EL GPS, UN ATRACTIVO BLANCO PARA EL ENEMIGO

Juan Antonio CHICHARRO SÁNCHEZ-AGUSTINO

Introducción

ENÍAMOS clara la situación; las órdenes eran precisas y las habíamos comprendido sin necesidad de recurrir a ningún tipo de explicación. Las Reglas de Enfrentamiento nos proporcionaban las respuestas necesarias y disponíamos de los medios óptimos para alcanzar el éxito. Estábamos bien preparados para cumplir nuestra misión; no había motivo para abrigar duda alguna.

Habíamos recibido la *tasking order* del Commanding Task Force (CTF) un día antes. Hacía 22 horas que el Tactical Action Officer (TAO) había firmado el visto bueno del mensaje de carácter reservado y precedencia FLASH que trajo en la tablilla el marinero de guardia del Centro de Comunicaciones (CECOM). Inmediatamente, fuimos destacados a unas millas de la Fuerza para acometerla. Con rumbos erráticos, con objeto de no desvelar nuestras intenciones, y a alta velocidad procedimos al punto designado para nuestro ataque. Desde ese momento, el planeamiento de la misión no cesaría hasta completar su ejecución. Horas y horas en el Centro de Información y Combate (CIC) y en la sala de reuniones realizando un estudio exhaustivo de la situación, de las posiciones relevantes, de las condiciones meteorológicas y la orografía, de las posibles capacidades del oponente, de los neutrales de la zona, de los sospechosos, del *pattern of life* (POL); en definitiva, de nuestras líneas de acción (COA). Todo configuraba un escenario complicado según la evaluación del jefe de Operaciones. Su estimación era que con las referencias bien establecidas no habría problema.

Nos encontrábamos en zona, a unas rigurosas 59 millas náuticas (NM) de la costa y a 83 de nuestro objetivo, descrito por el mando como el centro de gravedad (COG) de nuestro oponente. Los alcances eran buenos para nuestros misiles superficie-tierra Tomahawk (1) disparados desde nuestro lanzador vertical con un empuje inicial que le proporciona su *booster*, con un guiado inercial mediante *waypoints* establecidos previamente, con viaje de crucero rozaolas —indetectable— y un guiado final en ataque al último punto de coordenadas gracias al GPS. Además, las distancias eran suficientes para no ser detectados por las direcciones de tiro de la costa y sus sistemas de defensa Bastion-P (2), equipados con los letales misiles costeros antibuque Yakhont (3). En realidad, no esperábamos tener que enfrentar este tipo de amenaza; no obstante, el rigor militar nos mantenía alejados y prevenidos ante cualquier imprevisto. No hubiese sido el primero. Meses atrás, un destructor aliado recibió tres misiles del tipo Saccade (4) desde las costas yemeníes y tuvo que defenderse a base de misil tras misil. Éramos plenamente conscientes de esta situación.

Nuestra política de emisiones era muy restrictiva. Gracias a ello habíamos conseguido evadir, o eso parecía, a las unidades de superficie rusas y chinas que por Inteligencia y otras fuentes sabíamos que iban a encontrarse por la zona. La única actividad relevante al respecto fue la recepción de emisiones electromagnéticas, informando el operador de Guerra Electrónica de un posible *Ilyushin 20* (5), aeronave rusa dedicada exclusivamente al reconocimiento. Nos alertó y mantuvo tensos hasta no tener más noticias. Habíamos conseguido monitorizar sus movimientos gracias a la información proporcionada por la Fuerza tras nuestro informe. A la hora de la detección se encontraba a unas 127 NM de nuestra unidad, lo que indicaba que volaba alto, seguramente buscando algo de interés: probablemente a nosotros. Al alejarse comprendimos que su misión había finalizado, desistiendo de conseguir nuestra identidad y posición en la zona.

