

NAVWAR EN LA ARMADA. CAMBIO DE PARADIGMA EN LAS OPERACIONES NAVALES

Introducción

EL 17 de enero de 1991 comenzó la Operación Tormenta del Desierto, liderada por Estados Unidos, en la que participaron 42 países con la finalidad de liberar Kuwait tras ser invadida por Irak en agosto de 1990. Por primera vez en la historia de los conflictos armados, se usaron masivamente sistemas de armas, de navegación, de comunicaciones y de Mando y Control (C2) que emplearon señales proporcionadas por sistemas de navegación por satélite GNSS (*Global Navigation Satellite Systems*).

Las ventajas que proporcionan estos sistemas son muchas: utilizar armamento guiado de precisión, sincronizar sistemas de C2, de comunicaciones, *links*, etc. Con el paso de los años se ha generalizado el empleo de los GNSS, hasta el punto de que dependemos de ellos en gran medida para ejecutar cualquier operación militar.

Actualmente, muchos actores estatales y no estatales centran sus esfuerzos en denegar el acceso a estas señales, o como mínimo degradarlas, con el fin de anular o reducir la eficacia operativa de sus oponentes. Sin irnos muy lejos, la guerra entre Ucrania y Rusia que comenzó en febrero de 2022 se caracteriza por

que ambos bandos intentan denegar el acceso a la señal GNSS de su adversario reduciendo la eficacia de los drones, bombas guiadas de precisión, sistemas de posicionamiento global, así como de equipos de comunicaciones cifradas y de transmisión de datos.

No sólo el ámbito militar está afectado por estas acciones: en los últimos años se han detectado cientos de perturbaciones provocadas por pequeños dispositivos comerciales, especialmente en las cercanías de aeropuertos, que han obligado a cerrar incluso el espacio aéreo a su alrededor al perderse las ayudas a la navegación por satélite.

La OTAN ha encajado este tipo de acciones bajo el acrónimo de NAVWAR (*Navigation Warfare*), y en este artículo voy a tratar de explicar —basándome en los dos años que dediqué a ella como parte de mi trabajo en el Estado Mayor de la Armada— en qué consiste, cómo nos afecta, en qué situación se encuentra la Armada al respecto, y daré unas breves pinceladas sobre el futuro de este nuevo desafío.

¿Qué es NAVWAR?

A simple vista la traducción literal de NAVWAR como guerra de la navegación pudiera sugerir que son los esfuerzos para impedir la



navegación segura del adversario en cualquiera de los dominios físicos (terrestre, naval o aéreo). Esta interpretación es muy común, especialmente entre los profanos en el tema, pero en realidad su alcance es mucho mayor.

El STANAG 4621 de la OTAN, *Navigation Warfare Definition*, dice que NAVWAR son «... aquellas acciones militares y/o medidas técnicas necesarias para asegurar la superioridad en el posicionamiento, en la navegación y en la sincronización de la señal tiempo (*Positioning, Navigation and Timing* o PNT)»; es decir, la lucha por acceder y mantener la señal PNT de los sistemas GNSS a la vez que se la negamos al adversario. La PNT se obtiene en la mayoría de los casos de las señales satelitales, pero también, como veremos más adelante, de medios no satelitales.

La pérdida de PNT tiene implicaciones no solamente militares, sino también civiles. Por ejemplo: las operaciones bancarias y los sistemas de telecomunicaciones requieren una sincronización horaria proporcionada por la T, y las ayudas a la navegación aérea y marítima por satélite necesitan obtener información de

posicionamiento y de navegación (la P y la N). Es fácil imaginar el caos que se puede producir si se corta esta señal!

Si nos vamos al campo militar, los radares, los sistemas de combate, las municiones guiadas de precisión, los sistemas de navegación, etc., dependen de la PNT, por lo que son vulnerables si el adversario consigue anularla o degradarla, y la mayoría de los sistemas militares reciben la PNT de los GNSS, por lo que debe preocuparnos el impacto que produciría su pérdida durante el desarrollo de una operación. Hay que destacar que obtener la posición es importante, pero más lo es la señal de tiempo que sincroniza todos los equipos y sistemas.

