11.2013.

39 En 2009 el aeropuerto de Newark Liberty International Airport (New York) tuvo inutilizados de forma intermitente sus receptores de GPS durante dos meses debido a que un camionero tenía instalado un dispositivo *jammer* en su camión para evitar ser localizado por su jefe.

En 2012 sucedió lo mismo en ese aeropuerto debido a otro camionero. Disponible en http://fjallfoss.fcc.gov/edocs_public/attachmatch/FCC-13-106A1.pdf Fecha de consulta 04.11.2013.

40 Navsys Corporation, *GPS Technologies and Threat Mitigation for Wide Area Sensing*, 07.03.2012. Disponible en http://www.navsys.com/papers/12-03-

del 2010, el del GPS JLOC (un localizador de dispositivos *jammer* contra GPS) y otro en 2012, el de la Aplicación para *smartphones* (sistema Android) que permite visualizar los aparatos *jammer* del enemigo detectados por el GPS JLOC en un área y así evitarlos. Estos dos proyectos originariamente militares seguramente tengan buena aceptación en el ámbito civil en un futuro no muy lejano.

Habría que añadir que dentro de la modalidad del referido *jamming* estaría la del *meaconing*[41] que consiste sustancialmente en un dispositivo que captura la señal emitida por el satélite y la retransmite de nuevo con un retardo suficiente como para provocar la confusión en el receptor de las señales GNSS. Ya en el año 2005 generó el interés del DoD el conocimiento de que una empresa alemana había solicitado y obtenido una licencia de patente para este tipo de dispositivos y por consiguiente quedaban documentados los posibles escenarios de uso del aparato en cuestión[42].

Spoofing

Se trata de un nivel superior de ataque - y por lo tanto más peligroso - ya que si el *jamming* enmascara la señal GNSS, con el *spoofing* lo que se consigue es sustituir - de forma progresiva y sin ser detectada - esa señal original de los satélites por una distinta emitida desde un dispositivo no autorizado. Esta suplantación de señal no es una quimera a nivel civil - dada la vulnerabilidad manifiesta de las señales civiles del GPS que, a diferencia de un sistema informático, el primero carece de validaciones de usuarios, contraseñas o cortafuegos- puesto que así ha sido reconocido oficialmente que incluso puede ocurrir en el ámbito militar[43].

De esta forma, entre otros, están los siguientes experimentos que han puesto de manifiesto las vulnerabilidades de los receptores civiles de GPS instalados en *drones* y embarcaciones.

- Experimento de la Universidad de Texas de junio de 2012.

A petición del DHS el profesor Todd Humphreys y sus alumnos del Laboratorio de Radio-Navegación de la Universidad de Texas en Austin tomaron el control en vuelo de una pequeña aeronave no tripulada (UAV) mediante un dispositivo *spoofer* demostrando que se puede alterar su rumbo y destino tras hacerla ejecutar las maniobras que quisieron[44].

001%20GPS%20Technologies%20and%20Threat%20Mitigation%20for%20Wide%20Area%20Sensing.pdf Fecha de consulta 04.11.2013.

41 *Meacon*: Neo-anglicismo formado por las palabras inglesas, *m(islead) + b(eacon)*.

42 HOEY, David, BENSHOOF, Paul, (Comandante del *US Air Force 746 th Test Squadron* y Director del *GPS Test Center of Expertise* del *US Air Force 746 th. Test Squadron*, respectivamente) *Civil GPS System and potencial vulnerabilities*. 25.10.2005.

43 United States Air Force Scientific Advisory Board, *Report on Operating Next-Generation Remotely Piloted Aircraft for Irregular Warfare*, abril 2011, páginas 25-26.

44 Slate Magazine, Research Team Hacks Surveillance Drone With Less Than $1,000 in Equipment, septiembre 2012. Disponible en http://www.slate.com/blogs/future_tense/2012/07/02/hacked_surveillance_drone_with_spoofed_gps_system_demonstrates_uav_security_flaws_.html Fecha de consulta 04.11.2013.

Conscientes del peligro que entraña dicha actividad -especialmente cuando está previsto que unos 30.000 UAVs sobrevuelen EE.UU. antes del final de la década- estos investigadores decidieron trabajar en el desarrollo de un dispositivo que fuera capaz de detectar a su vez y en tiempo real a los dispositivos *spoofer*[45].

- Experimento de la Universidad de Texas de junio de 2013[46].