No obstante y para el posterior análisis de lo ocurrido, el operador de Guerra Electrónica en un momento dado hizo ademán de querer informar sobre algo que había percibido, pero finalmente todo quedó en un amago y lo dejó pasar. Tenía gran experiencia, llevaba 20 años de carrera a bordo de este

---

(1) Misil de largo alcance, guiado por GPS y muy utilizado por unidades de la US Navy desde 1991. Destacar el lanzamiento de entre 60 y 70 misiles sobre Siria en 2017.

(2) Sistema de defensa de costa móvil ruso equipado con misiles antibuque Yakhont. Desplegado en Siria, entre otros.

(3) Misil antibuque supersónico y de largo alcance con guiado GLONASS y radárico activo.

(4) Misil antibuque de origen chino, subsónico, de largo alcance y guiado radárico.

(5) Aeronave rusa turbopropulsada dedicada al reconocimiento desde los años 50.

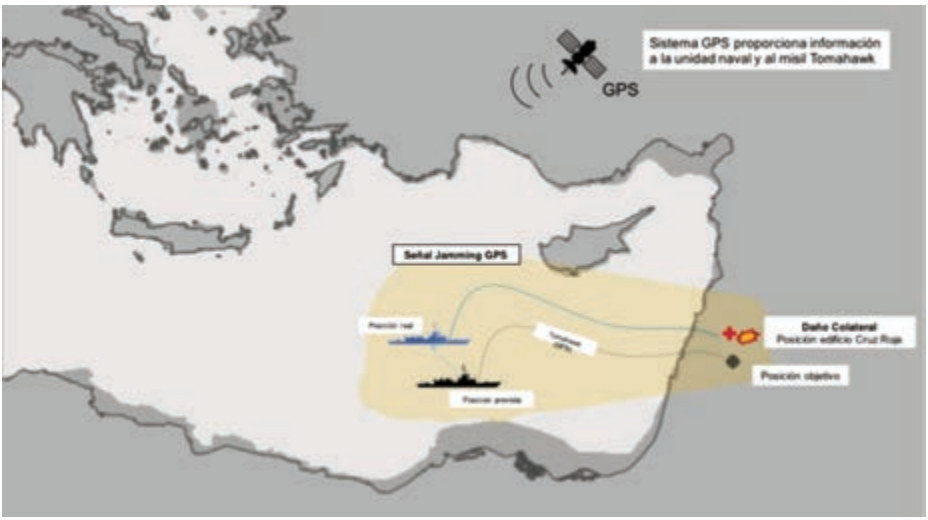
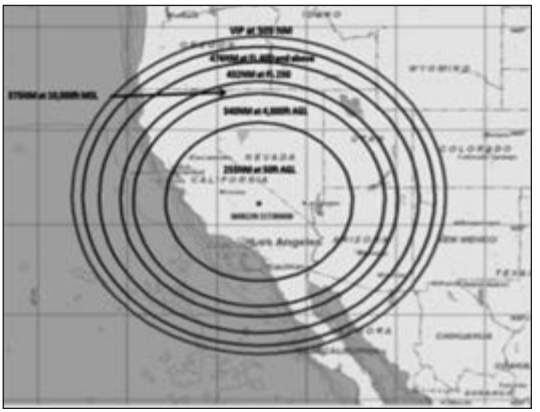


Ilustración gráfica del daño colateral ficticio ocasionado por el *jamming* del GPS.
(Ilustración realizada por el autor).

tipo de buques, utilizando los mismos equipos, de los que conocía todas sus posibilidades e incluso aquellas que no poseía. Hablar de parámetros de anchos de pulso, frecuencias, períodos, ángulos de llegada y un gran etcétera era música clásica para sus oídos. No obstante, ese día andaba algo «mosca» con una variación extraña que no había visto nunca en el equipo y que ocurrió en milisegundos. Sabía de algunos experimentos electrónicos que ejércitos y armadas de otras naciones suelen realizar con frecuencia, pero desconocía su magnitud e intensidad al no haberlos probado nunca. Este pensamiento aumentó su inquietud, pero tras unos minutos acabó por quitarle importancia al no sufrir ningún tipo de movimiento ni nada relevante. En la zona, todos los emisores eran conocidos y de poco interés, concluyó; así, su inicial intención de intervenir quedó en una falsa alarma.