La OTAN estableció que el sistema primario para recibir PNT debe ser el proporcionado por la constelación NAVSTAR-GPS-PPS (*Navigation Satellite Timing and Ranging-Global Positioning System-Precise Positioning Service*). Hay otras constelaciones que utilizan países como Rusia (GLONASS), la UE (Galileo), China (Beidou) e incluso la India (NavIC) y Japón (QZSS). Para recibir su PNT, el GPS-PPS necesita unas

1. En abril de 2013 el aeropuerto de Seúl en Corea del Sur se vio afectado por una perturbación de un transmisor de 50 W de potencia que aparentemente tenía su origen en Corea del Norte. Esto provocó interferencias en los sistemas de navegación aérea por satélite del aeropuerto, así como cortes intermitentes en los teléfonos móviles de la capital.

claves para descifrar los dos tipos de códigos que cifran las señales de bajada del satélite: el P(Y) y el M (militar). Más adelante vamos a ver cómo el uso del GPS provoca una vulnerabilidad estratégica por la dependencia de los Estados Unidos para obtener su servicio.

Amenazas a los sistemas GNSS. Las interferencias electromagnéticas

Las interferencias electromagnéticas afectan enormemente al funcionamiento de los GNSS al moverse la señal de radiofrecuencia del satélite en el espectro electromagnético. Pueden ser de dos tipos:

- Interferencias electromagnéticas (EMI) no intencionadas.
- EMI intencionadas (provocadas por el adversario), que son el *jamming*, el *spoofing* y el *meaconing*.

Las EMI no intencionadas son producidas por diversos factores: la disposición geométrica

de los satélites, las condiciones de propagación, las obstrucciones físicas a la señal o incluso la propia posición de la antena respecto a los satélites.

El *jamming* consiste en introducir la suficiente potencia en la banda de radiofrecuencia en la que opera el GNSS, de manera que los receptores que estén cerca no puedan engancharse a los satélites².

El *spoofing* (engaño) se basa en transmitir la información que recibe el receptor al que queremos engañar y en aumentar la potencia de la señal para que se enganche a la que transmite el dispositivo de *spoofing*. Después, se puede manipular la información que se envía para que el «engañado» tenga unos datos de navegación erróneos.

El *spoofing* es más complejo de ejecutar que el *jamming*, aunque es más difícil de detectar por la víctima. Además, el alcance del *spoofing* no es tan grande como el del *jamming*. Esto es relativamente sencillo de hacer en los GNSS



Un *spoofing* en la zona del mar Rojo. Puede observarse cómo el barco aparece sobre tierra.
(Imagen facilitada por el autor)

2. Un perturbador de baja potencia (un vatio) a bordo de un avión puede desenganchar a los receptores que estén situados a unas seis millas y evitar que se enganchen a otros satélites hasta las 45 millas.

civiles, al no estar protegida su señal³ y tener una potencia bastante débil. La señal de radiofrecuencia de bajada del satélite que transporta la PNT es bastante débil (equivalente a una bombilla de 40 W) desde una distancia de 20.200 km sobre la Tierra. Por lo tanto, es fácil perturbarla con cualquier dispositivo que transmita en una potencia mayor⁴.

No obstante, en la mayoría de las ocasiones las denegaciones suelen ser por errores o causas no intencionadas (un mero apantallamiento se puede interpretar como una perturbación).

El *meaconing* consiste en recibir una señal GNSS, modificar su parámetro T y reenviarla para confundir al receptor. Esta técnica es más sencilla que la del *spoofing* porque no hay que conocer ni los parámetros de navegación ni los códigos de los satélites.

Para el caso de los GNSS (GPS) militares, ya hemos dicho que la PNT está cifrada gracias al empleo de los códigos P(Y) y M. Es más difícil perturbarlos porque requieren una potencia mayor al ser su señal más fuerte, y no se pueden engañar gracias al cifrado, aunque sí les puede afectar el *meaconing*.

No obstante, no son las EMI las únicas formas que existen de impedir el acceso a la PNT. Desde los dominios espacio y ciberespacio también es posible realizar acciones de NAVWAR, por ejemplo a través de ciberataques contra las redes informáticas que controlan los satélites o mediante ataques contra los satélites mismos empleando

armas de energía dirigida o misiles, aunque la descripción de éstos daría para otro artículo especialmente dedicado a ellos.

¿Cómo protegernos de los ataques contra los sistemas GNSS?

De una forma o de otra, todos los sistemas que dependen de GNSS para obtener la PNT pueden verse afectados en mayor o menor medida por NAVWAR. Tendremos por lo tanto que buscar soluciones que nos permitan acceder a la PNT sin comprometer la eficacia operativa de nuestras unidades.