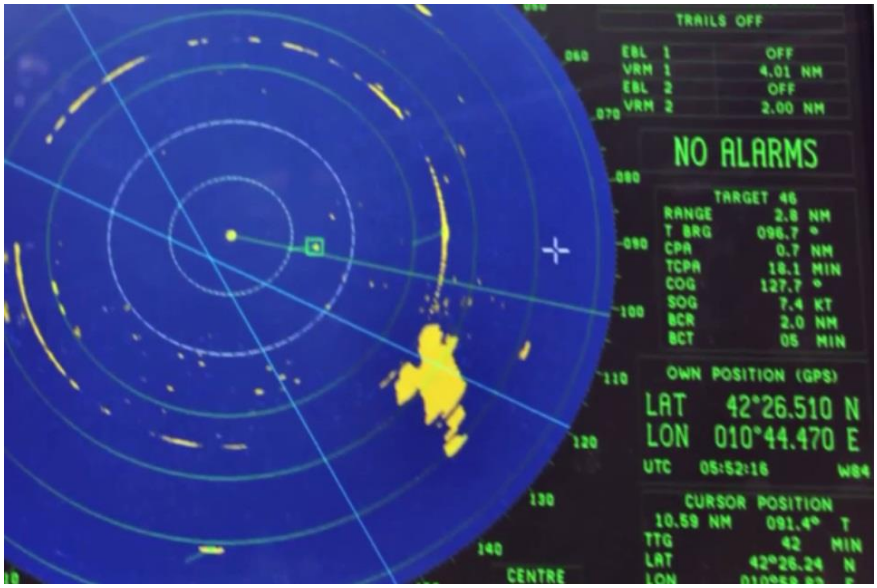
Que las investigaciones en el campo del *spoofing* no han pasado desapercibidas para los millonarios que temen ser objeto de atentados terroristas, robos o secuestros, queda patente gracias al interés del propietario del súper-yate de lujo (60 metros de eslora y 60 millones de euros), en conocer las vulnerabilidades del mismo.

Fotografía del Súper-yate *White Rose of Drach* por cortesía de la Universidad de Texas.

Al igual que en el caso anterior los investigadores se hicieron con el control del sistema de recepción de las señales GPS. Ni siquiera la tripulación se dio cuenta de ello pues ninguna de las alarmas de pérdida de señal GPS real se encendieron en la instrumentación del puente de mando. Esto, sin duda, permitió que las falsas señales de GPS transmitidas por el dispositivo *spoofer* -del tamaño de un maletín y de un precio de unos 1.000 euros - se interpretaran poco a poco por el receptor de GPS del barco y por la tripulación como verdaderas.

[45] The University of Texas at Austin, *GPS Spoofing Detection System*, 2012. Disponible en http://radionavlab.ae.utexas.edu/publications/gps-spoofing-detection-system Fecha de consulta 04.11.2013

[46] Ibid, Researchers Coerce Super-Yatch off Course, junio 2013. Disponible en http://www.youtube.com/watch?v=YbWpFMXADAY&feature=youtube_gdata_player Fecha de consulta 04.11.2013.



Sistema de navegación del súper-yate sin aviso de señales de alarma.

Fotografía por cortesía de la Universidad de Texas.

PROTECCIÓN DE LOS INTERESES HUMANOS Y ECONÓMICOS

Gastos por desvíos de las rutas

Es indudable que cualquier desvío de su ruta por parte de un gran barco porta-contenedores puede suponer una gran cantidad de combustible[47]. No hace falta más que hacerlo desviarse ligeramente durante su viaje oceánico entre puertos para incrementar el gasto con la ya vista técnica del *spoofing*.

Robos

Todavía estamos lejos de los deseos de Frederick Smith - fundador y presidente de la multinacional del transporte de paquetería, FedEx – de cambiar toda la flota de aviones que posee por otra de aeronaves no tripuladas (UAVs)[48].

Lógicamente en su momento y en relación a la vulnerabilidad del GPS civil anteriormente mencionada (*spoofing*), también habría que tenerse en cuenta el riesgo que puede suponer la sustracción de mercancías valiosas al hacerse los ladrones con el control de los UAVs.

[47] Ejemplo: El Maersk Mc Kinney Moller gasta 150 toneladas de combustible por día de navegación. Disponible en http://www.marinetraffic.com/ais/es/shipdetails.aspx?MMSI=219018271 Fecha de consulta 04.11.2013.

[48] DIY Drones, Fred Smith: FedEx wants UAVs, 12.02.2009. Disponible en http://diydrones.com/profiles/blogs/fred-smith-fedex-wants-uavs Fecha de consulta 04.11.2013.