Llegó el momento. El *time on target* (TOT) se aproximaba. La misión estaba clara: neutralizar y destruir el edificio situado en la posición indicada en el mensaje FLASH. Esta tarea resultaría determinante para el devenir de la guerra en el país. Pondríamos probablemente fin a años de crisis. Sería un duro golpe. No había dudas ni margen de error en la consecución del objetivo, todo estaba claro: «donde pongo el ojo, pongo la bala».

«Permiso comandante, ¡fuego!», ordenó el oficial del subcontrol de Guerra de Superficie. «Tiempo de 12 minutos y 34 segundos y fin». «Salgamos de aquí», ordenó el comandante. Había pasado un día desde la recepción de la orden a su ejecución. Era la primera misión para toda la dotación de lanzamiento real sobre unas instalaciones. El nivel de adrenalina era muy alto, y la



Alcances obtenidos durante pruebas realizadas de perturbación de GPS del Departamento de Defensa en California (2016). (*https://gis.utah.gov*).

emoción de llevarla a cabo lo era aún más.

Lo que no podían imaginar era que habíamos fracasado estrepitosamente.

El informe resultante revelaba que las instalaciones que nos habían ordenado destruir estaban intactas y que las explosiones se localizaban lamentablemente en un edificio de la Cruz Roja atestado de refugiados de la cruel guerra. Había quedado hecho añicos y los daños colaterales eran vitales e irreparables. No había consuelo alguno; ni el comandante, hombre tranquilo y con gran sentido común, sabía cómo asumir este inesperado desenlace. Era el peor día de nuestras vidas. ¿Qué podía haber fallado? ¿Cómo había ocurrido si todo estaba en orden?

Poco a poco la respuesta se fue abriendo paso. Habíamos sido perturbados, perdiendo las situaciones geográficas. ¡Estaban todas hackeadas! Ni nos hallábamos en el sitio que creíamos, ni el objetivo estaba en la posición calculada. Alguien había modificado deliberadamente nuestras referencias y, para colmo, el perfil de crucero del misil había resultado erróneo (6).

El *Ilyushin 20* debió de detectarnos e informó de nuestra posición. Las extrañas sensaciones del operador de Guerra Electrónica eran reales: habíamos recibido un ataque de decepción electromagnética, un *jamming* al Sistema de Posicionamiento Global (GPS).

La dependencia del GPS

Todo lo relatado anteriormente es pura ficción, pero no tiene por qué alejarse necesariamente de la realidad. La amenaza de perturbación del GPS es real y factible. Para calibrar la gravedad de esta situación bastará apuntar que los Estados Unidos reconocen que el 80 por 100 de sus operaciones no podrían llevarse a cabo sin el GPS y en el futuro aún serán más. Para neutrali-

(6) El Ministerio de Defensa ruso afirmó que más de la mitad de los misiles lanzados por las unidades de la US Navy en abril de 2017 sobre Siria no llegaron correctamente a su objetivo.

zar los resultados negativos que estas perturbaciones pueden acarrear, la US Navy realiza asiduamente adiestramientos frente a estas amenazas. La realidad es que con un mísero perturbador del tamaño de una lata de Coca-Cola comprado por internet se pueden provocar grandes daños con consecuencias muy negativas.

Pequeño perturbador de GPS que se puede obtener fácilmente en internet. Uno como este puede perturbar 500 m a su alrededor. (Fuentes abiertas).