Hay una serie de medidas de mitigación que ayudan a paliar los efectos de NAVWAR en nuestros equipos y sistemas. Para empezar, existe un tipo de antenas receptoras de GPS denominadas CRPA (*Controlled Reception Pattern Array*) que utilizan un *array* de varios elementos de antena y que son capaces de generar «nulos», es decir, zonas de baja ganancia de antena en una dirección concreta, de manera que se anule o al menos se reduzca la potencia de una perturbación en esa dirección. De esta forma se bloquea la perturbación en una demora y puede seguir recibiendo señales de los satélites utilizando el resto de los elementos de la antena.

Se puede complementar a los GNSS con sistemas que no dependan de los satélites para obtener PNT, como relojes atómicos, sistemas de navegación inercial (INS) y/o de radiofrecuencia —el TACAN (*Tactical Air Navigation*), el LORAN (*Long Range Navigation*), etc.—, sensores

3. De hecho, la información PNT que proporcionan estos satélites se puede obtener de fuentes abiertas, por lo que es muy sencillo replicarlas y modificarlas.

4. Es posible acceder fácilmente a la compra de estos dispositivos en el mercado a precios muy asequibles. En la página de Amazon se pueden encontrar algunos por 20 euros.

doppler de movimiento e incluso sextantes digitales⁵. De esta forma, si perdemos el GNSS todavía podemos suministrar PNT a nuestros sistemas, aunque con el tiempo perderán eficacia.

Si, por otro lado, tuviéramos la capacidad de cambiar de constelación al detectar que están anulando el GPS, podríamos seguir obteniendo PNT, ya que las frecuencias de trabajo son distintas. Quizás no sea aconsejable utilizar el GLONASS ruso, pero sí el Galileo europeo (que además tiene una versión encriptada). Más adelante veremos cuáles son los planes de nuestras Fuerzas Armadas en general y de la Armada en particular al respecto.

NAVWAR en la Armada

El tema de NAVWAR es relativamente reciente en las Fuerzas Armadas españolas, aunque, en nuestro caso particular, la Armada comenzó hace pocos años a interesarse por este tema y a dar los pasos necesarios para identificar nuestras vulnerabilidades y tratar de mitigarlas.

Dentro del Estado Mayor de la Armada, la Sección de Armas y Guerra Electrónica (SARM-GE) de la División de Logística es la encargada de liderar todos los asuntos relacionados con NAVWAR —colaborando con la Jefatura de Sistemas de la Información y Telecomunicaciones (JECIS) en los aspectos relacionados con los sistemas de navegación— y de asesorar a la División de Planes en la elaboración

de los documentos de requisitos de obtención de todas las capacidades relacionadas con ella.

Uno de sus oficiales es designado de forma permanente para representar a España en el Grupo de Trabajo sobre NAVWAR en la OTAN (CaT2)⁶, donde defiende la postura nacional al respecto y además colabora en la elaboración de las publicaciones de nivel estratégico de la Alianza que versan sobre el tema (actualmente está en desarrollo una versión del AJP-3 denominada *NAVWAR in Multi Domain Operations*).

Además de esto, la SARM-GE representa a la Armada en los grupos de trabajo conjuntos, liderados por el EMACON, que trabajan en el desarrollo de la doctrina nacional sobre operaciones electromagnéticas (EMO), al ser NAVWAR una parte de éstas. Sin pretender profundizar en este tema, puesto que daría para otro artículo, mencionaré que las EMO son un concepto nuevo que va más allá de lo que conocemos como guerra electrónica, y se definen como las actividades de carácter conjunto que permiten coordinar las acciones en el espectro electromagnético (EMS) relacionadas con guerra electrónica (EW), NAVWAR, SIGINT (*Signals Intelligence*) y SM (*Spectrum Management*), de forma que se reduzca o impida al adversario la capacidad de operar en el mismo.

Respecto a esto último, existe un debate sobre si NAVWAR es EW o no, y mi opinión es que es parte de ella sólo cuando se utiliza el EMS para realizar acciones de NAVWAR ofensivas

5. Desde 2016, la US Navy ha vuelto a introducir en sus currículos académicos el aprendizaje de la navegación astronómica, preocupada por los efectos que pueda provocar un apagón total de los sistemas GNSS.