Peligros potenciales

Quedaría finalmente por valorar -aunque fuera de forma remota o residual- lo que suponen las provocaciones intencionadas de desvíos de rutas de los medios de transporte - de barcos principalmente- con el objeto de exponerlos de forma continua o intermitente a riesgos potenciales tales como:

Zonas de arrecifes para hacer encallar un barco;

Rutas asoladas por la piratería para incitar o facilitar un asalto;

Climatologías sumamente adversas que podrían provocar una pérdida de vidas humanas y materiales si no se evita pasar por una determinada zona y momento concreto.

Sistemas de redundancia

Dadas la vulnerabilidades evidentes de las señales civiles de GNSS, a nivel civil habría que concienciar a la población sobre la planificación y correcto uso de estrategias y sistemas de redundancia para evitar los problemas que una denegación de servicio de origen natural, accidental o intencionada, (aunque la mayoría de los dispositivos no sepan de que tipo es) pueda ser avisada por parte de un receptor de señales GNSS.

Uno de los ejemplos más claros lo tenemos en la navegación recreativa donde son muy pocos los que son capaces de utilizar en el día a día un sextante para determinar su posición en una carta náutica, pues la mayoría confía ciegamente en la instrumentación tecnológica de a bordo en lo que pierden de vista la costa -o antes-. Así, los conocimientos que se adquirieron en algún momento, si no se practican con asiduidad, tienden a desaparecer –especialmente en momentos de tensión -.

EL ASPECTO LEGAL EN LAS INVESTIGACIONES POLICIALES

Sin duda alguna la sentencia más importante en materia de GPS en EE.UU. y a nivel de investigaciones policiales es la que ha declarado inconstitucional el uso -sin una orden judicial previa- por parte de las Fuerzas Policiales (en este caso el FBI), de rastreadores de vehículos basados en receptores de señales civiles de GPS [49].

Esencialmente se trata de un dispositivo que recibe las señales civiles de los satélites GPS y las reenvía a un servidor central donde se almacenan y analizan los datos captados para la geolocalización del vehículo donde ha sido instalado. Es lo que se conoce como balizar un vehículo para rastrear su posición y por ende reproducir los movimientos y posible paradero actual del conductor.

[49] *United States Court of Appeals for the Third Circuit Nº 12-2548. 22.10.2013* Disponible en http://www2.ca3.uscourts.gov/opinarch/122548p.pdf . Fecha de consulta 04.11.2013

No deja de ser curioso que el fallo judicial haya supuesto:

Declarar de forma vertiginosa, -en menos de tres años desde la detención *in fraganti* de los interesados- y al más alto nivel judicial posible, que se estaban vulnerando los derechos constitucionales de esos ciudadanos -recogidos en el Cuarta Enmienda de su Constitución y que regula entre otras cuestiones la forma en la que se les puede investigar-.

Que el organismo gubernamental que utilizó el dispositivo fuera el mismísimo FBI.

Que la Oficina del Fiscal tuviera conocimiento previo y preciso del asunto en cuestión pero que no se contara con autorización judicial para la instalación.

ESCRIBIENDO EL SEGUNDO CAPÍTULO DE LA HISTORIA EN MATERIA DE GEOLOCALIZACIÓN Y NAVEGACIÓN POR SATÉLITE

Que algo más está cambiando en la materia es evidente. Solo hay que ver la rueda de prensa de la Directora de la DARPA en la primavera de 2013[50] para darse cuenta de que en muy poco tiempo se han logrado a nivel militar grandes avances -como los que se verán a continuación- por lo que es posible que alguno de ellos pase rápidamente al ámbito civil autorizado.

No se trata por tanto de abandonar el GPS sino de buscar un conjunto de soluciones tecnológicas nuevas que sirvan para complementar el sistema y evitar o minimizar sus vulnerabilidades.

Microchips

Para navegar entre dos puntos dados se necesitan tres datos: Orientación, aceleración y tiempo.

La medición de dichos datos es precisamente lo que los ingenieros de la DARPA - dentro del programa *Micro-Technology for Positioning, Navigation and Timing* (Micro-PNT)[51]- consiguieron unir en un solo dispositivo miniaturizado al extremo por primera vez.

De esta forma en abril de 2013 se hizo público el logro de haber diseñado y fabricado el *Timing & Inertial Measurement Unit* (TIMU). Lo extraordinario del TIMU es que se trata de un prototipo de microchip de seis capas, con tan solo 10 mm^3 y 1 W de potencia que contiene siete dispositivos de medida miniaturizados (un reloj, tres acelerómetros y tres giroscopios).