Es del dominio público que el uso de la geolocalización por GPS se ha generalizado vertiginosamente. Desde su creación se ha instalado en nuestras vidas sin apenas darnos cuenta. Está en nuestros vehículos, relojes, teléfonos... y especialmente en el transporte marítimo, terrestre y aéreo, a los que proporciona precisión y seguridad.

Debemos remontarnos al año 1973 para conocer sus inicios. Nace de la necesidad del Gobierno de los Estados Unidos de tener un sistema riguroso que mejorase los anteriores: *Transit* y *Timation* de la US Navy, *621B* de la Air Force y *SECOR* del US Army para determinar las posiciones exactas de sus buques, aeronaves y unidades terrestres en todo el globo terráqueo, y así contar con una clara ventaja con respecto a sus enemigos; el objetivo era dejar atrás a la URSS. Sus aplicaciones eran sensacionales. El GPS mejoraría la coordinación entre elementos de una fuerza, la efectividad en los objetivos de las armas, reduciendo daños no deseados, e incluso conseguiría dejar al «hombre» fuera de peligro mediante sistemas no tripulados, reduciendo así el número de bajas.

El GPS fue creado exclusivamente en el ámbito militar para interés propio del Departamento de Defensa (DoD) de los Estados Unidos y bajo su control, considerándolo de gran valor estratégico. El derribo de un avión de pasajeros coreano de la compañía Korean Airlines en 1983 al invadir el espacio aéreo soviético por error —fallo de navegación— obligó al Gobierno estadounidense a autorizar a la aviación civil un cierto nivel de uso del sistema GPS con el objetivo de evitar la inclusión de los medios de transporte en zonas conflictivas e impedir incidentes similares potencialmente capaces de llevar a situaciones poco afortunadas. Evidentemente fue una medida política, pero también económica. Eso sí, no iba a ser tan sencillo para el enemigo y tampoco para los no enemigos. Estados Unidos impuso restricciones en la precisión de los receptores, de forma que el error en el posicionamiento fuese mayor. Facilitaba navegar en aguas abiertas (daba una referencia), pero no permitía realizar una canal dragada. Había que utilizar otros medios, por ejemplo el sistema

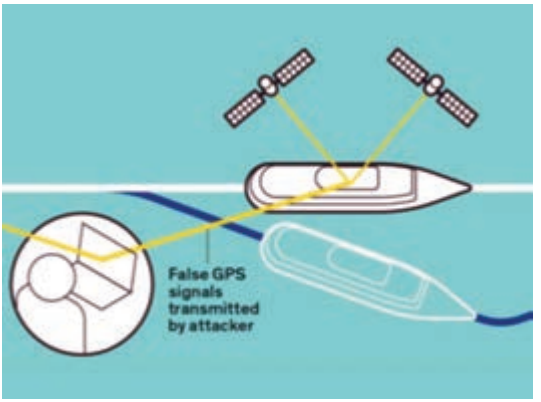


Ilustración gráfica de perturbación de la señal GPS sobre la navegación de un barco. (*ATIS Technical Report*, figura 5.2, p. 9).

Trisponder con antenas en las montañas que triangulasen la posición. Destacar que durante la guerra en el Adriático, los norteamericanos manipulaban la señal de forma que creaba una zona de sombra para el GPS, al menos para los no usuarios.

En el año 2000, el Gobierno de Bill Clinton decidió liberar toda restricción y su error deliberado, la llamada «disponibilidad selectiva», permitiendo así el uso global, lo que provocó su empleo generalizado tanto para las unidades militares y sus sistemas —navegación, misiles, vehículos no tripulados— como para cuestiones más mundanas —relojes, vehículos, teléfonos, etcétera—.

En el ámbito militar, la influencia de estos equipos es muy marcada en las operaciones navales; es evidente que dependen mucho del GPS, tanto para la navegación como para los sistemas de mando y control y sistemas de armas o de combate.

