ieee.es
Instituto Español de Estudios Estratégicos

Documento
Opinión

56/2018 14 de mayo de 2018

*Jesús Abraham Fernández**

La necesidad de un nuevo sistema de Seguridad Integral 4.0 para instalaciones navales

La necesidad de un nuevo sistema de Seguridad Integral 4.0 para instalaciones navales

Resumen:

Las instalaciones navales han sido desde hace siglos fortalezas infranqueables dotadas de un elevado nivel de seguridad. Una seguridad que, debido a la aparición de nuevas tecnologías en el ámbito civil, es necesaria reevaluar en el nuevo escenario multidimensional.

Palabras clave:

Instalaciones navales, Seguridad Integral, PESCO, Armada 4.0

The need for a new 4.0 Integral Security system for naval installations

Abstract:

Naval facilities have been for centuries insurmountable fortresses with a high level of security. A security that, due to the appearance of new technologies in the civil field, it is necessary to re-evaluate in the new multidimensional scenario.

Keywords:

Naval facilities, Integral Security, PESCO, Armada 4.0

*__NOTA:__ Las ideas contenidas en los ***Documentos de Opinión*** son de responsabilidad de sus autores, sin que reflejen, necesariamente, el pensamiento del IEEE o del Ministerio de Defensa.

A lo largo de los últimos años hemos experimentado un aumento en el tipo y número de amenazas, principalmente de tipo asimétrico.

Las nuevas tecnologías han «democratizado» en cierta medida el uso del conflicto armado, proporcionando a actores no gubernamentales múltiples herramientas que, usadas con fines dañinos, se pueden convertir en armas o favorecer el uso de estas contra ejércitos organizados y bien equipados, así como a infraestructuras críticas, con un alto índice de eficacia y letalidad.

El elevado gasto en I+D+i del sector privado durante los últimos años ha reducido notablemente el *gap* entre las tecnologías comerciales y las aplicadas exclusivamente a la seguridad y defensa, obligando a las Fuerzas Armadas y los Cuerpos de Seguridad del Estado a redefinir sus procesos de Gestión de Innovación y a aumentar su inversión en I+D+i. Este hecho se ha visto materializado, por ejemplo, en el *Third offset strategy* del antiguo secretario de Defensa de EE. UU., Chuck Hagel.

Mientras estas nuevas herramientas al servicio de la sociedad se han ido desarrollando, las antiguas instalaciones portuarias militares o civiles han visto cómo sus vulnerabilidades se han incrementado en zonas y aspectos hasta ahora protegidos y seguros.

Se podría pensar, por ejemplo, en el caso del Arsenal Militar de Ferrol o de Cartagena para los que hayan tenido la posibilidad de conocerlo. Aunque el caso es perfectamente extrapolable a cualquier puerto civil dado el gran impacto que un ataque contra un buque dentro de un recinto portuario podría tener, especialmente en aquellos en los que se trabajan con derivados del petróleo o productos químicos.

Estas instalaciones navales se diseñaron y construyeron en el siglo XVIII, y basaban su seguridad en altos y robustos muros a lo largo de todo el perímetro con garitas de observación para los centinelas, ubicados en bahías fuertemente protegidas por castillos o baluartes que eran capaces de cerrar los accesos por mar y abrir fuego de artillería contra una flota enemiga que decidiese aproximarse. También se cuidaba la defensa extendida, instalando torres de vigía y baterías de costa en los puntos de ésta donde una flota enemiga pudiese llevar a cabo un desembarco próximo a las instalaciones navales.

Así pues, la ventaja táctica por tierra y mar, las dos únicas dimensiones de la guerra por aquel entonces, estaba servida.

Figura 1. Panorámica de Ferrol

Figura 2. Defensa interior de la ría de Ferrol (www.ferrol.es)

Figura 3. Defensa exterior de la ría de Ferrol

Figura 4. Defensa exterior (www.ferrol.es)

No obstante, las cosas han cambiado considerablemente en el siglo XXI. Aunque se mantienen las amenazas tradicionales, más desarrolladas y sofisticadas si cabe, han aparecido nuevas amenazas y nuevos dominios en los que se libra una guerra o conflicto,

poniendo a disposición de cualquier ciudadano o actor no gubernamental la capacidad de realizar un ataque antes únicamente al alcance de un ejército o fuerza naval al servicio de un Estado soberano.