6. *Capability Team 2*.

y defensivas (mediante ataques electrónicos o defensa electrónica). Pero no sólo se producen sus acciones en el EMS, sino que NAVWAR puede consistir también en acciones cinéticas (la destrucción física de un centro de control del satélite), ciberespaciales (vigilando los sistemas informáticos que controlan la señal PNT de los satélites) e incluso espaciales (el derribo de un satélite por un misil). Es decir, que NAVWAR no es EW al 100 por 100, y además sus efectos se producen en todos los dominios (físicos, ciberespacio y espacio).

Por último, la SARM-GE sigue de cerca los desarrollos tecnológicos de las empresas, especialmente españolas, con la finalidad de probarlos y hacer sus recomendaciones acerca de la conveniencia o no de incorporarlos a nuestras unidades con el fin de mejorar su protección ante denegaciones de PNT.

En lo que a doctrina específica de la Armada se refiere, existen algunos conceptos y guías para el planeamiento de operaciones, pero no se dispone de publicaciones que detallen TTP (tácticas, técnicas y procedimientos) o algún concepto de empleo de medios en relación con NAVWAR, ni tampoco procedimientos tácticos para las unidades.

No obstante, esta situación ya está cambiando, puesto que en 2022 la Junta de Táctica (JUTAC) identificó esta carencia como deficiencia táctica, comenzando la elaboración de un EXTAC (tácticas experimentales) que en breve se incorporará a la publicación *X-JT-01. Táctica Experimental* y que abarcará las diferentes áreas de NAVWAR (ofensiva, defensiva

y de apoyo) para todas las unidades y ámbitos de actuación⁷.

Por otro lado, en lo que respecta a la enseñanza de perfeccionamiento, NAVWAR se incluye en los cursos de EMO para oficiales (próximamente se convertirá en aptitud), así como en los de supervisor de EW para suboficiales. También en los planes de estudio de las especialidades complementarias de Sistema de Combate, Tecnologías de Comunicaciones y Control de Plataforma se están introduciendo algunas horas lectivas. Gracias a esto, se está concienciando a los oficiales y suboficiales más jóvenes sobre la importancia que tiene este asunto.

Además, la Armada, a través de la Fuerza de Acción Marítima (FAM), impulsa la participación en ejercicios como el MARSEC, en el que en uno de sus escenarios se practica la ejecución de operaciones marítimas sin señal GNSS. Estos ejercicios requieren de una detallada planificación porque la normativa nacional es muy estricta en lo relacionado con las perturbaciones del GNSS en España (por cuestiones de seguridad en la navegación aérea y marítima). Un elemento clave en dicha planificación es el *software* React, que permite predecir los efectos de una denegación GNSS en una zona determinada. Este *software* lo proporciona la OTAN a través de la NCIA⁸ y se está introduciendo progresivamente en todas las unidades de la Armada.

Además, se abre la puerta a la industria de cara a probar sus proyectos y desarrollos en cuanto a tecnología NAVWAR se refiere. Por último, la OTAN impulsa la práctica de los

7. A nivel conjunto.

8. NATO Communications and Information Agency.


mismos escenarios en las NEMO (*Naval Electromagnetic Operations*).

En ambos ejercicios se cuenta con la participación de los medios del JEWCS⁹, el cual ofrece un perturbador de GNSS. En los MARSEC también colaboran entidades universitarias españolas que aprovechan para probar sus proyectos de antenas y de perturbadores de GNSS.

Para ilustrar de alguna manera todo lo dicho hasta ahora, me gustaría proponer un caso hipotético que bien podría ocurrir en cualquier momento en alguna de las unidades navales desplegadas en cualquier zona de operaciones: una de nuestras fragatas que navega por

el mar Rojo sufre una denegación real de la señal GNSS que se mantiene durante 400 millas. El GPS civil se pierde por completo, mientras que el militar P(Y) sufre errores de posición de hasta 2°. Incluso cambiando de constelaciones para alimentar los sistemas de navegación, el radar, etc., no se consigue restablecer su operatividad hasta pasadas 20 horas.

Este caso se informa al Mando de Operaciones (MOPS) a través de su Centro de Operaciones Electromagnéticas (COEM) y se hace constar, en primer lugar, que la elevada distancia recorrida mientras dura la perturbación sugiere que podría haber varios perturbadores a lo largo de la derrota seguida; y por otra parte que, aun cambiando de constelación, las señales PNT de todas ellas fueron confundidas, lo que resulta interesante porque habría que perturbar en distintas frecuencias y además sería necesario conocer los códigos cifrados de Galileo. Las medidas de mitigación aplicadas por el barco son: navegar por estima alimentando el radar y la WECDIS (*Warship Electronic Chart Display and Information System*) con giroscópica y corredera. El futuro ya está aquí...