Son numerosos los sistemas y equipos que actualmente se sirven de la información del GPS (PNT: *positioning, navigation and timing*). Los de combate, para los sistemas de armas y el corazón del mando y control (LINK), la navegación en sus sistemas AIS, WECDIS, comunicaciones VHF de emergencia o de llamada selectiva y NAVTEX, los radares de navegación y superficie, las giroscópicas y largo etcétera, lo que en definitiva se traslada a numerosas capacidades de los medios navales (superficie y aéreos) tanto en aguas litorales (imagínese el lector qué cantidad de operaciones navales se pueden realizar en las proximidades y a la merced de la costa hostil) como en aguas abiertas.

En la vida civil, su uso está asimismo plenamente extendido. En la navegación marítima, el GPS se ha convertido en una herramienta indispensable, ya que proporciona el método más rápido y preciso para navegar, medir la velocidad y determinar la posición en todo el mundo con una mayor seguridad y eficiencia. No hay que olvidar que actualmente el comercio por mar representa el 80 por 100 de los intercambios mundiales. Lo mismo sucede en la navegación aérea, que ha visto crecer su actividad considerablemente, y asimismo en la tecnología más mundana, que no es necesario recordar. Esta dependencia definitivamente ha acabado creando un serio problema.

Consideraciones

El sistema GPS es vulnerable. Su señal es débil y fácil de interferir (perturbable por ruido y engaño). Además, el avance de los misiles balísticos capaces de atravesar grandes capas y alturas y destruir los satélites hace que el GPS se haya convertido en un blanco muy atractivo para el hipotético enemigo, que puede forzar daños irreparables y provocar situaciones muy desfavorables.

Gráfico en el que se puede apreciar el guiado del misil Tomahawk desde su lanzamiento mediante el sistema GPS. (*Chicago Tribune*).

Son ya varios los casos de supuestos ataques de este tipo en maniobras y ejercicios de la OTAN. Casi todos acusan a un actor, Rusia, pero no es descartable que no sea el único interesado en este tipo de acciones. Lo que parece claro es que el tema no se debe dejar a un lado, pues cada mes hay nuevos incidentes y de repercusiones mayores. Algunas informaciones (7) han señalado que la fragata noruega *Helge Instad* (8), previamente a su choque en uno de los fiordos noruegos con el tanque *Sola TS* el pasado noviembre, había sufrido un error en los equipos de navegación, coincidiendo con ataques rusos a los GPS durante el ejercicio TRIDENT JUNCTURE 2018 de la Alianza Atltántica.

Tampoco se salvan los actores civiles. El rastreo, el *big-data*, el reconocimiento y la privacidad se ven afectados por las señales continuas de GPS que emiten los equipos electrónicos. Recuerde el lector lo sucedido el pasado noviembre cuando STRAVA (aplicación de móvil para correr) reveló mediante puntos de GPS los lugares en los que hacían deporte los soldados estadouni-

---

(7) O'Dwyer, Gerard: *Finland, Norway press Russia on suspected GPS jamming during NATO drill*, *Defense News*, *https://www.defensenews.com/global/europe/2018/11/16/finland-norway-press-russia-on-suspected-gps-jamming-during-nato-drill/*.

(8) La fragata de la clase *Fridtjof Nansen* de la Armada Real de Noruega se hundió en un fiordo al norte de Bergen tras un accidente ocurrido el 8 de noviembre de 2018 cuando regresaba de su participación en el ejercicio TRIDENT JUNCTURE 2018.

denses durante sus despliegues en Afganistán, Irak o Siria: El resultado permitía localizar las bases secretas de las Fuerzas Armadas de los Estados Unidos. Una información con una elevada clasificación de seguridad.