Estas nuevas amenazas, principalmente de carácter asimétrico, han permitido que, con un mínimo coste económico material y humano, se pueda poner en peligro a una fuerza naval en sus propias instalaciones o dañar gravemente las infraestructuras críticas portuarias causando un elevado coste medioambiental, material y personal.[1]

Así las cosas, y dado que los recursos humanos y materiales no han jugado a nuestro favor en estos tiempos de restricciones económicas, se hace necesario realizar un análisis transversal y horizontal para encontrar soluciones de seguridad integral que nos permitan mantener la superioridad táctica en nuestras instalaciones portuarias a fin de poder proteger a las unidades y al personal en ellas ubicadas frente a posibles ataques asimétricos por tierra, mar, aire o el ciberespacio. Para ello, se requiere un estudio pormenorizado de riesgos, vulnerabilidades y amenazas que permita diseñar un sistema de seguridad integral que pueda hacer frente a las amenazas asimétricas que utilicen cualquiera de los dominios presentes en la actualidad de forma automatizada y utilizando el mínimo número de recursos humanos y materiales, aprovechando para ello el uso de las nuevas tecnologías al servicio de la seguridad y la defensa. Teniendo en consideración requisitos tan importantes como los costes de adquisición y mantenimiento, escalabilidad, resiliencia, integrabilidad o ciberseguridad entre otros.

Conscientes de la necesidad de seguir manteniendo la seguridad dentro de las instalaciones portuarias en las antiguas y nuevas dimensiones, este aspecto se recoge como uno de los 12 proyectos europeos de defensa en los que participa España dentro del marco de la recién aprobada PESCO (cooperación estructurada permanente). Concretamente, en el proyecto de vigilancia marítima y protección de puertos, al que también se han sumado Grecia y Portugal.

La ministra de Defensa, María Dolores de Cospedal, no ha concretado cuántos de los 12 proyectos aprobados en los que participará España cree que podrían optar a recibir ayudas del Fondo Europeo de Defensa, y ha recordado que hasta junio no se acordarán las normas de gobernanza de los proyectos, algo que «va a determinar hasta qué punto

[1] https://www.aspistrategist.org.au/changing-face-maritime-terrorism/

y de qué manera van a recibir financiación» y también habrá que calcular «la cuantía definitiva» de cada proyecto.

Este Fondo, que contará con 590 millones de presupuesto para comenzar con las fases de investigación y definición de prototipos iniciales, se podría incrementar en 10.000 millones adicionales a partir de 2021 de mantenerse la estabilidad y previsión de crecimiento económico en Europa. Es, por tanto, el punto de partida de la tan anhelada Europa de la Defensa que durante años ha estado paralizada en parte por la reticencia de Reino Unido, y en parte por la sensación de Seguridad que proporcionaba nuestro principal aliado y mayor potencia militar, EE. UU.

No obstante, la nueva coyuntura política y la creciente inestabilidad mundial ha hecho del desarrollo de la industria europea de defensa una necesidad y no una opción.

España, por su parte, ha mostrado la capacidad e intención de erigirse como un socio fundamental en este nuevo marco. Y fruto de ello es la participación en 12 de los 17 proyectos iniciales de este primer impulso a un sector estratégico esencial para la seguridad y defensa europea y de los intereses de la industria nacional, la cual posiblemente tenderá a una nueva regulación que permita la especialización por capacidades en pro de una necesaria reducción de costes y aumento de la competitividad en el escenario internacional.