Predicción de efectos de una perturbación de 200 W sobre la señal L1 P(Y) a 100 pies MSL (nivel medio del mar) realizada por un dispositivo en tierra a una altura de 10 pies MSL.
(Fuente: NAVWAR Playbook)

El futuro. La obtención de una capacidad PNT robusta en las Fuerzas Armadas

Como mencioné al principio de este artículo, el sistema NAVSTAR-GPS es el que la OTAN ha establecido como primario para obtener la señal PNT. Para evitar depender de terceros países, es recomendable tener la soberanía estratégica plena sobre ella, ya que de esta forma nos aseguraríamos su disponibilidad en

9. NATO Joint Electronic Warfare Core Staff.

el caso de que tengamos que afrontar una operación militar en solitario.

Es por ello que el JEMAD autorizó el inicio del «proceso de adquisición de la capacidad PNT

No es lo mismo un barco que sólo está equipado con un GPS comercial que otro que incorpora GPS-PPS con antenas CRPA (con patrón de recepción controlado). Por lo tanto, es necesario conocer hasta qué punto se ve-

Resilience Value	PNT System Based on:	J/S Tracking Threshold {dB}	Anti Jamming Technology	Anti Spoofing Technology	Augmented System
1	GNSS Open Service (single or multiple constellations) + FRPA	44	No	No	No
2	COTS GNSS Open Service + INS + FRPA	44 + 8 = 52	Partial - due to Augmented System	Partial - due to Augmented System	Yes
2	COTS GNSS Open Service + CRPA	44 + 20 = 64	Yes	No	No
3	GNSS military encrypted + FRPA	54	No	Yes	No
3	COTS GNSS Open Service + INS (or local Timing Sys) + CRPA	44 + 8 + 20 = 72	Yes	Partial - due to Augmented System	Yes
4	GNSS military encrypted + INS + FRPA	54 + 8 = 62	Partial - due to Augmented System	Yes	Yes
4	GNSS military encrypted + CRPA	54 + 20 = 74	Yes	Yes	No
5	GNSS military encrypted + INS (or Local Timing Sys) + CRPA	54 + 8 + 20 = 82	Yes	Yes	Yes
6	Un-Reliant on external input (Super PNT)		Yes	Yes	N/A

Niveles de resiliencia asociados a plataformas. (Fuente: NAVWAR Playbook)

robusta (PNT-R) en las FAS», que permitirá obtener la plena soberanía sobre la señal. Abarca una serie de acciones, la primera de las cuales es saber cuáles son los niveles de resiliencia de cada sistema dependiente de la señal PNT para evaluar el impacto que tiene en las operaciones la denegación del acceso a ella.

rían afectados nuestros sistemas de armas en caso de tener que movernos en un entorno electromagnético degradado con pérdida de la señal PNT, y para ello la OTAN establece una clasificación por niveles de resiliencia del 1 al 6, siendo el más protegido el 6. De esta forma, podremos saber qué plataformas son las más aptas para operar en un entorno

operativo en el que se espera una alta degradación del EMS.

El empleo del Galileo PRS¹⁰ (*Public Regulated Service*) como fuente primaria de PNT es quizás la acción más importante del proceso y aporta mayor seguridad que el abierto OS (*Open Service*) porque su señal está cifrada, lo cual lo hace más resistente al *jamming* (la potencia de su señal es mayor que la del GPS) y al *spoofing* (ya que no sólo cifra el mensaje, sino también la señal moduladora). Además, tendremos plena soberanía nacional sobre la señal PNT, pues es posible utilizar un canal de recepción de la PNT alternativo al primario que se llama «canal secundario nacional». Éste dependerá directamente de una autoridad española competente en PRS (CPA) y permitirá, entre otras cosas, que seamos capaces de generar nuestras propias claves de cifrado¹¹.

No obstante, la implantación del Galileo PRS no resuelve el problema de la soberanía al 100 por 100, puesto que muchos equipos y sistemas son de procedencia estadounidense (por ejemplo, una bomba GBU-38 JDAM) y sólo reciben señales del GPS. Es por ello que será muy difícil alcanzar la autonomía de los Estados Unidos en este terreno, aunque podemos consolarnos pensando que sí seremos capaces de reducir un poco esa dependencia.