Conclusión

La geolocalización es una herramienta estratégica en términos militares y de enorme impacto comercial en términos civiles, y el asunto es demasiado importante como para permitir el monopolio global del Gobierno estadounidense. Sin duda, a las demás potencias —y principalmente a las conocidas como posibles adversarias o enemigas, emergentes, como el caso de China, Rusia o India— este monopolio les causa preocupación y recelo. El sistema GPS funciona, es vital en nuestros días, pero es inseguro y poco fiable para cualquier nación que no sea la que lo controla, y son muchas las que dependen directamente del GPS para su defensa e industria.

Por estas razones, determinadas potencias llevan años desarrollando sistemas de geolocalización propios con el objetivo de finalizar con esta dependencia y evitar así las cuestiones mencionadas. Rusia lleva años con su sistema GLONASS, China con el BEIDOU-1 que cubriría toda Asia, la India con el GAGAN, Japón con el JRANS y Europa comienza su singladura en un futuro próximo con el GALILEO, *a priori* más fuerte en señal y más dificultoso de perturbar. El desarrollo de estos nuevos sistemas tendrá un gran impacto en el futuro. ¿Será beneficioso en su comercio, en su industria? ¿Les ayudará en sus conflictos? ¿Es un motivo más para una hipotética guerra global?

Mientras tanto, parece claro que debemos proteger lo que tenemos: impulsar el esfuerzo técnico para endurecer los receptores GPS y antenas o mediante relojes atómicos como blindaje físico; no descartar la utilización de otro sistema como *back-up* (eLoran); tener el sextante a mano y, por supuesto, maximizar los adiestramientos en entornos de denegación, puesto que la realidad es que el GPS es un atractivo blanco para el enemigo.

BIBLIOGRAFÍA

CHICHARRO SÁNCHEZ-AGUSTINO, Juan; RUIZ ROJAS, Roberto: Trabajo Fin de Curso-Especialidad de Sistemas de Combate. *Jamming GPS, Consecuencias*. Escuela Especialidades «Antonio de Escaño», enero 2017.

BURREL, J.: *Disruptive Effects of Electromagnetic Interference on Communication and Electronic Systems*, abril 2003.

DE BAKKER, P. F.: *Effects of Radio Frequency Interference on GNSS Receiver Output*. Delft University of Technology Faculty of Aerospace Engineering.

GLOMSVOLL, Oeystein: *Jamming of GPS & Glonass Signals*. University of Nottingham, 2014.

MANGESH DESKPANDE, S.: *Study of Interference Effects on GPS Signal Acquisition*. University of Calgary, Alberta, 2004.

RUEGAMER, A.; KOWALEWSKI, D.: *Jamming and Spoofing of GNSS Signals. An Underestimated Risk?,* 2015.

—*Navegación en condiciones de denegación de señal GNSS*. Ministerio de Defensa.

VÁZQUEZ, J. R.: *Detection of Spoofing, Jamming, or Failure of a Global Positioning System (GPS)*. Air Force Institute of Technology, 1992.

AMIN, M. G.; LINDSEY, A. R.; LIANG, Zhao y YIMIN, Zhang: *Anti-Jamming Techniques for GPS Receivers*, 2001.

National PNT Advisory Board. Jamming the Global Positioning System. A National Security Threat: Recent Events and Potential Cures, noviembre 2010.

KANDANGATH, A.: *Jamming Mitigation Techniques for Spread Spectrum Communication Systems*.

BAO-YEN TSUI, James: *Fundamentals of Global Positioning System Receivers: A Software Approach*. John Wiley & Sons Inc., 2000.

—*Introducción al sistema GPS*, 1999. Leica Geosystems AG. Heerbrugg, Suiza.

GRAHAM, A.: *Communications, Radar and Electronic Warfare*. UK: John Wiley & Sons Inc., 2011.

HOLANDA BLAS, M. P.; BERMEJO ORTEGA, J. C.: *GPS & GLONASS*, 1998.

The Economist, from the print edition, Technology Quarterly. GPS Jamming: No jam tomorrow, 10 de marzo 2011.

HENDRICK, M.: *GPS Jamming. Smith Power Program*, 2013.