Dominio terrestre

Dentro de este dominio podemos encuadrar las amenazas físicas cuyo vector de ataque sea proyectado desde tierra. A efectos de este estudio identificamos las siguientes:

- Vehículos pesados lanzados a gran velocidad contra los paramentos verticales al objeto de establecer una brecha física por la que poder entrar con otros vehículos o a pie. Una solución viable para esta amenaza es la instalación de bolardos férreamente anclados al firme a una distancia tal que impida el paso de vehículos a lo largo del perímetro. En aquellos lugares donde sea posible, la instalación de un contraperaltado a modo de foso sería incluso más efectivo.
- Vehículos que traten de eludir el control de accesos. Una solución viable para esta amenaza es la utilización de lectores de matrícula integrados en un sistema integral de seguridad de manera que impida el acceso mediante barrera a aquellos vehículos

cuyo paso no esté previamente autorizado, y la instalación de una barrera anti-pánico que bloquee cualquier intento de intrusión por la fuerza. Este sistema, instalado en el control de acceso de vehículos, debería trabajar conjuntamente con un sistema de reconocimiento facial o lector de retina que identifique a todos los ocupantes del vehículo, un scanner que permita la visualización de espacios ocultos como pueden ser los maleteros o los bajos, y un detector de explosivos mediante el análisis químico del aire en las inmediaciones del vehículo. El sistema, automáticamente y con la supervisión de un centinela, permitiría el acceso a los vehículos y ocupantes autorizados o daría la voz de alarma en caso de cualquier discrepancia.[2]

- Personas físicas que traten de acceder al interior del recinto franqueando los paramentos verticales. Dada la altura de los paramentos verticales que delimitan el perímetro terrestre, es complicado el acceso a través de estos. No obstante, mediante la instalación de cámaras EO/IR con procesos de videoanálisis con capacidad de detección de movimiento y alarma automática integradas en el sistema de seguridad integral se podría tener un control perimetral sin fisuras que permitiese avisar a la guardia de seguridad en caso de intento de intrusión.[3]
- Personas físicas que traten de acceder al interior del recinto eludiendo el control de accesos. Este es posiblemente el método más asequible para realizar un ataque asimétrico. Mediante técnicas de ingeniería social y decepción, o mediante un ataque sorpresa por saturación, es posible que un grupo de individuos armados pueda intentar acceder al interior del recinto por las puertas de acceso. Puesto que el personal de guardia de armas en estos accesos no es ilimitado para hacer frente a un ataque de este estilo, la delimitación de vías de acceso a pie es una opción viable y asequible que permitiría tener un mínimo tiempo de reacción para un repliegue y cierre físico de accesos. Estas vías de acceso a pie deberían estar físicamente delimitadas mediante un vallado y contar con una jaula de acceso con doble

[2] https://www.theguardian.com/world/2011/sep/11/us-base-suicide-bomber-afghanistan
http://www.mirror.co.uk/news/world-news/drone-footage-suicide-bomb-attack-9114605
http://www.rtve.es/noticias/20170118/medio-centenar-muertos-ataque-suicida-norte-mali/1475180.shtml

[3] http://www.geutebrueck.com/es_ES/pagina-de-inicio-del-producto-31934.html

identificación, reconocimiento facial/lectura de retina y tarjeta, y un detector de explosivos mediante el análisis químico del aire alrededor del individuo tipo arco.[4]

Dominio marítimo

Dentro del dominio marítimo es donde posiblemente se dé una mayor vulnerabilidad, pues las diferentes amenazas se pueden presentar sobre la superficie y por debajo de esta, una cualidad esta última que dificulta su detección y seguimiento.

Si bien en el siglo XIII las amenazas cuyo vector de ataque proyectado desde la mar se ceñían a fuerzas navales con tropas de infantería embarcada que pudiesen llevar a cabo un desembarco en la costa cerca de las instalaciones militares, o incluso un bloqueo naval desde el que asediar con fuego de cañón, pero con tiempo suficiente de reacción desde que se advertía la presencia enemiga, las amenazas que se presentan hoy en día son principalmente de índole asimétrico y con un mínimo tiempo de reacción.