En lo que respecta a la Armada, me parece interesante mencionar cómo se va a alinear con los requisitos para alcanzar la PNT-R a través de sistemas como el SENDA (Sistema Español

de Navegación de la Armada), que incorpora GNSS e inerciales para obtener la señal PNT y lo que hace es procesar la información de todos ellos a la vez para obtener la mejor fuente PNT posible. Es capaz de trabajar con GPS-M y Galileo PRS simultáneamente y detectar el *spoofing* al comparar constantemente las soluciones obtenidas de ambos.

Por otro lado, el SENDA puede integrar sensores inerciales, de corredera *doppler*, del AIS, etc., que añadirán mayor resiliencia si se pierde la disponibilidad de los GNSS. Mejor aún: incorpora antenas CRPA que son capaces de detectar y proteger de interferencias en el GPS-M y en el Galileo PRS. Y ya para terminar, dispone de una central horaria propia, formada por un reloj atómico o de rubidio, que proporciona una señal muy precisa de sincronización horaria (T).

Las fragatas *F-110* serán las primeras en utilizar el SENDA y, gracias a la integración de los equipos y sistemas arriba mencionados, podrán tener un nivel 5 de resiliencia frente a denegaciones de la señal PNT (prácticamente más elevado según la tabla anterior).

Conclusión

En los últimos años han aumentado exponencialmente los actos de denegación de las señales GNSS con el fin de negar el acceso a la información de la señal PNT a los usuarios afectados, tanto civiles como militares. Los efectos que provocan podrían traducirse en la

10. Los servicios prestados por Galileo son: *Open Service* (OS), *Search and Rescue* (SAR), *Commercial Service* (CS) y el PRS, que es el único cifrado. Como es lógico, ciertos países de la OTAN no pertenecientes a la UE tienen limitado el acceso completo al servicio PRS.

11. El control de las claves disminuye nuestra vulnerabilidad a consecuencia de depender de un único GNSS (GPS), del que además no tenemos su propiedad.

pérdida de las capacidades necesarias para garantizar el éxito en una operación militar al depender la inmensa mayoría de nuestros sistemas de armas, de navegación, etc., de la señal PNT, de forma que puedan sincronizarse y obtener los datos de posicionamiento y navegación.

La OTAN ha identificado esta vulnerabilidad y ha agrupado bajo las siglas de NAVWAR todas las acciones militares encaminadas a alcanzar la superioridad y mantener el acceso a la señal PNT, a la vez que se le niega al adversario. A su vez, NAVWAR forma parte de un concepto mucho más amplio, denominado Operaciones Electromagnéticas (EMO) que consisten en la coordinación de todas las actividades que utilizan el espectro electromagnético, entre las que se encuentran EW, SIGINT, SM y NAVWAR. Además, NAVWAR puede utilizarse en operaciones multidominio al ser empleada tanto en los dominios físicos como no físicos.

La Armada está apostando fuertemente por posicionarse a la cabeza de las Fuerzas Armadas en materia de NAVWAR. Para ello, la Sección de Armas y Guerra Electrónica del Estado Mayor de la Armada no sólo impulsa y supervisa todos los desarrollos tecnológicos que ofrece la industria tanto nacional como extranjera, sino que además participa en todos los grupos de trabajo de doctrina OTAN y nacional. En este sentido, ya están a punto de incorporarse a la doctrina técnicas y tácticas

experimentales que contribuirán a cubrir el vacío doctrinal que hasta ahora ha existido en materia de NAVWAR. Como colofón final, ya se han introducido en los planes de estudios de la enseñanza de perfeccionamiento módulos dedicados a NAVWAR con la finalidad de mentalizar a los jóvenes oficiales y suboficiales de su importancia e influencia en las operaciones militares.

A nivel conjunto, la fuerte dependencia estratégica y la absoluta carencia de soberanía sobre la señal GPS han obligado a las Fuerzas Armadas a buscar alternativas encaminadas a obtener una capacidad PNT robusta, lo que implicará obtener la plena soberanía sobre la señal GNSS. El empleo del Galileo como fuente primaria de la señal PNT es la línea de actuación principal, además de otras muchas, aunque se tardará todavía tiempo en obtener la plena independencia estratégica respecto al GPS, debido a que la inmensa mayoría de nuestros equipos y sistemas son de procedencia estadounidense y emplean la PNT del GPS.

BIBLIOGRAFÍA

- AC/322-D (2021) 0016 Navigation Warfare (NAVWAR) Playbook.
AC/322-N (2019) 0104 NAVWAR Primer. Edition B. May 2019.
STANAG 4621. NAVWAR Definition.