Las aplicaciones militares del TIMU estarán principalmente en el campo de:

[50] PRABHAKA, Arati, DARPA, Press Conference at Pentagon, 2013. Minutos 23 a 29. Disponible en http://www.youtube.com/watch?v=_Ldsb1kPvxc Fecha de consulta 04.11.2013.

[51] DARPA, Micro-Technology for Positioning, Navigation ad Timing, 2010. Disponible en http://www.darpa.mil/Our_Work/MTO/Programs/Micro-Technology_for_Positioning,_Navigation_and_Timing_%28Micro-PNT%29.aspx Fecha de consulta 04.11.2013.

Los *Unmanned Aerial Vehicles* (UAVs);

Los *Unmanned Underwater Vehicles* (UUVs).

Los sistemas de guiados de municiones y misiles;

La navegación de los soldados en tierra.

Es dentro de este último apartado donde cobra más interés este avance -dado el tamaño del TIMU-, ya que no supondrá problema alguno el poderlo integrar dentro de:

Un *smartphone* -con su correspondiente aplicación-, puesto que además el DoD pretende que todo su personal disponga de este tipo de teléfonos cuanto antes[52];

Una tarjeta de crédito;

Un permiso de conducir;

Un pasaporte;

Una acreditación de seguridad;

Etc.

Timing & Inertial Measurement Unit (TIMU).

Fotografía por cortesía de la DARPA.

[52] Department of Defense, *DOD Releases Commercial Mobile Device Implementation Plan*, 26.02.2013. Disponible en http://www.defense.gov/releases/release.aspx?releaseid=15833 Fecha de consulta 15.03.2013.

Con esta solución se evitarían los graves problemas que supone el uso de dispositivos GPS comerciales[53] por parte del personal militar dentro de territorio hostil, ya que además de ser objetivos de la guerra electrónica pueden ser detectados por el enemigo y facilitarles a su vez una posición precisa de su ubicación.

Misiles

En agosto de 2013 se realizó la prueba de un nuevo misil anti-buque dentro del novedoso proyecto de la DARPA llamado *Long Range Anti-Ship Missile* (LRASM) que prescinde de las señales GPS para el guiado del mismo hasta el objetivo, etc.[54]

Impacto del misil -con cabeza inerte- en todo el centro de un blanco flotante en movimiento.

Fotografía por cortesía de la DARPA.

CONCLUSIONES

Ya sea por motivos estratégicos, económicos, tecnológicos, políticos, etc. el GPS sigue suscitando gran interés pese a haber pasado dos décadas de la disponibilidad de su señal civil.

Sus vulnerabilidades y los usos contrarios a sus intereses, marcaron el inicio de una toma de medidas en el año 2001 que se ha visto condicionada en general por los incrementos presupuestarios, debido a la complejidad que supone poner en funcionamiento y mantenimiento los sistemas GNSS – y los sistemas regionales ya vistos-.

---

53 A veces algunas unidades militares no disponen de suficientes dispositivos GPS militares, o estos son muy pesados o no disponen de una cartografía actualizada, por lo que los soldados deciden utilizar imprecisos dispositivos GPS comerciales, incluidos algunos especialmente problemáticos como el de la marca GARMIN modelo RINO, que puede facilitar la posición propia al enemigo. Video de Aerospace Corporation de EE.UU. *Commercial GPS Receivers: Facts for the Warfighter.* Disponible en http://www.youtube.com/watch?v=fVxDVUsiejQ&feature=youtube_gdata_player Fecha de consulta 04.11.2013.

54 DARPA, *Anti-ship missile prototype successfully conducts first solo flight*, 06.09.2013. Disponible en http://www.darpa.mil/NewsEvents/Releases/2013/09/06.aspx

Igualmente la tecnología que se encuentra detrás de estos sistemas ha generado no pocos conflictos entre los actores gubernamentales en cuestión, llegando al punto de que todos los que han querido y podido, han desarrollado -o lo están haciendo- sus propias soluciones.

Por otra parte el ataque a las señales GNSS -mediante *jammming*, *meaconing,* o *spoofing*- está generando nuevas líneas de investigación, al objeto de evitar los posibles daños en vidas y bienes económicos, principalmente.

De esta manera la imperiosa necesidad de superar sus vulnerabilidades y la aparición en escena de otros sistemas de posicionamiento global o regional sin duda marcarán el devenir de al menos la próxima década.

[i]

*Fernando Ruiz Domínguez**
Subinspector del Cuerpo Nacional de Policía