Estas amenazas pueden proyectarse de la siguiente manera:

- Sobre la superficie en forma de lancha rápida cargada de explosivos, bien pilotada remotamente o por un terrorista suicida. Ante esta situación, una posible solución pasa por la instalación de un radar asociado a una dirección de tiro con cámara EO/IR y una *laser gun* como arma anti asimétrica. Otra medida añadida sería la instalación de una barrera de flotabilidad positiva retráctil desde el fondo hasta la superficie, de manera que una vez activada la alarma de superficie esta se dispare y pueda desplegarse en superficie impidiendo el paso de embarcaciones en menos de tres segundos, a través del interface humano del sistema de seguridad integral.[5]
- Bajo la superficie en forma de buceadores o UUV. Ante esta situación, una posible solución pasa por la instalación de un sonar 3D sectorial de fondo con cámaras subacuáticas, todo ello integrado en el sistema de seguridad integral. Este sistema permitiría la detección, seguimiento y reconocimiento de las amenazas subacuáticas, y la activación de la barrera de flotabilidad positiva retráctil que, una vez desplegada

[4] http://edition.cnn.com/2016/11/11/asia/afghanistan-bagram-blast/

[5] http://www.maritime-executive.com/article/drone-boat-used-to-strike-saudi-frigate

en superficie, extienda una malla resistente desde el fondo a la superficie pudiendo estar esta electrificada.[6]

Dominio aéreo

Es en este dominio donde se puede presentar un mayor porcentaje de probabilidad de ataque. Hoy en día, el uso de cualquier dron comercial con un alcance superior a 500 metros, puede suponer una amenaza real para las instalaciones navales dada su proximidad a la zona urbana donde se encuentran. La facilidad de adquisición y manejo, así como su compleja detección, seguimiento y enfrentamiento, los convierten en excepcionales vectores de ataque asimétricos.[7]

Dado que estos sistemas cuentan con cámaras de TV, posicionamiento GPS y, en algunos casos, sistemas de navegación inercial o de reconocimiento del medio mediante videoanálisis, se hace muy compleja su eliminación.

Si bien un sistema de *jamming* sobre la señal GPS, wifi y radiocontrol estándar puede suponer una buena herramienta, esta no es infalible contra los drones que cuentan con sistemas de navegación inercial o de reconocimiento del medio por videoanálisis.

En este caso, las armas de energía dirigida o las de pulso electromagnético tampoco son las más adecuadas en entornos urbanos, pues pueden provocar graves daños a la infraestructura civil.

Así pues, una opción viable sería la integración de armas «no letales» integradas en sistema de vigilancia radar y EO/IR con procesos de videoanálisis como el que se muestra en la imagen, basado en la utilización de proyectiles sin carga explosiva que despliegan redes capaces de atrapar y derribar a los drones en vuelo.

---

[6] https://www.electronica-submarina.com/defensa/sonar-y-sistemas-embarcados/dds-03-sonar-de-deteccion-de-intrusos/

[7] https://www.nytimes.com/2016/10/12/world/middleeast/iraq-drones-isis.html?_r=0
https://www.bellingcat.com/uncategorized/2017/02/10/death-drone-bombs-caliphate/
http://www.thedailybeast.com/articles/2017/02/28/as-isis-prepares-its-terror-resurrection-watch-out-for-drone-swarms.html
http://heavy.com/news/2017/01/new-isis-islamic-state-video-knights-of-bureaucracy-mosul-iraq-wilayat-ninawa-modified-weaponized-drones-bombings-airstrikes-uncensored-video/

Foto 5. Sistema «no letal» anti-drones

Dominio del ciberespacio

Este ha sido el último dominio reconocido por la OTAN, entendiendo como tal «el ámbito artificial creado por medios informáticos» según la RAE.

Puesto que la eficacia y eficiencia del sistema informático que albergue este sistema de seguridad integral se basa en la posible utilización de una base de datos MySQl única corriendo sobre un entorno LINUX, esta tiene que presentar unas garantías de confidencialidad, integridad, seguridad y disponibilidad que le permitan que estar accesible desde la red segura del Ministerio de Defensa.

Uno de las mayores brechas de seguridad de la información que afectan a la LOPD 15/1999, de 13 de diciembre, (que se actualizará en mayo de 2018 al nuevo RGPD) es el incremento exponencial de bases de datos que albergan datos de carácter personal de personal militar y civil del Ministerio de Defensa en las diferentes UCO, así como el almacenamiento y uso que se hace de estos datos.

El establecimiento de una única base de datos con diferentes API que permitan, dentro del marco de la Arquitectura Técnica Unificada, acceder a las múltiples aplicaciones orientadas a servicios desarrolladas en el Ministerio de Defensa y que requieren datos personales sería un buen comienzo para la «securización» de los datos de carácter personal y el cumplimento eficiente del nuevo RGPD, complementario a lo ya ganado con el actual sistema SILOPDEF.

Esta base de datos única debería contener todos los datos del personal militar y civil que puedan tener relación con el Ministerio de Defensa o afecten a la Seguridad Nacional, de tal manera que simplemente cruzando datos biométricos o identificativos se pueda tener un férreo control de los accesos de personal a las diversas instalaciones militares, independientemente si estos están en Madrid, Ferrol, Cartagena, Canarias, Cádiz o donde se requiera. Empresas contratistas, subcontratistas o visitas oficiales tendrían un mejor control y gestión de acceso evitando largos trámites y una mayor eficiencia del recurso humano en los controles de seguridad.

De esta manera, múltiples aplicaciones, entre las que por supuesto se encuentra la aplicación ideada para el Sistema de Seguridad Integral objeto del presente artículo, podrían acceder de forma rápida y segura a los datos necesarios para el cumplimiento de sus objetivos operacionales. No solo se mejoraría en aspectos de seguridad sino también en una mejor racionalización de los datos y el hardware que soporta las diferentes bases de datos existentes, y por lo tanto del recurso económico dedicado a la mejora de la seguridad.

Volviendo al sistema que nos centra, la aplicación que gestione el control de accesos de personal y vehículos debe permitir tener diferentes niveles de usuario. Desde el súper administrador, quién gestiona la totalidad de la aplicación, pasando por el administrador local que se encarga de las altas/bajas o modificaciones de usuarios o vehículos en determinadas instalaciones, hasta el usuario final que debe poder acceder a los diferentes trámites telemáticos a fin de poder cursar la solicitud de accesos a las diferentes instalaciones en base a sus necesidades. De esta forma se evitarían largas esperas en las Oficinas de Seguridad de las diferentes instalaciones militares y una reducción en los tiempos de trámite. Una simple y rápida tramitación telemática previa permitiría, de forma segura, poder autorizar los accesos del personal y los vehículos a aquellas dependencias a las que necesiten acudir.

Igualmente, se eliminaría el crecimiento exponencial de las actuales tarjetas de accesos a los diferentes recintos, redes y servicios. Con una única tarjeta basada en tecnología RFID sería suficiente para dotar a todo el personal que lo requiera de los diferentes accesos a dependencias, redes y servicios. Una tecnología de autenticación material que podría utilizarse complementaria o alternativamente, según las necesidades, con otra de

autenticación personal basada en reconocimiento facial, o lectura de retina, huella o conocimiento, lo cual dotaría de una mayor seguridad a los diferentes accesos

Y todo ello bajo la premisa de ser utilizada a través de la red segura de la red privada del Ministerio de Defensa. Esta seguridad se puede conseguir mediante las técnicas SSL ya utilizadas en las conexiones bancarias por internet.

Conclusiones

Las nuevas amenazas del siglo XXI han creado nuevos riesgos que han hecho aparecer vulnerabilidades en zonas que hasta ahora eran inimaginables. Estas nuevas amenazas han demostrado estar al alcance de cualquier persona u organización con una escasa inversión económica y mínima exposición.

A pesar de que el riesgo cero no existe, un enfoque integral y multidimensional de las diferentes amenazas y vulnerabilidades nos ayudará a hacer una mejor evaluación de riesgos que redunde en una seguridad física más adaptada a las necesidades del siglo XXI, pues las instalaciones portuarias han pasado a ser un objetivo estratégico en los planes de diversas organizaciones terroristas.[8]

Tomando como referencia la bahía de Ferrol, que cuenta con las unidades navales más tecnológicamente avanzadas de la Armada Española por valor de más de cuatro mil millones de euros, el astillero público Navantia, el puerto comercial de la ciudad y la planta regasificadora Reganosa entre otros activos de interés, donde trabajan en su conjunto y a diario más de tres mil profesionales, la inversión en un sistema como el propuesto, que no alcanza los 15 millones de euros, supondría un ROI (*Return On Investment*) más que considerable.

[8] http://www.abc.net.au/news/2015-12-23/two-charged-after-sydney-counter-terrorism-raids/7049918
http://www.dnaindia.com/world/report-multiple-blasts-at-a-mosque-inside-bangladesh-navy-base-6-injured-2157389
http://www.dailymail.co.uk/news/article-2756249/Newly-formed-Al-Qaeda-branch-India-botches-terror-attack-mistakenly-trying-capture-Naval-ship-thought-American-aircraft-carrier.html
https://tribune.com.pk/story/174808/pns-mehran-attack-vulnerable-embarrassed-and-targeted/

Un ataque asimétrico por saturación podría dañar la capacidad de proyección de la fuerza naval española, causar unos elevados daños medioambientales, económicos, materiales y personales, y crear un impacto psicológico entre la población de dimensiones inconcebibles.

A pesar de que el nivel de alerta antiterrorista para las FAS no se incrementado en la misma medida que lo ha hecho el de del Estado (Nivel 4), es necesario dotarse de medios adecuados que permitan incrementar el estado actual al deseado en un corto periodo de tiempo optimizando al máximo los recursos.

Debemos asumir cuanto antes que con un ataque de bajo nivel de planificación y coste (se estima que un ataque asimétrico efectivo podría costar menos de 10 000 euros) se puede causar un daño considerable a una flota, un área de población y la economía de la región en cuestión de minutos. A pesar de la gran capacidad de los medios actuales, se hace necesaria una nueva evaluación de riesgos y amenazas para que, con el menor número de recursos y la mayor eficacia y eficiencia, se pueda seguir manteniendo en un futuro la ventaja táctica de la que hasta ahora hemos gozado.

La Armada Española, como actor experimentado y de referencia en la materia, está en la mejor disposición para liderar este proyecto coordinando al conjunto de la administración nacional, de Comunidades Autónomas y de las ciudades con Estatuto de Autonomía de Ceuta y Melilla. Así como los órganos que correspondan de las distintas Comunidades Autónomas según lo dispuesto en los respectivos Estatutos de Autonomía en conexión con las competencias relacionadas con la Seguridad Nacional y las autoridades locales, a través del recientemente regulado Consejo Nacional de Seguridad Marítima presidido por el Jefe del Estado Mayor de la Defensa, y en el que la Armada Española cuenta con una importante representación.

El actual ciclo inversor, las favorables previsiones macroeconómicas, y el decidido impulso político nacional y europeo hacen de este el momento idóneo para mostrar el liderazgo de España en este proyecto que requiere de una adecuada estrategia de gestión de la innovación entre el sector académico, empresarial y público a fin de posicionar a nuestro país como un referente en seguridad portuaria. Y conseguir las economías de escala que permitan incrementar la ventaja competitiva en un mercado globalizado y, por ende, el mantenimiento de las capacidades necesarias en el presente y futuro escenario de inestabilidad.

Es, sin duda, la gran apuesta de Europa para asegurar su propia seguridad y defensa. Y España tiene la opción y la capacidad de aportar su gran potencial humano e industrial para consolidarse como actor clave.

> «Hemos activado una Cooperación Estructurada Permanente en materia de defensa, ambiciosa e inclusiva. 25 Estados miembros se han comprometido a unir sus fuerzas de manera regular, hacer cosas juntos, gastar juntos, invertir juntos, comprar juntos y actuar juntos. Las posibilidades de la Cooperación Estructurada Permanente son inmensas».
>
> Federica Mogherini,
> diciembre de 2017

*Jesús Abraham Fernández**
Teniente de navío
Segundo comandante P-46 «Furor»